

Draft Letter Report

**TASK 1—CONTROL AND PROTECTION SYSTEMS IN VHTRS
FOR PROCESS HEAT APPLICATIONS**

T. L. Wilson, Jr., W. P. Poore, T. J. Harrison, and R. A. Joseph
Oak Ridge National Laboratory

September 2010

Prepared for the
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

	Page
LIST OF FIGURES	vii
LIST OF TABLES	ix
1. INTRODUCTION	1
1.1 Project Overview	1
1.2 Objectives	1
2. DESCRIPTION OF THE BASIC SYSTEMS IN GAS-COOLED REACTORS	2
2.1 Prismatic Reactor Core Subsystem	3
2.2 Pebble Bed Reactor Core	6
2.3 Reactor Internals	7
2.4 Main Heat Transport Systems	8
2.4.1 Secondary steam cycle power generation	9
2.4.2 Direct cycle, gas turbine energy conversion	12
2.4.3 Process heat systems	14
2.5 Reactor Service Systems	14
2.6 Safety Systems	15
2.7 Engineered Safety Features	15
2.7.1 Shutdown cooling system	15
2.7.2 Vessel cooling system	16
2.7.3 Containment/confinement structure	18
3. DESCRIPTION OF INSTRUMENTATION AND CONTROL SYSTEMS FOR SAFETY AND CONTROL OF HTGRs	18
3.1 Description of Basic Safety and Control Strategies in Gas-Cooled Reactors	19
3.2 Protection Systems	19
3.2.1 Regulatory basis for protection systems of HTGRs	19
3.2.2 Proposed applicability of NRC's or advanced reactor characteristics to HTGRs	22
3.2.3 Protection system functions	24
3.3 Operational Controls	27
3.3.1 Startup and shutdown	27
3.3.2 Normal operation	28
4. DESCRIPTION OF PROTECTION AND CONTROL SYSTEMS	33
4.1 HTGR Descriptions	33
4.2 Modular High Temperature Gas Reactor—MHTGR	33
4.2.1 Reactor system design	33
4.2.2 Current status	35
4.2.3 Plant protection, instrumentation, and control systems	37
4.2.4 Miscellaneous control and instrumentation group	49
4.2.5 Safety evaluation	49
4.2.6 Concerns from a regulatory perspective	55
4.3 High Temperature Engineering Test Reactor (HTTR)—Japan	57
4.3.1 Reactor system design	57
4.3.2 Reactor cooling system	64

4.3.3	Engineered safety features	66
4.3.4	Instrumentation and control system	67
4.3.5	Safety and demonstration tests planned in HTTR.....	73
4.3.6	Safety evaluation.....	73
4.4	Arbeitsgemeinschaft Versuchsreaktor–AVR.....	80
4.4.1	Reactor system design ²⁷	80
4.4.2	Heat transport loop.....	83
4.4.3	Online refueling	85
4.4.4	Containment	86
4.4.5	Shutdown cooling system.....	88
4.4.6	Helium purification plant	88
4.4.7	Current status	88
4.4.8	Plant instrumentation and control systems.....	88
4.4.9	Safety evaluation.....	92
4.5	Fort St. Vrain Reactor	97
4.5.1	Reactor system design.....	97
4.5.2	Decay heat removal systems	100
4.5.3	Containment heat removal	101
4.5.4	Leak detection systems.....	101
4.5.5	Current status	102
4.5.6	Plant protection, control, and instrumentation systems.....	102
4.5.7	Plant control system	108
4.5.8	Plant control system transient events	112
4.5.9	Plant instrumentation	115
4.5.10	Safety evaluation.....	122
4.5.11	Evaluation of operating experience.....	124
4.5.12	Significant issues.....	125
4.6	10 MW High Temperature Gas-Cooled Test Reactor (HTR-10).....	125
4.6.1	Reactor system design.....	125
4.6.2	Heat transport loop.....	128
4.6.3	Online refueling	128
4.6.4	Confinement.....	131
4.6.5	Shutdown cooling system.....	132
4.6.6	Helium purification plant	132
4.6.7	Plant instrumentation and control systems.....	134
4.6.8	Safety evaluation.....	137
5.	NEXT GENERATION NUCLEAR PLANT—NGNP	139
5.1	Reactor System Design	139
5.2	Current Status.....	139
5.3	Fuel	140
5.4	Westinghouse PBMR Design.....	142
5.4.1	Reactor	142
5.4.2	Shutdown cooling.....	143
5.4.3	Reactor cavity cooling.....	143

5.4.4	Fuel handling.....	143
5.4.5	Helium services.....	143
5.4.6	Instrumentation and control systems.....	143
5.5	AREVA Prismatic Core Design.....	148
5.5.1	Reactor.....	148
5.5.2	Shutdown cooling.....	151
5.5.3	Reactor cavity cooling.....	151
5.5.4	Fuel handling.....	152
5.5.5	Helium services.....	152
5.6	General Atomics Prismatic Core Design.....	152
5.6.1	Reactor.....	153
5.6.2	Shutdown cooling.....	153
5.6.3	Reactor cavity cooling.....	153
5.6.4	Fuel handling.....	154
5.6.5	Helium services.....	154
5.7	Power Conversion and Hydrogen Production.....	154
5.8	Vendor Design Comparisons.....	157
5.9	Pending Issues.....	158
6	KEY ISSUES IN I&C FOR NGNP.....	159
6.1	Issues in Licensing.....	159
6.1.1	Safety system vs investment protection system.....	159
6.1.2	Confinement vs containment.....	160
6.2	Issues in Protection System.....	161
6.2.1	High-temperature effects.....	161
6.2.2	New types of protection systems.....	161
6.3	Issues in Control Systems.....	161
6.3.1	Automation and operational awareness.....	161
6.3.2	Protection of heat exchangers from hot helium in loss of process heat plant.....	162
6.3.3	Support system controls.....	162

LIST OF FIGURES

Figure		Page
1	Plan view MHTGR core	4
2	TRISO fuel particle	4
3	Fuel components	5
4	Fuel element	5
5	Conceptual design of pebble fuel	6
6	Pebble bed modular reactor–reactor vessel	7
7	Vessel internals	8
8	Reactor and steam generator for MHTGR	9
9	Simplified power generation flow diagram	10
10	Typical steam generator tube	11
11	Main circulator design for MHTGR	12
12	Simplified process flow diagram for GT-MHR	13
13	Conceptual process flow for combined gas turbine and process heat plants (General Atomics)	14
14	Example shutdown cooling system (SCS) in a prismatic core modular HTGR	16
15	Passive decay heat removal in the RCCS	17
16	Representative water cooled RCCS flow diagram (AREVA NGNP)	18
17	Two-level cascade controller with demand output	29
18	Two level control with increase/decrease output	29
19	Turbine generator configuration and heat balance	36
20	Protection system data buses	39
21	Plant supervisory control subsystem control overview	42
22	Plant control and interface configuration	43
23	NSSS control subsystem functions and interfaces	47
24	MHTRG module response to reactor trip	48
25	MHTGR module response to turbine trip	49
26	Core temperatures during depressurized conduction cooldown	52
27	Cumulative frequency for whole body dose	54
28	Cumulative frequency for thyroid dose	54
29	HTTR pressure vessel and core	59
30	HTTR fuel	61
31	HTTR reactor internals	62
32	HTTR control rod	63
33	Reactor pressure vessel	64
34	Main cooling system	65
35	Nuclear instrumentation	68
36	Nuclear instrumentation	69
37	Reactor coolant outlet temperature control instrumentation	70
38	Reactor coolant outlet temperature control instrumentation	71
39	Sequence of abnormal events	75
40	Sequence of abnormal events	76

41	Vertical cross section of AVR reactor	81
42	AVR reflector with graphite “nose” extending into pebble bed	83
43	Circuit diagram of the AVR steam generator with materials and dimensions	84
44	Diagram of AVR online refueling system	86
45	AVR double pressure vessel and sealed containment	87
46	Demonstration of inherently safe shutdown of the AVR	94
47	Demonstration of decay heat removal in depressurized loss-of-flow event at AVR.....	95
48	Fort St. Vrain fuel showing fissile and fertile particles, fuel rod (compact of particles), and hexagonal matrix fuel element.....	97
49	Fort St. Vrain arrangement of components within the PCRV	98
50	Turbine generator configuration and balance of plant.....	100
51	Control logic diagram—scram logic	104
52	Primary coolant pressure vs circulator inlet temperature	105
53	Programmed trip limits for helium circulator speed vs feedwater flow	106
54	Fort St. Vrain plant control system.....	109
55	Normal load change at maximum design rate	113
56	Turbine trip from full load.....	114
57	Reactor scram from full power	115
58	Nuclear instrumentation diagram	116
59	Core locations for startup sources (and detectors).....	117
60	Moisture sampling system	118
61	Moisture detector—operating in trip mode	120
62	Moisture detector—operating in indication mode	121
63	The HTR-10 reactor and steam generator arrangement in the primary cavity	127
64	Online refueling system; cross-section of the HTR-10	130
65	Schematic of the HTR-10 helium purification system	133
66	HTR-10 data acquisition and control system.....	135
67	TRISO fuel	140
68	PMBR	142
69	Reactor cavity cooling system	144
70	Prismatic reactor	149
71	Prismatic fuel blocks	149
72	RPV	150
73	RCCS	151
74	Fuel handling system	152
75	Fuel block assembly	153
76	RCCS	154
77	Fuel handling system	155
78	Westinghouse original NGNP configuration.....	155
79	AREVA original NGNP configuration.....	156
80	General Atomics original NGNP configuration	157

LIST OF TABLES

Table		Page
1	PBMR's analysis of advanced reactor characteristics	23
2	Protection variables and setpoints for HTR-10.....	25
3	Design basis accidents, protection variables, and their group definition.....	26
4	Cascade control schemes for three HTGRs	31
5	MHTGR design parameters.....	34
6	PCSC control strategy for normal startup or shutdown.....	44
7	PCSC control strategy for normal startup or shutdown.....	45
8	PCSC control strategy for normal startup or shutdown.....	46
9	HTTR design parameters.....	58
10	HTTR design parameters.....	60
11	Containment specifications.....	67
12	Reactor scram and engineered safety features actuation signals	72
13	Safety demonstration test schedule.....	73
14	Postulated events classified into AOOs.....	77
15	Postulated events classified into accidents	77
16	Single failures consideration for AOOs.....	78
17	Single failures consideration for accidents	79
18	Initial conditions for normal reactor operation	80
19	Main design characteristics and safety concept.....	82
20	Fort St. Vrain design parameters	99
21	Major design parameters of the HTR-10 test reactor	129
22	Reactor protection system trip parameters of the HTR-10	134
23	Principal parameters of the fuel handling system.....	137
24	Generic NGNP reactor parameters	141

TASK 1—CONTROL AND PROTECTION SYSTEMS IN VHTRS FOR PROCESS HEAT APPLICATIONS

DRAFT LETTER REPORT

T. L. Wilson, Jr., W. P. Poore, T. J. Harrison, and R. A. Joseph
Oak Ridge National Laboratory

September 24, 2010

1. INTRODUCTION

1.1 Project Overview

The objective of JCN 6177 is to support NRC in identifying and evaluating the regulatory implications concerning the control and protection systems proposed for use in the Department of Energy's (DOE) Next Generation Nuclear Plant (NGNP). The NGNP, using gas-cooled reactor technology, will provide the basis for the commercial industry to manage the heat for energy production and industrial processing including hydrogen production. The high temperature gas-cooled reactor (HTGR) can provide heat for industrial process at much higher temperatures than conventional light water reactors, from 700 to 950°C. (Note that for the upper range of these operating temperatures the HTGR is sometimes referred to as the Very High Temperature Reactor or VHTR. In this project, the gas-cooled reactor design for the NGNP is referred to as the VHTR even though DOE's current plans focus on the lower end of the above-noted temperature range for ultimate deployment of NGNP.)

Task 1 is the first of five tasks in the JCN 6177 project. The five tasks are titled:

- Task 1. Control and Protection Systems in VHTRs for Process Heat Applications
- Task 2. Highly Automated Control Room Design
- Task 3. Models for Control and Protection System Designs
- Task 4. Advanced Control and Protection System Design Methods
- Task 5. Develop Technical Guidance and Acceptance Criteria for Safety Related Protection and Control Systems Designs

The overall objective of this research is to review potential technologies likely to be employed for the control and protection system design for the VHTR for process heat applications including possibly hydrogen production. Modeling methods and plant models, including multimodular models, will be investigated. As well, this research examines such design aspects and issues as prediction of the state and effect of control systems actions, overall robustness of the control and protection systems designs, and fault detection capability. The culminating activity, to the extent possible based on the maturity of the VHTR design and particular process heat application, is to assist NRC in developing technical guidance and acceptance criteria for these safety-related protection and control systems designs for the VHTR.

1.2 Objectives

In Task 1, the objective is to review the (1) design of recent HTGR control and protection systems (e.g., HTTR, MHTGR, and PBMR) and (2) state-of-the-art technologies anticipated for use for the VHTR and process heat application design and identify the protection and control system designs likely to be used.

Specifically, this review will cover details of the potential control and protection system designs for pebble bed and prismatic gas-cooled reactors, the critical parameters in the VHTR that need to be controlled, the proposed protection and control systems to be used in these reactors, the methods and procedures to be used in the design of these protection and control systems, and the conditions to enable the protection systems.

Task 1 provides the background literature search for Tasks 2 through 5. One of the most useful products of this research is a collection of relevant documents and an annotated bibliography that will simplify information for this project and for the NRC analysts in the future.

2. DESCRIPTION OF THE BASIC SYSTEMS IN GAS-COOLED REACTORS

This chapter describes the basic systems in a gas-cooled reactor to provide a context for the control and protection systems that are described in the following chapter. The focus is on the inherent safety characteristics of the HTGR fuel and moderator design in the reactor that led to the important differences in dynamics and safety strategies with respect to light-water reactors. The variations in plant configuration for the various existing reactors and proposed NGNP designs as of this writing are discussed in the summary.

The existing HGTR reactors and the proposed VHTR designs discussed in the report are helium-cooled, graphite moderated design. The fissile material, typically uranium dioxide, is encapsulated in particles which are coated with high temperature ceramic layers. The ceramic coated fuel for the MHTGR is a foundational component upon which the safety and strengths of the reactor design are built. The fuel particle serves as the primary fission product containment under normal and accident conditions. By relying on the fuel itself as a proven fission product barrier and developing a design to ensure fuel integrity under all credible conditions, numerous design benefits extend to almost every aspect of the plant. The number and functions of safety systems and containment structure are reduced and simplified. Critical operator actions are eliminated or reduced. The time frame for required actions is lengthened from minutes to days. The beneficial characteristics of the fuel particles and graphite moderator are large negative Doppler coefficient, high core thermal mass, and safe operation without fuel damage or radiation release on exposure to worst case temperatures following reactor accidents such as a depressurized loss of flow event (equivalent to a large break loss of coolant event in a light water reactor). These unique design features result directly in a simpler plant to design, build, operate, and maintain than a conventional light-water reactor. Potential benefits of greater inherent safety and reduced threat of radioactive release to the public may extend to the regulatory environment as well. The inherent safety of the fuel leads to simpler I&C for the active protection systems.

Two main variations in HTGR design are the configuration of the fuel and moderator as either prismatic fuel or pebble fuel. The prismatic fuel consists of hexagonal blocks of graphite with fuel formed into rod-shaped compacts with graphite binder and contained in holes in the graphite blocks. The prismatic fuel was originally developed in the United States for the Peach Bottom and Fort St. Vrain reactors and has been adopted in the General Atomic's proposed concept for the NGNP. The pebble fuel design consists of spherical compacts of fuel particles surrounded by a graphite layer. The pebbles are slightly smaller than a billiard ball. The advantage of the pebble bed design is the ability to circulate the pebbles through the core region while in operation for online refueling whereas the prismatic fuel requires the unit to shutdown for refueling. The disadvantages of the pebble design are the variability of fuel packing and imprecise arrangement of the enrichment of pebbles in the core during operation to flatten the neutron flux distribution and reduce peak temperatures in the fuel. The pebble bed design was originally developed in Germany for the AVR and THTR reactors. The pebble design is proposed for the Westinghouse-PBMR concept for the NGNP. The following sections discuss the fuel and resulting core designs separately.

2.1 Prismatic Reactor Core Subsystem

For the prismatic fuel-moderator design, the reactor core subsystem consists of hexagonal, block-type graphite fuel and reflector elements, control rods and other reactivity control material, and startup sources contained in a steel pressure vessel. Fuel compacts are placed in holes drilled in the graphite blocks. Helium coolant passes downward through full-length flow channels. Control rods for operational power control and for emergency shutdown are located in channels in the reflector region of the core rather than the central fuel region to reduce operating temperatures of the metal cladding of the control rod. Additional control rods are provided in the central fuel region for cold shutdown. Near-central channels in the graphite are also provided for boron carbide neutron absorber pellets that are used by the reserve shutdown system as a backup to the main control rods. The arrangement of the reactor core subsystem components is shown in Fig. 1.

TRISO-coated fuel particles consist of a spherical refractory kernel of uranium dioxide or carbide (for MGHTR, for example, the fissile particles are 19.8% enriched uranium oxycarbide, and the fertile particles are natural or depleted uranium or thorium as shown in Fig. 2). The fuel coatings protect and provide structural integrity to the fuel particle and contain fission products. The particle size is about 800 microns. About 12,000 particles are bonded into a rod-shaped fuel compact about 13 mm in diameter and 50-mm long, which is inserted into drilled holes in the graphite fuel element as shown in Fig. 3. Helium coolant flows down through coolant holes in the fuel elements as shown in Fig. 4. For the MHTGR design, the fuel cycle is about 3.3 years. After the initial loading, half of the fuel in the core will be replaced every 1.65 years.

A design requirement for the fuel is to retain fission products within the fuel particles to limit their release to the primary coolant during normal operation and abnormal conditions. The typical core design limits for maximum fuel temperature are about 1600°C for off-normal conditions. Fuel tests¹ in Germany for similar fuel show no fuel failures for fuel particles at 1600°C for 500 hours. For severe accidents such as the depressurized loss of flow event (DLOF), models of the HTGR cores show that the large negative temperature coefficient and high thermal inertia of the moderator and fuel protect the fuel from exceeding the design limit. The fuel model shows that heat up occurs relatively slowly, and temperatures of about 1600°C exist for only about 20–30 hours following the accident; therefore, the data indicate that significant fission product release will not occur. The temperature coefficient of reactivity is very negative for the HTGR fuel because of the Doppler broadening of the resonance cross-sections of ²³⁸U in the fertile and fissile particles.

Peak fuel temperatures and fuel element stresses and coolant gas temperatures are controlled by a radial and axial variation of the fuel enrichment. The varying fuel enrichments maintain the maximum time-averaged fuel temperature at less than 1250°C. The MHTGR thermal parameters are typical design numbers for operating HTGRs. MHTGR core inlet helium temperature is about 250°C; average exit temperature is 687°C. The core inlet helium coolant pressure is about 925 psia. NGNP designs are slightly higher in operating temperature than MHTGR (current proposals for NGNP are for average core exit of 700 to 750°C). Safety conclusions regarding inherent safety are not expected to be affected by the higher temperature.

¹MHTGR Fuel Performance and Supporting Data Base, GA-A-19877, October 1989.

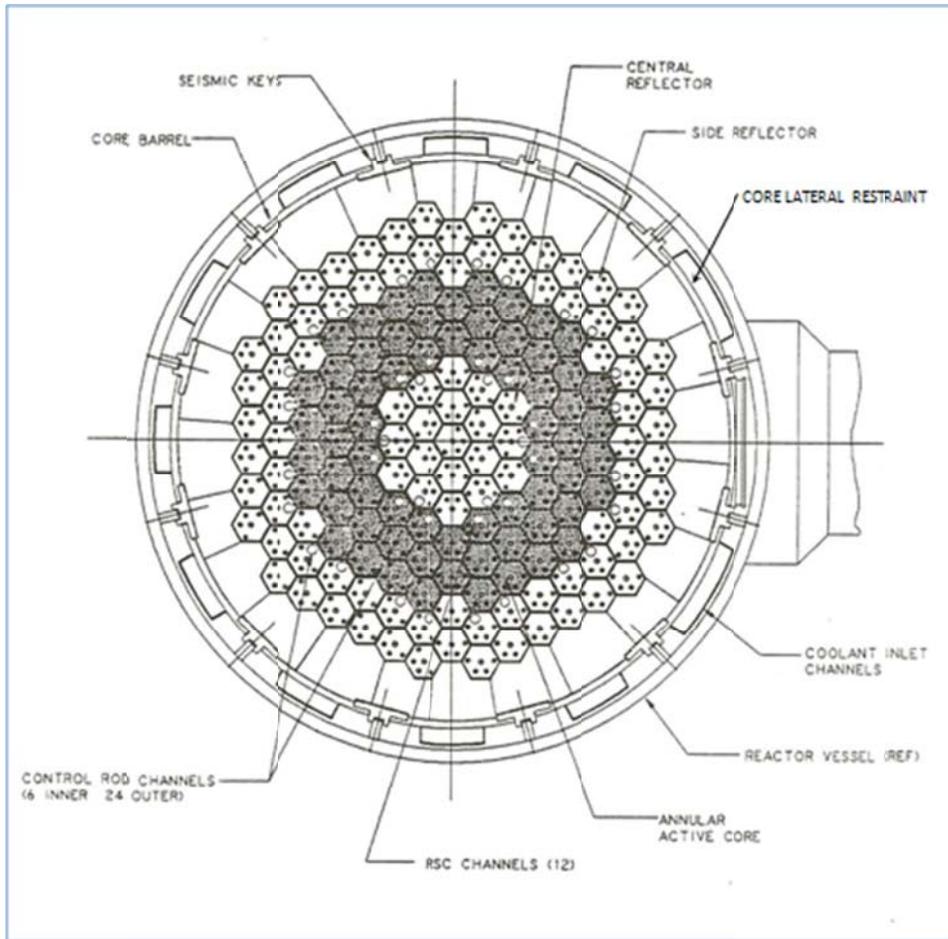


Fig. 1. Plan view MHTGR core.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

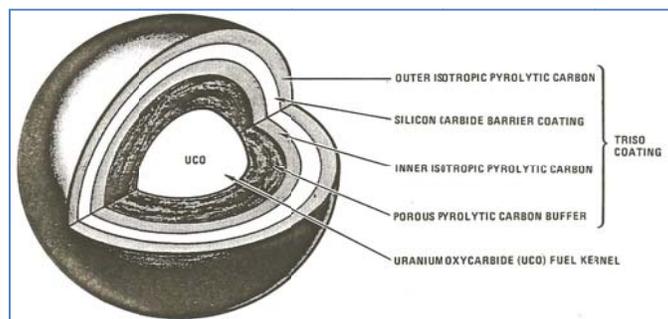


Fig. 2. TRISO fuel particle.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

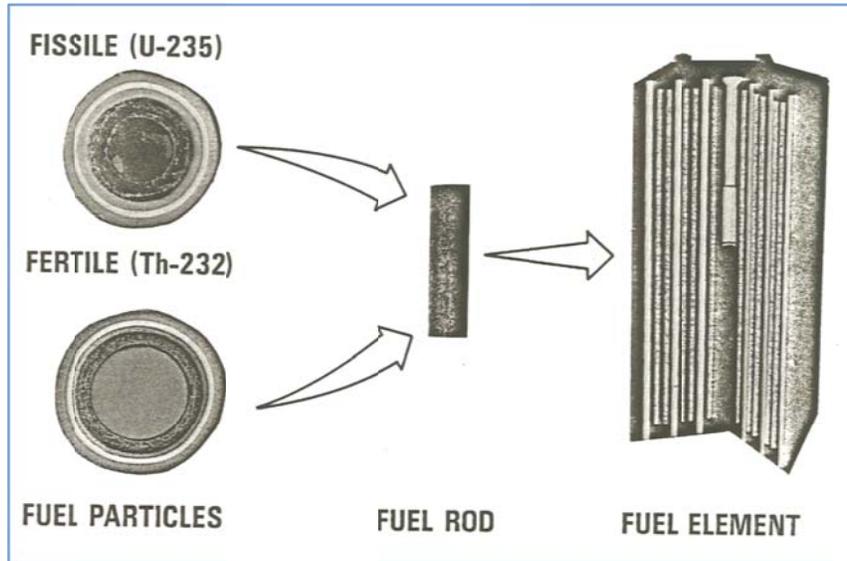


Fig. 3. Fuel components.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

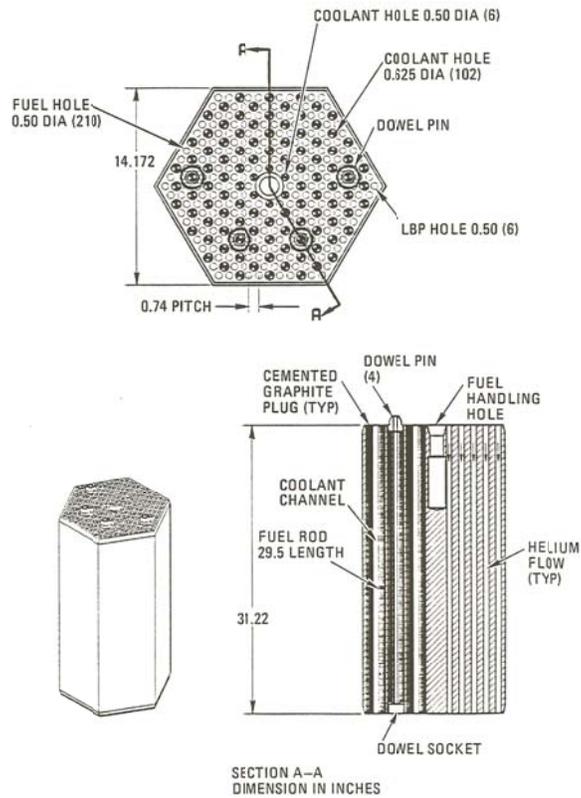


Fig. 4. Fuel element.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

Compared to light-water reactor fuel, the HTGR ceramic fuel and graphite moderator block possess better fission product retention, larger margin between the operating temperature and temperature for fuel failure, high-temperature process heat, higher efficiency electricity generation, simplified safety systems and operator requirements, and improved economics.

2.2 Pebble Bed Reactor Core

The pebble bed design uses the same TRISO fuel particles as prismatic fuel, but in the pebble design, the particles are formed into spherical elements, approximately the size of a billiard ball. The pebbles consist of a central fuel compact in which thousands of TRISO fuel particles are bonded into a carbon matrix. The fuel region is surrounded by a hard, pyrolytic graphite layer that provides a durable support structure for handling and circulating the fuel pebbles. The graphite also provides moderation of the neutrons. Figure 5 illustrates the pebble design in a view that telescopes from right to left. The fuel kernel on the right is contained within TRISO fuel particle which is contained with the graphite matrix of the fuel sphere.

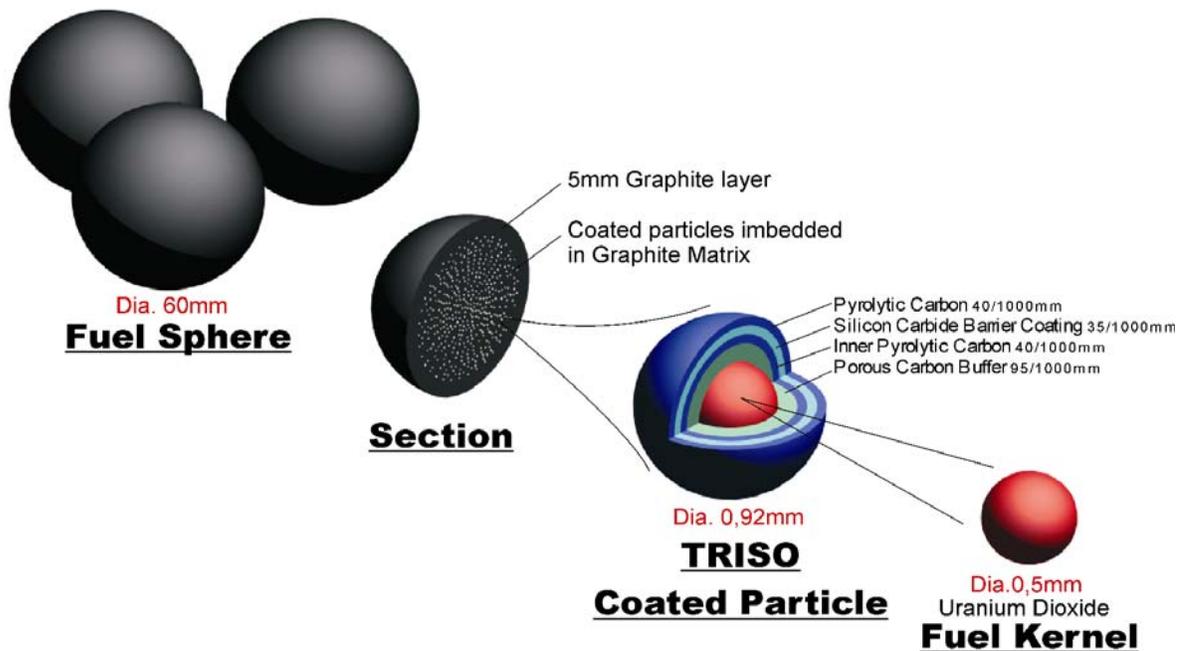


Fig. 5. Conceptual design of pebble fuel.

[Webpage, <http://www.pbmr.com/index.asp?Content=224>, *How the PBMR fuel works*, viewed 09/23/2010]

The pebble bed reactor vessel is a vertical steel pressure vessel which contains and supports a metallic core barrel, which in turn supports the cylindrical pebble fuel core. This cylindrical fuel core is surrounded on the sides by an outer graphite reflector and on top and bottom by graphite structures which provide similar upper and lower neutron reflection functions. Vertical bores in the side reflector are provided for inserting the reactivity control rods. Figure 6 shows the PBRM reactor vessel design. In this version of the core, both central and perimeter reflector blocks are included. The central blocks are used to reduce peak fuel temperatures because the pebble circulation does not allow a radial profile of

enrichment for shaping the neutron flux profile. Some concepts of the PBMR forgo the central reflector and simply reduce the average power density in the core.

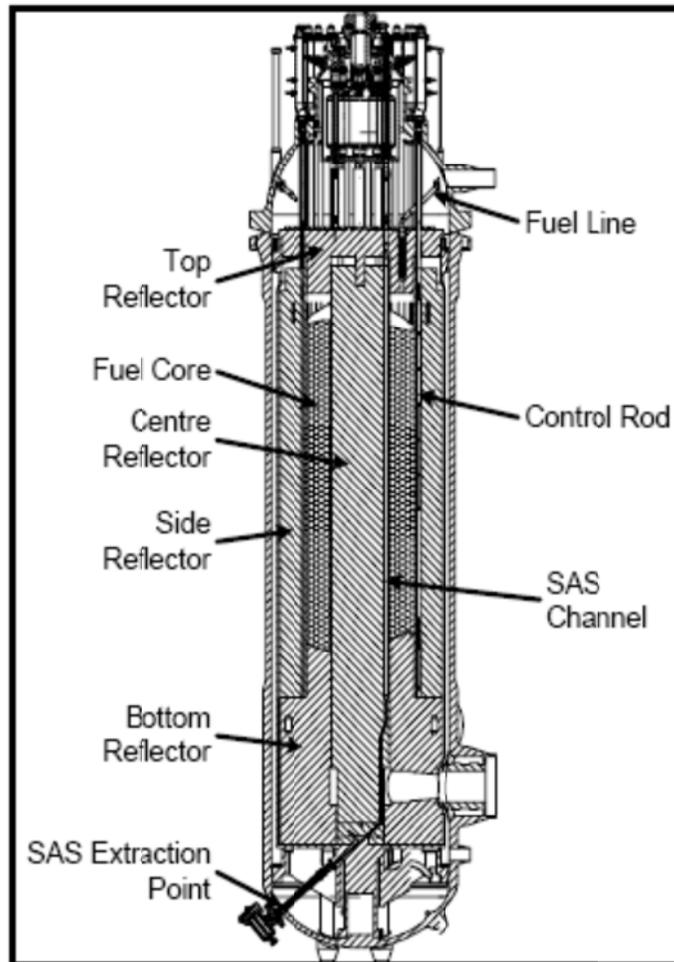


Fig. 6. Pebble bed modular reactor–reactor vessel.

[Johan Slabber, PBMR Reactor Unit and Main Support Systems, PBMR Safety and Design Familiarization (slide presentation), PBMR (Pty) Ltd., 2006]

In the pebble bed design, the pebbles continuously circulate downward through the core. Each pebble is re-circulated six to ten times over the course of its 3-year life cycle before being permanently discharged from the reactor. Pebbles are monitored upon each exit to measure composition and irradiation level and to determine if their life cycle is complete. Fresh fuel pebbles are added to replace those discharged.

2.3 Reactor Internals

The reactor internals consist of the core lateral restraint, permanent side reflector, graphite core support structure, metallic core support structure, upper plenum shroud, and the hot duct as shown in Fig. 7. (The core lateral restraint is shown in Fig. 1.) Most metallic structures will not be required to be high-temperature alloys. The core lateral restraint and the hot duct in the cross-duct will be a high-temperature alloy.

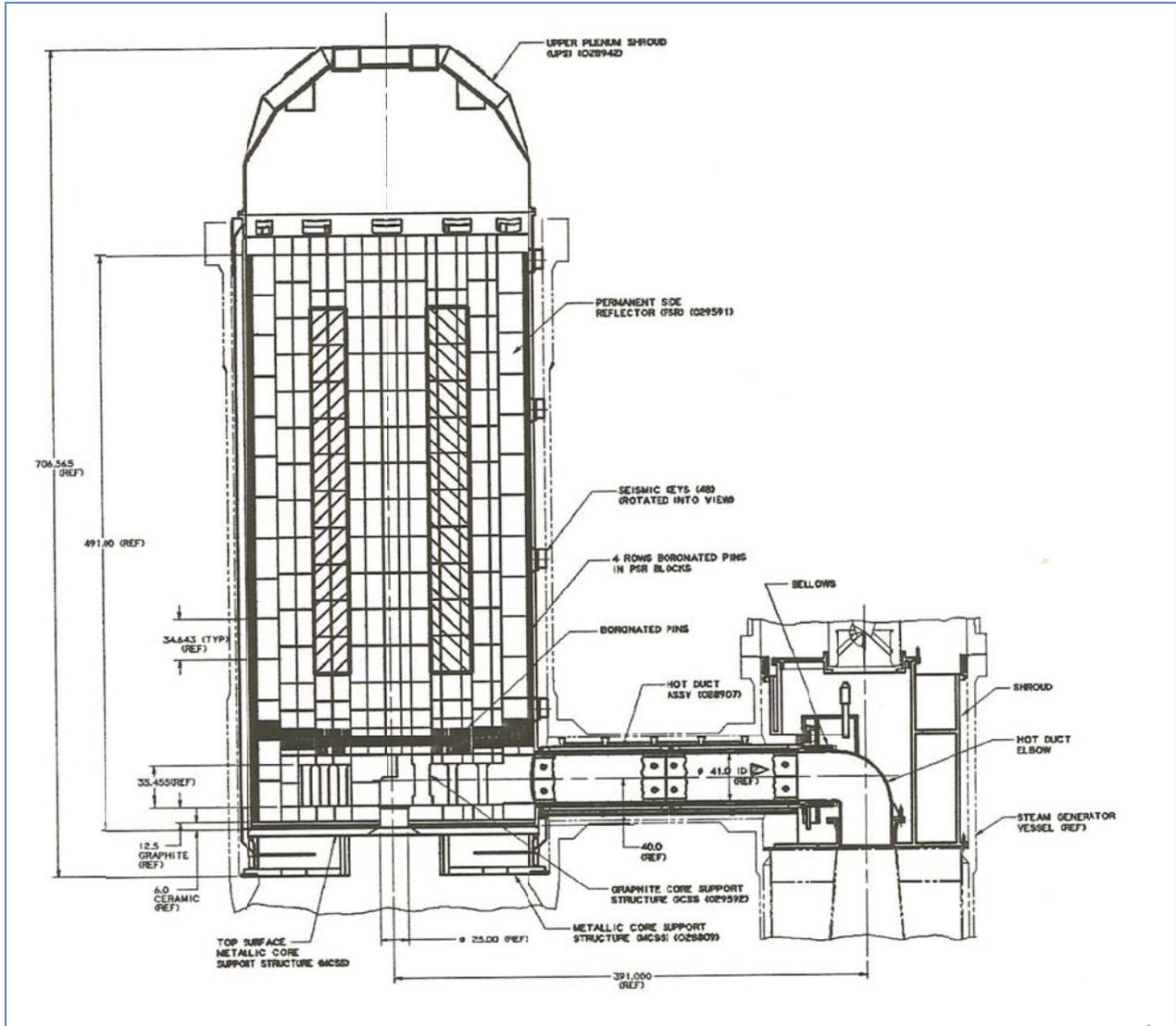


Fig. 7. Vessel internals.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

2.4 Main Heat Transport Systems

The main heat transport system consists of a forced convection helium coolant loop that removes heat from the core and conveys it to the heat load for the plant. The heat transport system consists of ducts, circulators, and heat exchangers. The walls of the main heat transport loop form the primary helium pressure boundary. Overpressure protection of the primary pressure boundary (reactor vessel, steam generator, and cross-duct) is provided by a system of pressure relief valves to meet ASME code requirements.

In all of the proposed reactor designs, the helium flow is forced circulation provided by circulators. The circulators are powered by electrical motors (except for direct Brayton cycle plants described later.) The flow is forced by the circulator into a bottom plenum region of the reactor vessel which distributes the flow around the outer annular region of the reactor vessel. The flow goes upward in the annulus between

the core barrel and the vessel wall. The helium flow is then directed downward through the core by the upper plenum region. The helium exits through lower plenum to the center pipe in the annular cross-duct.

2.4.1 Secondary steam cycle power generation

For plants such as the MHTGR and Fort St Vrain, the reactor heat is removed by a steam generator and converted to electrical energy in a conventional steam turbine. The MHTGR schematic in Fig. 8 shows the reactor vessel connected to the steam generator by a concentric annular cross-duct. The annular pipe design means that the interior hot pipe is within the pressure boundary. The pressure differential across the hot pipe is just the pressure drop across the steam generator, not the pressure difference to ambient pressure, which substantially reduces the strength and creep resistance required of the hot pipe. The inner pipe is compatible with the high-temperature environment and is insulated from the cooler outer pipe which returns helium to the reactor.

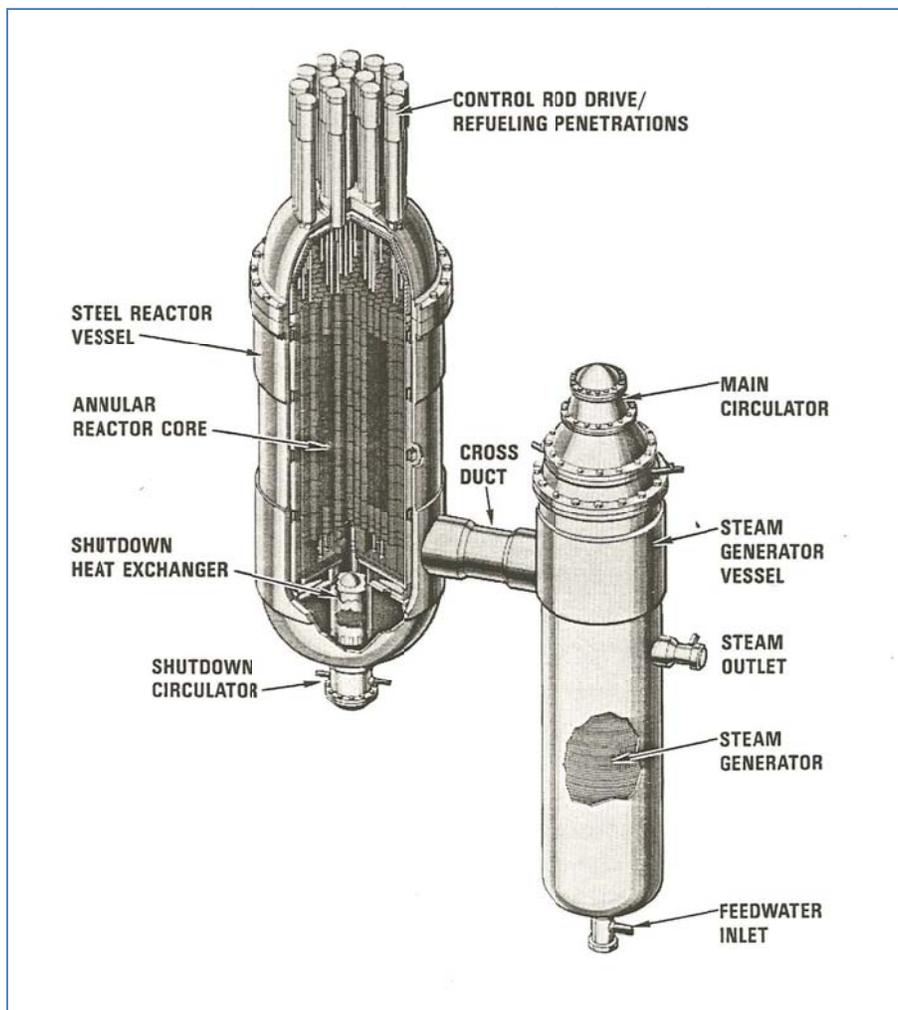


Fig. 8. Reactor and steam generator for MHTGR.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

The steam from the steam generator drives a steam turbine in much the same arrangement as a conventional nuclear power plant. A simplified flow diagram for normal plant operation and power generation is shown in Fig. 9. This figure also illustrates the transition from the reactor module/nuclear island part of the plant to the energy conversion part.

The steam generator in these designs is a vertically oriented, once-through shell and tube heat exchanger using a multitube helically wound tube bundle. Feedwater enters the tube side from the bottom; superheated steam exits in the upper side wall. The helium flows downward on the shell side nearly perpendicular to the tubes for very effective energy transfer. A typical steam generator tube is show in Fig. 10.

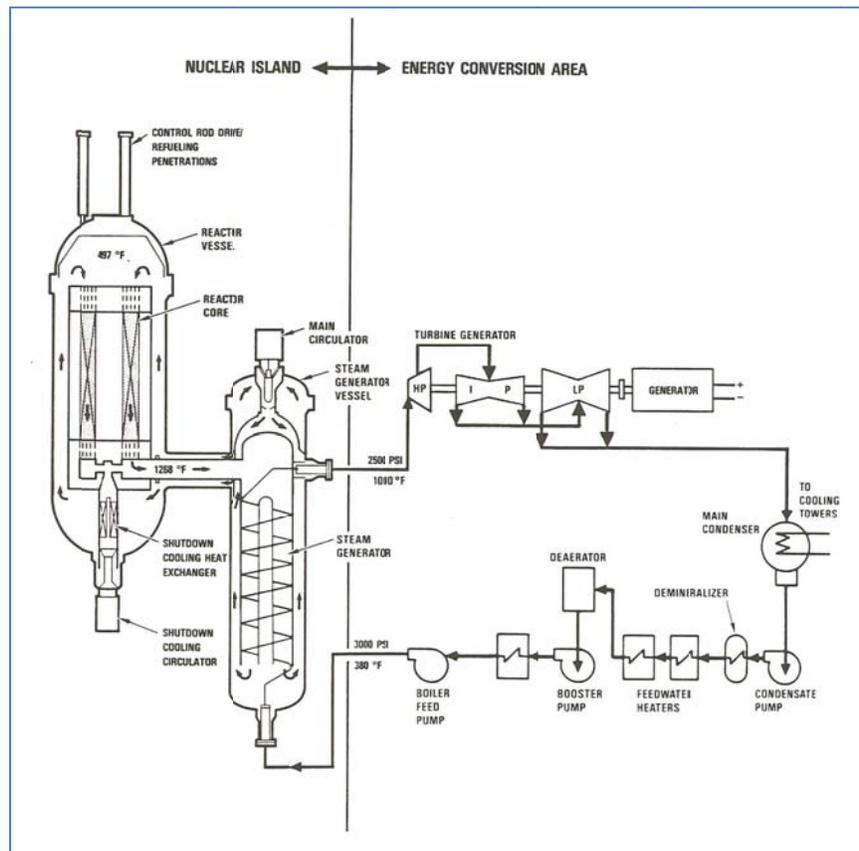


Fig. 9. Simplified power generation flow diagram.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

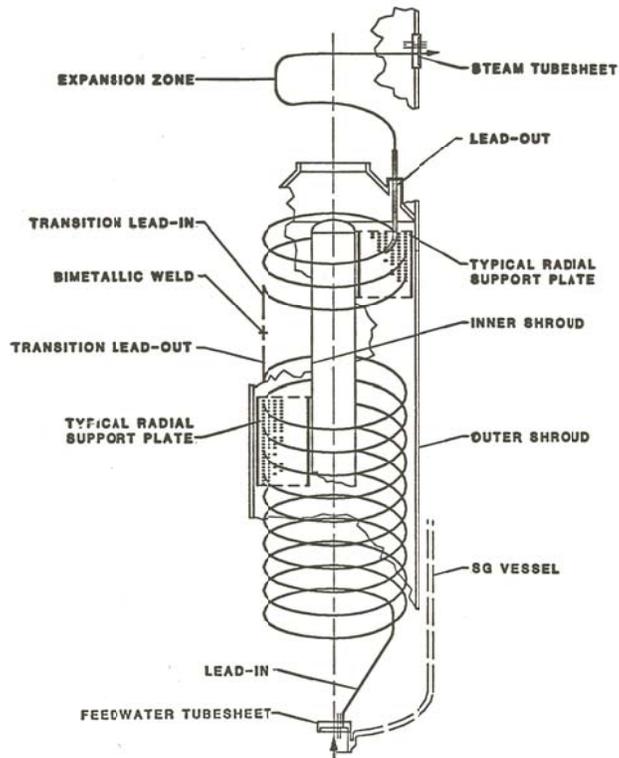


Fig. 10. Typical steam generator tube.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

The steam generator vessel contains the main coolant circulator mounted at the top and a vertical helical coil heat exchanger below. Figure 11 illustrates the configuration of the electrically powered circulator in the upper plenum of the steam generator.

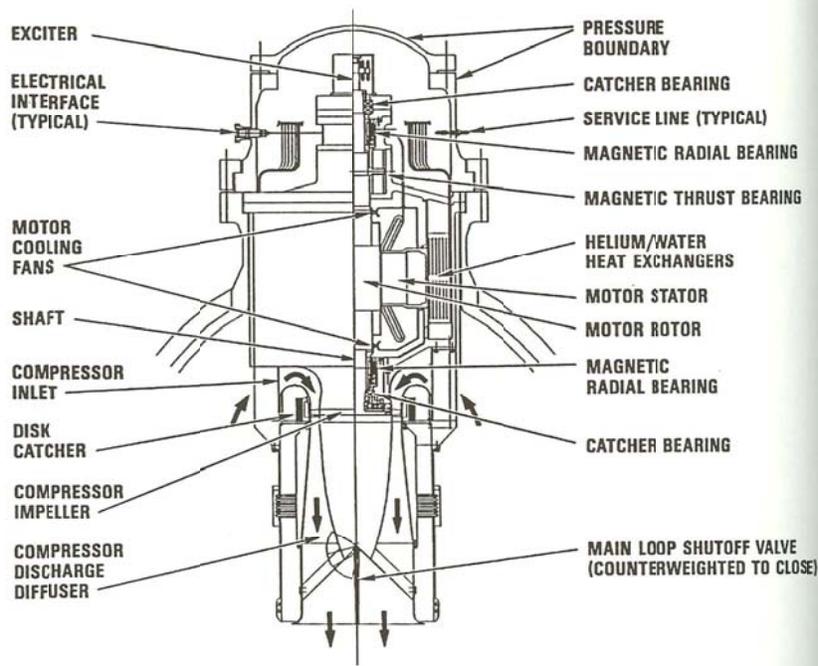


Fig. 11. Main circulator design for MHTGR.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

Several support systems are part of the turbine generator system. These include the feedwater and condensate system, main steam and turbine bypass system, startup and shutdown system, steam and water dump system, turbine plant cooling water system, heat rejection system, and other turbine plant systems.

2.4.2 Direct cycle, gas turbine energy conversion

For some plant concepts such as the Gas Turbine-Modular Helium Reactor, a direct Brayton cycle generates electricity using gas turbine and compressor with the primary helium as the working fluid. The gas turbine designs have the potential for higher electrical conversion efficiency because of the thermodynamic advantage of higher temperature of operation. Figure 12 illustrates the main components and flow of the gas turbine cycle.

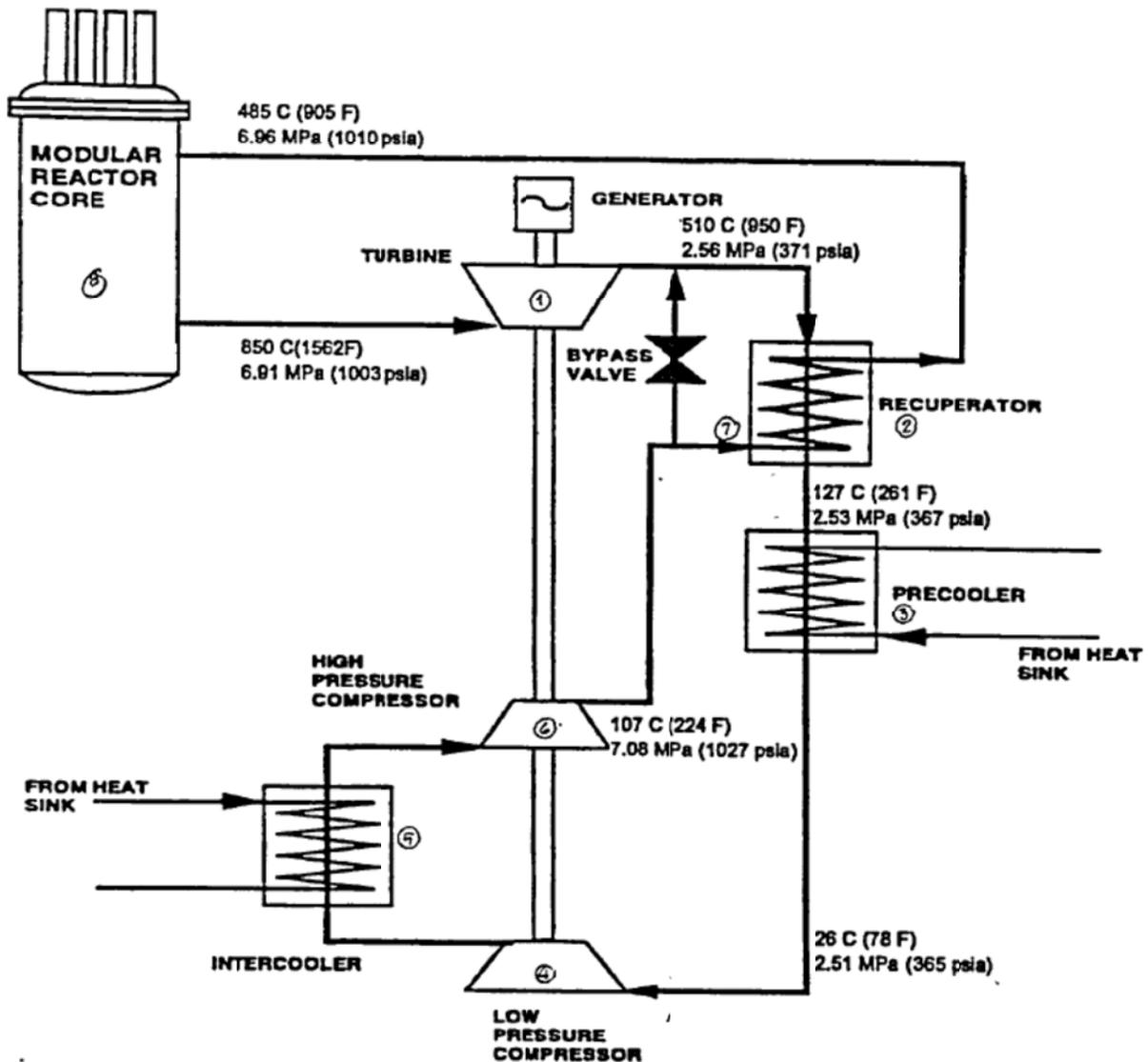


Fig. 12. Simplified process flow diagram for GT-MHR.

[C. Rodriguez, Jazgliczynski, and D. Pfremmer, *GT-MHR Operations and Control*, GA-A21894, IAEA Technical Committee Meeting on "Development Status of Modular High Temperature Reactors and Their Future Role," ECN, Petten, The Netherlands. November 28-30, 1994.]

Some NGNP configurations have proposed a co-generation plant with a Brayton cycle on top of a steam cycle. In the co-generation process diagram, a steam generator is used in place of the precooler in Fig. 12. The steam then drives a steam turbine system that is similar to Fig. 9.

2.4.3 Process heat systems

In general, the process heat applications are connected to the primary coolant loop via an intermediate heat exchanger. The intermediate loop coolant may be helium or another inert gas, molten salt, or steam. The design limitations of pumping losses and necessary distances separating the process heat plant from the reactor favor molten salt as the intermediate coolant. For combined electrical and process heat designs, the intermediate heat exchanger loop is in parallel with the electrical generation plant. Figure 13 illustrates a concept with electrical power production in parallel with hydrogen production by both high-temperature electrolysis and thermochemical production.

The NGNP designs envision the heat transport loop connected to a process heat plant for hydrogen production or other high temperature industrial process. The process heat plant may be the sole heat load or may be paired with an electrical generation process, either through a direct Brayton cycle or indirectly through a secondary steam cycle. A number of combinations of Brayton cycle, steam cycle, and process heat systems have been proposed to receive the heat produced by the reactor.

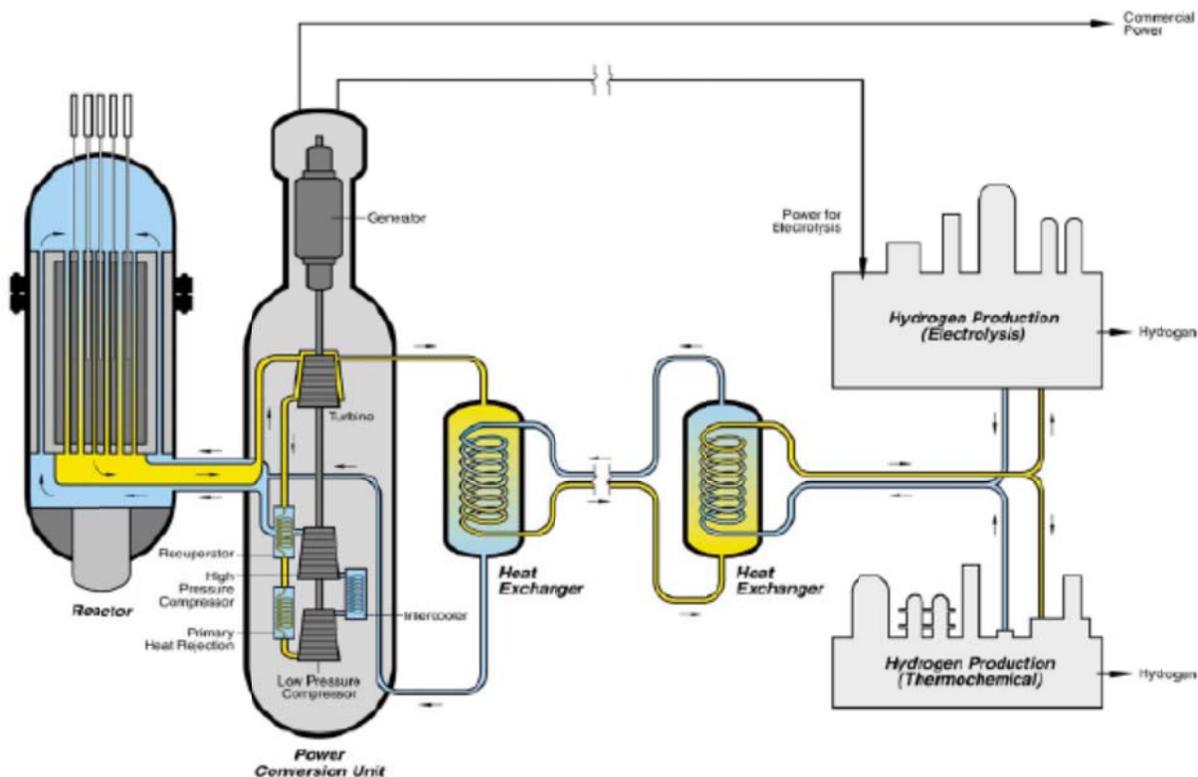


Fig. 13. Conceptual process flow for combined gas turbine and process heat plants (General Atomics).

[D. S. Vandel and S. Bader, *NGNP Engineering White Paper: By Products Trade Study*, INL/EXT-07-12728, April 2007.]

2.5 Reactor Service Systems

Several service systems are also necessary to maintain plant operation. These include the helium purification system, radioactive waste processing system, reactor plant cooling water system, fuel

handling, storage and shipping systems, and other miscellaneous service systems. The service systems are reviewed for potential initiating events that affect the reactor safety.

The helium purification system consists of filters, absorbers, oxidizers, coolers, heaters, compressors, and piping, valves, and I&C components that are used to purify the helium coolant. The system removes fission products and chemical impurities.

The radioactive waste processing system has systems for gaseous, liquid, and solid waste management. The gas waste management system filters, monitors, releases if appropriate, holds up, and compresses gaseous wastes. The liquid waste system collects and treats liquid wastes for the plant. The solid waste system dries, compacts, and solidifies waste.

A reactor plant cooling water subsystem provides cooling water for nonsafety-related heat loads in the plant, such as the helium purification system, main circulator motor, neutron control assemblies, and other equipment. This is a closed system to protect against release of radioactive materials to the environment.

The fuel handling, storage, and shipping system provides for core refueling, site fuel handling, and spent fuel cooling.

Other miscellaneous systems include reactor service equipment and storage wells; helium storage and transfer; liquid nitrogen; heating, ventilation, and cooling to reactor, auxiliary, service, and personnel services buildings; decontamination, and equipment and floor drain systems.

2.6 Safety Systems

The safety system performs three functions; shutdown the reactor, remove decay heat and confine radioactive releases.

Reactivity control

Control and safety rods are fabricated from natural boron in annular graphite compacts. Metal cladding is provided for structural support. The outer control rods located in the reflector are used to power control and to shut down from high power. The prismatic cores also have safety rods which are inserted in bores in the fuel block for cold shutdown.

The reserve shutdown system provides a second independent shutdown mechanism if needed. The reserve shutdown system operates by releasing boronated graphite pellets stored in hoppers above the core into channels bored in the graphite moderator in the central fuel region of the core.

2.7 Engineered Safety Features

The engineered safety features provide cooling to the core when the normal heat removal systems are unavailable.

2.7.1 Shutdown cooling system

The shutdown cooling system (SCS) normally provides temperature control and decay heat removal when the reactor is shutdown. The system consists of a gas-to-water counter-flow heat exchanger located in the lower plenum region of the reactor vessel to remove heat from the helium coolant and a water-to-air heat exchanger to dump the heat to the atmosphere. The forced circulation of the shutdown loop is provided by an electrically driven pump. The helium in the reactor vessel is circulated by the SCS circulator. The main components of the shutdown cooling system are shown in Fig. 14.

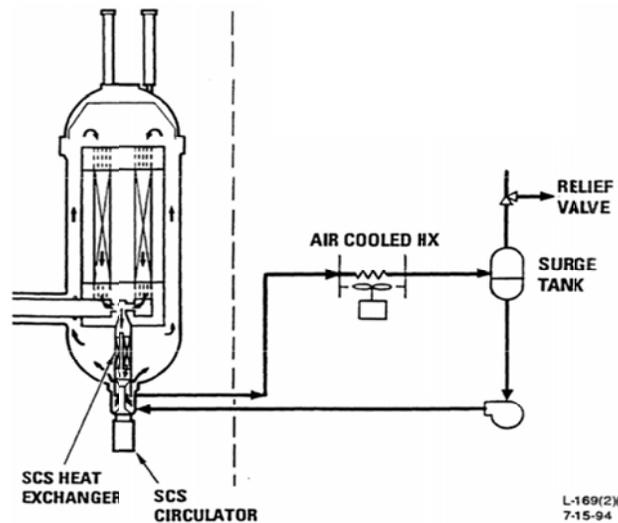


Fig. 14. Example shutdown cooling system (SCS) in a prismatic core modular HTGR.

2.7.2 Vessel cooling system

During normal shutdown, decay heat is removed using the main heat transport system (main circulator and steam generator) or the shutdown cooling system. If these are not available, the RCCS functions passively to remove decay heat.

The safety-related reactor cavity cooling system (RCCS) removes heat continuously and passively from the reactor vessel walls. The vessel wall is uninsulated and transfers heat to the reactor cavity via natural convection and thermal radiation. The reactor cavity transfers heat to cooling panels and then to the environs through natural convection of air as illustrated in Fig. 15. The cooling panels separate the outside air from the air in the reactor cavity to minimize release of air activated in the reactor cavity. They also serve to protect the cavity walls from overheating during normal operation.

The RCCS is a completely passive system with the capacity to remove all decay heat from the core, whether the core remains pressurized or not. Redundant inlet/outlet flow paths ensure adequate air flow to the heat panels. Heat rejection can also be accomplished to the ground surrounding the underground concrete reactor building. The RCCS has no valves or active components. In comparison to conventional light-water reactor emergency cooling system, the RCCS is a particularly noteworthy system because the safety system is always “on.” It does not have to detect a loss of cooling and initiate the emergency cooling function. There is just one alignment and one operating mode. Air flow through the system and heat rejection is simply a function of the reactor vessel temperature and the outside air temperature. The heat transport design of the cavity ensures that the system can remove the maximum decay heat from the reactor vessel without the vessel, internal structure or core exceeding thermal limits. The RCCS is the ultimate heat sink in the reactor designs credited in plant safety analysis. A passive system is only possible because of the capability of the fuel particles to withstand very high temperature without damage or radiation release in excess of allowable limits.

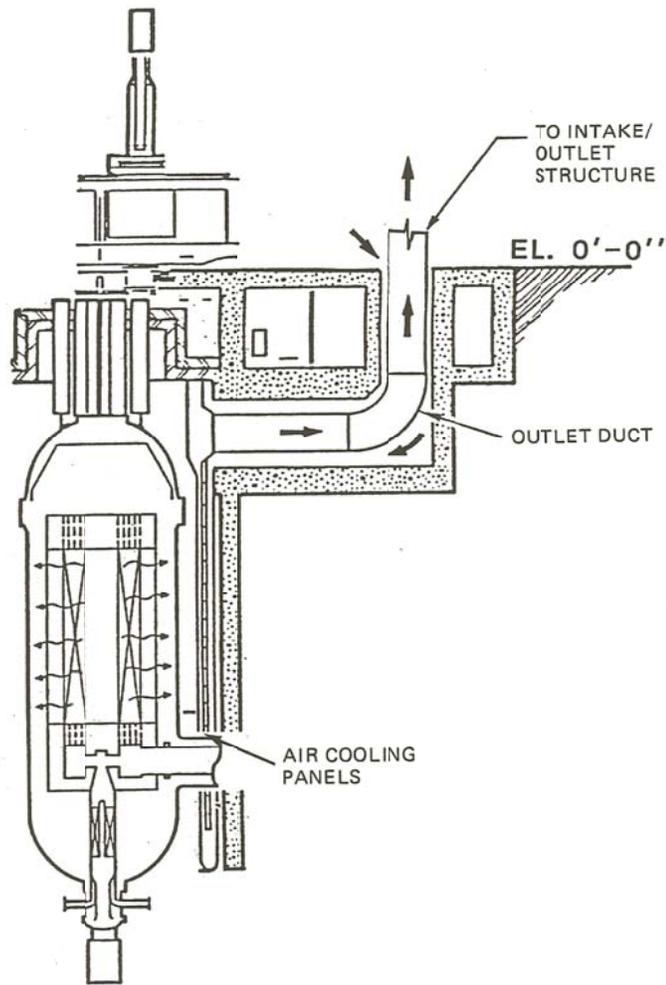


Fig. 15. Passive decay heat removal in the RCCS.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

Some proposed RCCS designs for NGNP use a natural circulation water loop rather than an air loop. The concept for RCCS for the AREVA NGNP is illustrated in the Fig. 16. The cavity cooling may occur by either boiling the water and release of steam through the steam relief valve or by the heat removal using the separate forced convection loop as shown in the figure.

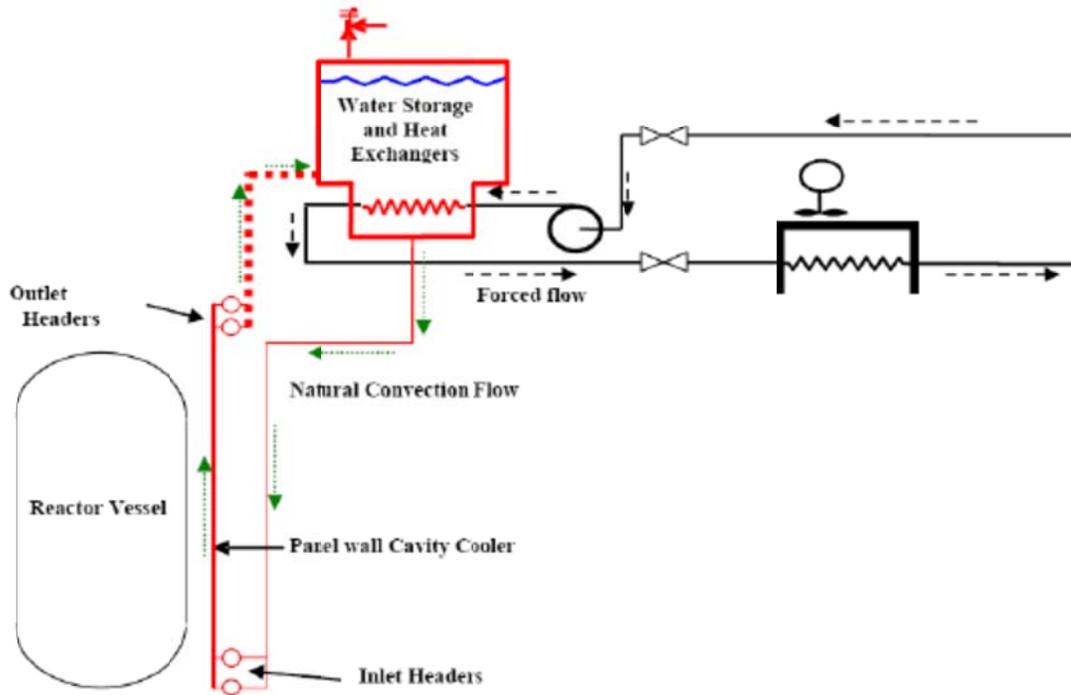


Fig. 16. Representative water cooled RCCS flow diagram (AREVA NGNP).

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

2.7.3 Containment/confinement structure

Historically, most HTGRs have a containment vessel that is designed to retain helium released from the reactor in the event of a primary loss of pressure accident. The containment structure consists of a reactor containment vessel (CV), service area (SA), and an emergency air purification system, which reduce the release of fission products to the environment during postulated accidents. The MHGTR and proposals for the NGNP have included a confinement rather than containment concept. The strategy was originally presented by Dilling for the MHTGR² and also proposed for the PBMR design.³ The confinement structure is designed to retain released gas from the reactor briefly to cool and filter it. Because of the design and reliability of the fuel particles, the gas is not highly contaminated and can then be released to atmosphere. The argument for release is that the containment vessel pressurized with the helium is more hazardous than the release of the gas to atmosphere.

3. GENERAL DESCRIPTION OF INSTRUMENTATION AND CONTROL SYSTEMS OF HTGRs

This chapter presents a general description of safety and control strategies and licensing issues for existing HTGR and proposed NGNP designs. The goal is to provide a general overview of issues that are

²D. Dilling, T. D. Dunn, and F. A. Silady, *A Vented Low Pressure Containment Strategy for the Modular High Temperature Gas-Cooled Reactor (MHTGR)*, General Atomics Project 7600, GA-A21622, April 1994.

³A. Koster and D. Lee, "The PBMR Containment System," 2nd International Topical Meeting on High Temperature Reactor Technology, Beijing, China, September 22–24, 2004.

common to all the HTGRs. The purpose of this study is to provide information to the NRC on the likely configurations of control and protection that may be applied and to work toward revised technical guidance for the applicants of NGNP designs and revised acceptance criteria for the review of control and protection systems such designs.

Task 1 is primarily a literature survey to gather information about the reactor designs and distill and collect their I&C features in a single document for background for the subsequent tasks in the project. The major components of the reactor, heat transport, and power conversion systems for HGTR reactors are described in Chapter 2. The general description of control and safety systems is described in this chapter. Chapters 4 and 5 discuss specific plant control system designs for existing HTGRs and proposed NGNP designs respectively.

3.1 Description of Basic Safety and Control Strategies in Gas-Cooled Reactors

The instrumentation and controls of an NGNP plant will constitute a major departure from conventional light water plants (LWRs) because of the inherent safety features of HTGRs. An NGNP plant will also include evolutionary changes in I&C because of the continuous advancement of digital control systems. The concept of passive safety relies to the inherent characteristics of the design and material. The impact of passive safety on I&C systems is the main subject of this chapter. Issues associated with the general advancement of control hardware and applications include increased automation of operations previously performed manually, increased communications and sharing of information between control and safety functions, and potential for software common mode errors in digital systems. The NGNP will have the advanced digital control issues in common with other advanced reactor designs such the Westinghouse AP1000, the Mitsubishi APWR, AREVA EPR, and the GE/Hitachi ESBWR. The issues of digital safety are covered in other studies and reports and are only important to the HTGR and NGNP system insofar as they present a different challenge for the NGNP than other advanced reactors.

3.2 Protection Systems

3.2.1 Regulatory basis for protection systems of HTGRs

The top level regulatory requirements for instrumentation and controls systems for a light-water reactor are stated in the General Design Criteria (GDC) in Appendix A of 10 CFR 50. The GDC are applicable to light-water reactors of the type previously licensed by the NRC but are considered generally applicable to other types of reactors like HTGRs. The GDC governing instrumentation and controls are primarily 13 and 20 through 29. These GDC state the main underlying principles for instrumentation and control systems for providing a high degree of assurance that the plant will operate as designed and public health and safety will be protected. The GDC capture, at a high level, the design philosophy of safety and protection. The requirements for protection against single failures inhibiting execution of the safety function, diversity and defense in depth, high reliability and testability, and separation of control and protection functions are specified in the GDC. This philosophy is considered the foundation of safety and is not expected to change substantially with the inherent safety features of the NGNP designs. The application of the GDC to HTGR safety structures and components (SSCs) must be adapted. The following discussion reviews the main GDC that are applicable to HTGRs and differences that may need to be addressed by the NGNP safety systems.

GDC 13 requires that instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Controls must be provided to maintain systems within their prescribed ranges. In satisfying this requirement, NGNP protection systems must show that instrumentation systems are provided to monitor the plant even when the safety of the plant is assured by inherent properties without active controls. The instrumentation and its survivability may be an issue for high temperature, post-accident

operation. The instrumentation topic is discussed in the companion research program N6668, Advanced Reactor Instrumentation.

GDC 20 requires sense and command functions to protect the fuel under abnormal operational occurrences. “The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.”

HTGR safety system design is derived from this top level requirement. That is, the safety system design is based on protecting the fuel from exceeding design limits for a variety of events. As a result, the protection system monitors variables such as flux, flow, temperature, and initiates various trip functions such as scramming the reactor, shutting down helium circulators, and isolating steam generators or heat exchangers when abnormal conditions are detected. However, the reliance on active sense and command functions is considerably lower for the HTGR design because of the inherent safety features of the reactor design. The inherent safety in HTGRs means that the fuel design limits are not exceeded mainly as a direct, physical consequence of the design and materials of the plant rather than the result of active detection and response systems. The design and materials properties which contribute to the inherent safety include a small operational excess reactivity, large thermal mass of moderator and fuel for slow heatup rates, a large negative temperature coefficient, inert gas coolant, the ceramic fuel particle coatings which can withstand high temperature without releasing fission products, and a passive heat removal capability that is sufficient for decay heat cooling. As a result, some of the most severe accidents for LWRs, such as a loss of coolant without scram, do not have adverse consequences for the HTGR even if the automatic protection functions for reactor scram and any emergency cooling system fail to activate.

GDC 21 requires that protection systems shall be designed for “high functional reliability and inservice testability commensurate with the safety functions to be performed.” GDC 21 also stipulates the single failure criterion and a design that is capable for test for failures and losses of redundancy.

The application of GDC 21 on I&C systems of HTGRs is not expected to be any different than conventional LWR protection systems.

GDC 22 stipulates the independence principle. Protection systems “shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.” The application of GDC 22 results in design techniques known commonly as diversity and defense in depth.

The application of GDC 22 on the I&C systems of HTGRs is not expected to be any different than for conventional LWR protection systems.

GDC 23 requires that protection system failure modes terminate in a “into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.”

The HTGR design utilizes the inherent safety attributes of the core and fuel so that the core is protected from radiation release against a range of events, even beyond design basis event such as loss of forced circulation without scram, for both pressurized and nonpressurized primary systems. The range of events that result in no adverse consequences to the public is considerably broader for HTGRs. The argument may be made that HTGRs terminate into a safe state inherently.

The impact of inherent safety on NRC regulation and guidance for reliance on a termination in a known safety state. One would have to expect that the confidence to rely on the inherent safety to satisfy GDC 23 will grow with testing and operating experience.

GDC 24 requires separation of protection and control systems. “The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.”

In advanced digital systems in nuclear power plants, the trend to interconnect the protection and control systems is increasing with the increasing capabilities of the digital control and protection systems. The bright line separating analog protection and controls in the past may fade over time. However, the issue of separation of control and safety is the same for all advanced reactors and has no special concern from the design of control and protection for HTGR. Neither NGNPs nor surveyed HGTRs have proposed any unique interconnection of control and protection systems.

GDC 25 specifies requirements for reactivity control malfunctions. “The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.” A large negative temperature coefficient of reactivity coupled with a large temperature margin between the operating fuel temperature and limiting temperature for TRISO coating failure means that a significant reactivity insertion from rod withdrawal or other mechanism is typically compensated by the inherent properties of the design. In some instances (e.g., AVR), rod insertion limits are necessary to ensure that an uncontrolled rod withdrawal can be handled inherently.

GDC 26 specifies a requirement for reactivity control system redundancy and capability. “Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.”

The primary scram mechanism for HTGRs is a control rod system. The secondary mechanism is usually a boron impregnated sphere system. One of the potential concerns for the combination of rods and spheres for reactivity controls in HTGR is the experience at the Fort St. Vrain plant in which a common failure mechanism, moisture in the coolant, caused failure of both reactivity control systems. Low levels of moisture in the coolant over time resulted in corrosion of the drive mechanism for the rods. An operational event occurred in which six rods failed to drop by gravity in a scram. (Operators were ultimately able to insert the rods by using the control rod drive motors to overcome the friction from corrosion.) Moisture in the coolant also caused leaching of boron from the spheres such that boric acid crystals formed on the surface and the balls became stuck together. A test of the backup system (a separate event from the rod drop failure) revealed that about half the balls in the hopper under test failed to fall into the core upon demand.⁴

Review of such backup shutdown mechanisms in the NGNP should address the design features that preclude similar common mode failures. Additional studies and requirements on moisture monitoring and control in new HTGRs may be justified. The concern should be for all types of NGNP plants, not just plants with steam generators in the primary loop. Studies (Copinger and Moses, NUREG/CR-6839) have shown that the largest source of moisture in the coolant is moisture from the atmosphere that adsorbs into the graphite moderator when the reactor vessel is open during shutdown.

⁴D. A. Copinger and D. L. Moses, *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, NUREG/CR-6839 (ORNL TM-2003/223), September 2003.

GDC 27 specifies that the combined reactivity control systems may be used to address the ability to maintain shutdown margin in the presence of a stuck rod and other postulated accident conditions. “The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with appropriate margin for stuck rods the capability to cool the core is maintained.”

The combined rod and ball system addresses the combined reactivity concern. The poison addition by the emergency core cooling systems refers to the liquid boric acid injection system in LWRs. This part of the criterion does not apply to HGTRs.

GDC 28 specifies limits on reactivity and reactivity insertion rate. “The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to assure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structures or other reactor pressure vessel internals to impair significantly the capability to cool the core. These postulated reactivity accidents shall include consideration of rod ejection (unless prevented by positive means), rod dropout, steam line rupture, changes in reactor coolant temperature and pressure, and cold water addition.

In general, the reactivity and insertion rate limits on HTGR protection system are similar to LWRs. The HTGRs have scrams on neutron power during power operation. In startup mode, a lower range neutron detector is used, trip levels are reduced and rate trips are added. When neutron power increases to detectable levels for power range detectors, the startup range instrumentation is put into bypass mode. This approach is basically the same approach as LWRs. The application of GDC 28 to HTGRs is expected to be similar to LWRs.

GDC 29 requires the protection and controls systems be protected against anticipated operational occurrences. “The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.” The application of GDC 29 to I&C systems of HTGRs is not expected to be any different than conventional LWR protection systems.

3.2.2 Proposed applicability of NRC’s or advanced reactor characteristics to HTGRs

The following table (Table 1) from Exelon Generation Company’s, “Proposed Licensing Approach for the Pebble Bed Modular Reactor in the United States,” provides an applicant’s interpretation of how the PBMR design complies with the NRC definition of advanced reactor characteristics. The same report evaluates the 10 CFR 50 section by section for applicability, rating each section and document as “applies,” “partially applies,” or “does not apply.”⁵

⁵Exelon Generation Company, “Proposed Licensing Approach for the Pebble Bed Modular Reactor in the United States,” March 15, 2002.

Table 1. PBMR's analysis of advanced reactor characteristics⁵

NRC's Definition of Advanced Reactor Characteristics	Corresponding PBMR Preliminary Design Features
Highly reliable and less complex shutdown and decay heat removal systems; The use of inherent or passive means to accomplish this objective....(negative temperature coefficient, natural circulation)	<ul style="list-style-type: none"> • Low excess reactivity and negative temperature coefficient provide passive shutdown capability • Two diverse active systems provided to insert negative reactivity to assure long term sub-criticality • Redundant, diverse and independent active forced cooling systems to remove core decay heat • Conduction/radiation cool-down capability without forced or natural convection of the primary coolant • No requirement for maintaining an inventory of primary coolant inside the reactor vessel.
Longer time constants and sufficient instrumentation to allow for more diagnosis and management prior to reaching safety systems challenge and/or exposure of vital equipment to adverse conditions.	<ul style="list-style-type: none"> • Low power density and large heat capacity of core fuel and graphite provides long time constants for power/temperature transients over full range of accident conditions • Low stored energy and single phase of primary coolant prevents rapid thermal and mechanical energy transfer to primary boundary and to containment structures; eliminates fuel coolant interactions that could challenge barrier integrity. • Capability to monitor circulating primary system radioactivity to confirm integrity of the fuel is within design limits
Simplified safety systems which, where possible, reduce required operator actions, equipment subjected to severe environmental conditions, and components needed for maintaining safe shutdown conditions.	<ul style="list-style-type: none"> • Capability to limit consequences of event sequences independent of any prompt operator actions; and reliant on passive safety features. • Safety systems are few, simple, and have few components needed to operate
Designs that minimize the potential for severe accidents and their consequences by providing sufficient inherent safety, reliability, redundancy, diversity and independence in safety systems	<ul style="list-style-type: none"> • The inherent capabilities of the fuel particles to retain their structural integrity over the range of normal and event sequence conditions with margins limit the source terms to very small levels; operation of active systems not required to support this capability • Long time constants of any releases and absence of any adverse physical and chemical processes • Any sequence with the primary system boundary intact results in no release of radioactivity • Design features that limit the potential for air or water ingress.
Designs that provide reliable equipment in the balance of plant, (or safety system independence from balance of plant) to reduce the number of challenges to safety systems	<ul style="list-style-type: none"> • The entire plant is very simple with a small number of components and support systems;

Table 1. PBMR’s analysis of advanced reactor characteristics (continued)

NRC’s Definition of Advanced Reactor Characteristics	Corresponding PBMR Preliminary Design Features
Designs that provide easily maintainable equipment and components	<ul style="list-style-type: none"> • Fuel elements are continuously monitored via on-line refueling and monitoring of circulating activity; broken and spent fuel elements replaced • Power conversion equipment (turbo-generator, turbo-units, etc.) can be maintained without compromising ability to support key safety functions
Designs that reduce the potential radiation exposures to plant personnel	<ul style="list-style-type: none"> • Performance of the fuel greatly reduces level of circulating primary coolant activity • Inert helium provides no impurities for activation products
Designs that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release and by reducing potential for consequences of severe accidents	<ul style="list-style-type: none"> • Fuel particles, fuel spheres, primary pressure boundary, citadel structure, containment envelope serve as concentric, independent barriers (See more detailed discussion in Section 6.2.1) • Design features provide accident prevention and mitigation (See more detailed discussion in Section 6.2.2)
Design features that can be proven by citation of existing technology or which can be satisfactorily established by commitment to suitable technology development program	<ul style="list-style-type: none"> • Innovation of earlier designs: extensive experience with gas cooled reactors, HTGRs, and significant experience with pebble bed reactors to provide confidence in performance of fuel and major components. • New and unique PBMR features important for power production but not needed to support key safety functions • experimental evidence to support confidence in the integrity of the fuel under normal and adverse conditions • Formula for proven fuel manufacturing process and quality assurance testing that ensure manufacturing reliability • Plan to feedback operating experience from early PBMR to refine technology

3.2.3 Protection system functions

The selection and analysis of anticipated operational occurrences and design basis events forms a significant part of the safety analysis of any plant. The applicability of GDC 20 to active protection and controls systems may be an area of change. A number of studies have been developed to determine events that are possible and to categorize them as abnormal operating occurrences, design basis events, or beyond design basis events. In designing a system that responds to the top level requirement of GDC 20, a safety analysis is conducted to determine that (1) events are adequately detected and (2) that protection functions adequately prevent radiological consequences in excess of dose limits from 10 CFR 20 and 10 CFR 100.

For example, the analysis of the HTR-10 protection system identifies the following set of protection variables and associated actions as shown in Table 2.⁶

⁶ F. Li, Z. Yang, Zhencai An, and L. Zhang, “The First Digital Reactor Protection System in China,” *Nuclear Engineering and Design*, **218**, pp. 215–225 (2002).

Table 2. Protection variables and setpoints for HTR-10⁶

Protection variables	Warning level	Trip setpoint	Applicable power range	Action
Nuclear power (source range)	150% rated power	1 MW	Power <1 MW	PA
Nuclear power (power range)	110% rated power	120% rated power	Power >1 MW	PA
Rate of power increase	2.3%/s	3.5%/s	Power <500 W	PA
Core outlet temperature	720°C	740° C		PA
Core inlet temperature	270°C	290° C		PA
Increase rate of helium pressure	0.01 MPa/min	0.03 MPa/min	Power >3 MW	PA
Decrease rate of helium pressure	0.01 MPa/min	0.03 MPa/min	Power >1 MW	PA, PC, PD
Ratio of helium to water flow	1.2	1.3	Power >1 MW	PA
Ratio of water to helium flow	1.17	1.33	Power >1 MW	PA
Helium humidity	50 ppmv	800 ppmv	Power >1 MW	PA, PB
Decrease rate steam pressure	0.6 MPa/min	1.0 MPa/min	Power >1 MW	PA
Deviation of helium flow from rated	20% of rated flow	20% of rated flow	Power >1 MW	PA

PA – Reactor trip, helium circulator shutdown, and the secondary loop isolation

PB – Isolate and drain steam generator

PC – Isolates refueling system and the helium purification system from the primary loop

PD – Isolate the thermal measurement system from the primary

The reactor trip system must protect the plant under all design basis accidents and the system architecture must exhibit diversity and defense in depth. In the same article, Li shows the HTR-10 approach for organizing and presenting compliance under Chinese guidance analogous to GDCs 21 and 22 for single failure criterion and diversity and defense in depth. In Table 3, the columns are the design basis accidents; the rows are trip functions. The trip functions are divided into A and B subgroups which are implemented on independent processors. For diversity, each design basis accident must be protected by at least two trip functions. Each subgroup must contain at least one of the two or more trips for each event. The subgroups protect against a failure of a single processors software common mode failure. The multiple trip functions for each event protect against a failure of any single detection method. The table is used to demonstrate the acceptability of the HTR-10 design against the general design criteria.

Table 3. Design basis accidents, protection variables, and their group definition

Subgroup	Protection variables	DBA											Protection action	
		False removal of control rods in subcritical or startup condition	False removal of control rods in power operation condition	Increase packing factor in case of earthquake	False speed-up of the helium blower	Increase of feedwater flow rate	Loss of power supply from outside of the plant	Loss of helium flow rate in primary loop	Loss of feedwater flow rate	Loss of pressure in primary loop	Steam generator tube rupture	Break of main steam pipeline		Break of feedwater pipeline
A	Nuclear Power	X	X	X	X	X					X			PA
	Increase rate of nuclear power	X		X										PA
	Hot helium temperature							X						PA
	Cold helium temperature				X				X				X	PA
	Increase of helium pressure						X	X			X			PA
	Decrease of helium pressure									X				PA, PC, PD
	Decrease of steam pressure					X	X					X	X	PA
B	Nuclear Power	X	X	X	X	X					X			PA
	Increase rate of nuclear power	X		X										PA
	Helium humidity										X			PA, PB
	Cold helium temperature				X				X				X	PA
	Ratio of helium flow rate to water flow rate				X		X		X				X	PA
	Ratio of water flow rate to helium flow rate					X		X		X		X		PA
	Deviation of helium flow rate						X	X		X				PA

Note: The protection actions PA, PB, PC, and PD are described in the previous table.

3.3 Operational Controls

In safety analysis, the operational controls are the first echelon of defense in depth. Because the operating point is within the envelope of safe conditions for the plant, the regulation of the plant to the operating point maintains safe conditions and coordinates and controls the process to remain in the safe envelope when disturbances occur.

Control schemes involve different modes and functions depending on the plant state. Most of the major equipment systems have four distinct control modes: offline, startup, normal operation and shutdown. The offline and normal operation modes are typically the continuous static states; startup/shutdown modes are transitional between normal operation and offline. In normal operation, the control systems regulate the process using feedback control. The normal operation mode encompasses both steady state and power maneuvering at rated ramp rates for power change. Additional submodes in normal operation may exist for low power, rapid runback, and special plant configurations (e.g., operation on turbine bypass versus normal turbine).

Automatic feedback regulation control is used in practically all HTGR plants for normal power operation. In early plants, the regulation was implemented using analog components. Modern plants use or will use digital controls. The HTRR and HTR-10 use full digital control systems. The digital systems are typically constructed as a distributed network of devices involving special devices for signal input and output; processing, computations, and logic; communications; and operator interface.

In addition to the regulation of the plant, the same digital control systems perform additional tasks, such as

- providing the operator displays and the operator input interface through touchscreens or trackball,
- diagnostics of the control system and the plant equipment,
- sensor and transmitter calibration,
- historical plant data logging,
- special data logging for accident review, and
- maintenance bypass and logout/tagout functions.

Important functions such as maintaining the ability to control the plant when the control room becomes uninhabitable are also addressed as part of the normal controls. These auxiliary functions, as a group, are not necessarily unique to NGNP designs and may be similar to other reactor designs.

Limited information about the control system designs and algorithms is available in the literature for existing or proposed HTGRs. Detailed control schematics of existing or previous plants have not been found. Operational functions have been described and controls system features can be inferred from the operational descriptions. NGNP control designs are not yet developed because plant configurations have not yet been decided. Only preliminary control system studies have been reported for the NGNP designs. Consequently, only general comments are made regarding the operational controls.

3.3.1 Startup and shutdown

Startup and shutdown of equipment involves a transition from an offline or standby condition to an operational state, or the reverse transition. The transition usually involves discrete logic to monitor the plant status to detect the point at which transition is required and then the performance of a series of steps to convey the system from one state to the other. The transition functions may be manually performed by an operator at the control panel, or in more modern plants, the transition may be controlled automatically with the operator monitoring and acknowledging the automatic transitions as needed to maintain

operational awareness. The previous HTGR plants constructed in the 1960s, such as Fort St. Vrain and AVR, were largely manually controlled in startup and shutdown. The more advanced plants including MHTGR were designed with automated digital startup and shutdown controls. It is expected that NGNP will be fully automated in startup and shutdown. The startup/shutdown controls modes include the operational controls for starting auxiliary systems, such as cooling and lubrication systems; conditioning the equipment for operation, such as, warming components to operating temperatures; and valve and power alignments to bring the equipment online. The startup/shutdown may include a transitional control mode in which one system is started and balanced with other systems already online.

The safety significance of the startup and shutdown control modes is that each control mode constitutes a different set of conditions and responses for the system. Each mode has a different response whose safety must be evaluated for normal conditions, external disturbances, and all types of failures in the plant or the control system.

3.3.2 Normal operation

3.3.2.1 Heat transport system control

The HTGR plant control involves control of a series of heat transfer processes. The reactor produces heat. The flow of helium coolant through the core removes the heat by convection and transports it to a heat exchanger or turbine which removes the heat. Secondary or tertiary loops, if they are part of the design, continue to convey the heat to heat loads, turbines, or other energy conversion processes. At steady state, the operational control system regulates the processes to the design point. The automated controls adjust for gradual changes in the plant, such as burnup or steam generator fouling, or changes in the temperature of the absolute heat sink. Feedback control is used to regulate temperatures and pressures within the heat transport system to their setpoints despite variations in the plant.

The control system is also responsible for normal maneuvering from one power level to another or for restoring the plant to equilibrium following major disturbances such as turbine trip or feedwater pump trip. Disturbances usually involve rapid changes in power level.

The control strategy for normal operation and regulation of the heat transport systems involves control designs that are similar to conventional power plants. The algorithms typically use single loop controls with proportional-integral or proportional-integral-differential action. In many instances, feedforward inputs are added to the feedback action to improve coordination between the different parts of the heat transport system and to improve the speed response. For feedforward action, the control system involves a two-level cascade in which a top level controller computes a setpoint for the lower level controller. The lower level controller in the cascade forms a second error using another measured variable in its feedback loop. The output from the lower level controller is an actuation signal (increase/decrease) or a position demand.

Figures 17 and 18 show typical two-level, cascade control loops with feedforward action for demand output and increase/decrease output. The demand output is used by actuators such as valve positioners which require a position demand. The increase/decrease output is used by systems such as rod controls. For increase/decrease signals, the actuator itself acts as an integrator of the error signal. The feedback devices are shown as proportional-integral action but could be any combination of proportional, integral, or differential action.

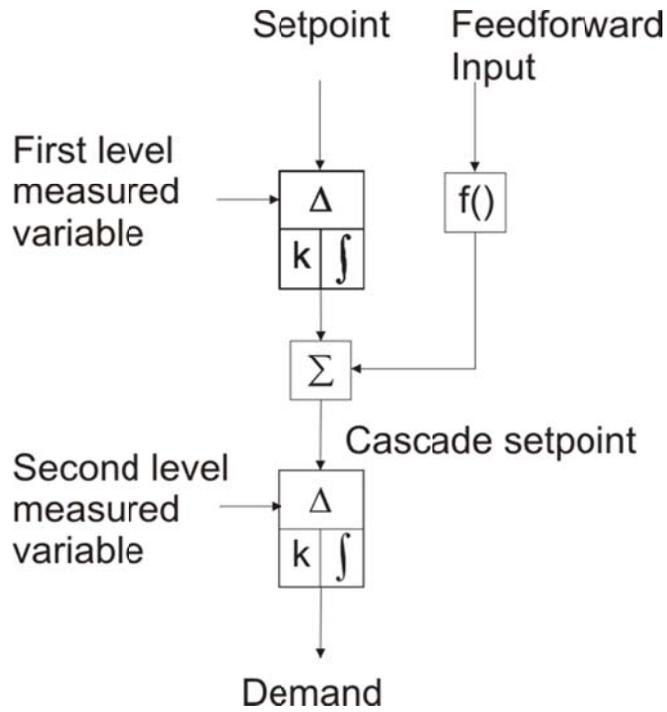


Fig. 17. Two-level cascade controller with demand output.

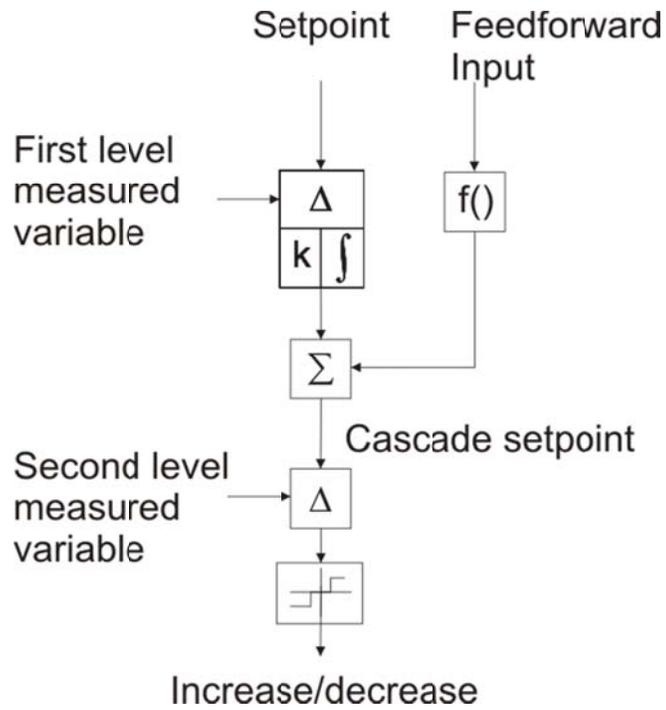


Fig. 18. Two level control with increase/decrease output.

In heat transport systems, the feedforward signal is either a load setpoint from a coordinated load controller or a measured variable that is related to the load, such as feedwater flow. The load signal acts as an exogenous input which causes the heat transport processes in the reactor, steam generator, and turbine to act in unison. The HTGR's dynamic response has a wide range of time constants. The feedforward component of the control signal helps to keep the different parts of the heat transport system responding together despite the differences in the time constants.

The first level feedback gives the corrective action for deviations due to variations in the process. If integral action is included in the first controller, then the cascade setpoint integrates to a value that yields zero offset in the first level error. Typically, this integral has a low gain for slow, stable approach to steady state and is tuned on the basis of the time constant of the first level measured variable to the system demand.

The second level feedback error takes advantage of a measured variable that is more directly affected by the actuator to provide rapid positioning. The open loop response from the demand to the second level measured variable is usually quite fast. The control gains can be much larger, which improves the tracking of the final demand to the feedforward signal. For example, the first level measured variable for the rod control is helium temperature, which has a very slow response. The low gain integral action applied the temperature error gradually corrects for effects such as burnup, errors in feedforward signal, and other disturbances so that the reactor stays at the operating point. The second level measured variable is neutron flux which responds more rapidly. The rod control at the lower level causes the neutron flux to track the load demand in unison with feedwater flow and turbine.

Although the cascade structure results in what is actually a multivariate control problem, modern control methods have not typically been applied to determine the gains analytically. Undoubtedly, this is because conventional tuning strategies work very well. The main limitation in operating response is not due to control algorithm issues; rather, it is the speed of actuators (rod drive, valve actuator, etc.) that limit the responsiveness. The rate limits and saturation limits of the actuators would impose constraints on a multivariate controller (or would be considered nonlinearities depending on the method of solution). The complexity of the resulting control system design has simply not been justified. Based on the survey of the literature, control schemes for HTGRs are developed with ad hoc structure and trial and error tuning. The similarity of the control problem to conventional fossil power plants gives historical basis to assume that this control design approach would prove to be satisfactory.

3.3.2.1.1 Steam generator-turbine heat transport controls

Four of the five existing HTGRs surveyed have a steam generator and steam turbine for power conversion. (The fifth, HTTR, has a water cooled heat exchanger that dumps heat to an air cooler without any power conversion.) The heat transport loop of steam generator plants consists of the reactor, helium circulation system, the steam generator, and the turbine-generator. The heat transport system's inputs and outputs are all closely coupled together so that many different input-output pairs give feasible control systems. This fact is borne out by the range of configurations that are found in the survey of existing plants.

Three of steam generator-turbine plants in the survey of existing plants have sufficient detail to compare the overall control scheme for the heat transport plant. The main heat transport loop at normal power operation involves control variables for four main systems: reactor power, feedwater control, electrical power, and circulator flow. The control schemes are compared in Table 4. What is interesting is that substantially the same control problem can be solved in three very different ways for the three reactors reviewed.

The table gives the specific input and output variables for each loop in terms of the general cascade controllers in Figs. 17 and 18. For example, the MHTGR column indicates that the first level process variables are assigned so that the allocated load (for each reactor module) is controlled by the module

feedwater flow valve, steam pressure (for a power block) is controlled by the turbine throttle valve, and steam temperature is controlled jointly by circulator speed and reactor neutron power. The MHTGR uses the measured feedwater flow setpoint as a feedforward input to coordinate the reactor power and the circulator speed. The input/output pairs and actions are based on the operational descriptions of the control systems. Some uncertainty in the data exists because of vague descriptions in the source documents. Questionable data are indicated with (?).

Table 4. Cascade control schemes for three HTGRs

Controlled variable	Controller input components	MHTGR	Fort St. Vrain	AVR
Control rods	Feedforward input	FW flow	Steam flow	None
	First level (action)	Steam temperature (PD or PID)	Reheat steam temperature (PI)	Reactor outlet temperature (Manual?)
	Second level (action)	Neutron flux (P)	Neutron flux (P)	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease
Helium circulator motor frequency	Feedforward input	FW Flow	FW flow	None
	First level (action)	Steam temperature (PD)	Main steam temperature (PI)	Electrical load (Manual?)
	Second level (action)	None	None	None
	Output	Speed demand	Speed demand	Speed demand
Feedwater valves	Feedforward input	Module load	Turbine first stage pressure	
	First level error (action)	FW flow (PI)	Steam Pressure (PI?)	Steam temperature (Manual?)
	Second level error (action)	None	FW Flow (PI?)	None
	Output	Valve demand	Valve demand	Valve demand
Turbine admission valve	Feedforward input	Total load	None	None
	First level error (action)	Steam pressure (P)	Electrical load	Steam pressure (P)
	Second level error (action)	None	None	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease

3.3.2.2 Direct cycle gas turbine plants

The other type of power conversion proposed for HTGRs is the direct-cycle, gas turbine.⁷ The most common configuration for the plants is a single shaft design in which the compressor, turbine, and generator are all on the same shaft. The control inputs are considerably different than a steam turbine plant. In normal operation, when the generator is synchronized to the grid, the helium circulator speed is fixed by the grid frequency. Also, the gas turbine is not usually throttled like steam turbines. Lacking circulator speed and turbine throttle valve takes away two degrees of freedom that the steam generator plants utilize. The control inputs for the gas turbine system are the rod position, helium inventory (mass in primary), turbine bypass valve, and the intercooler flow control valve. The turbine bypass valve routes the

⁷C. Rodriguez, J. Zgliczynski, and D. Pfremmer, *GT-MHR Operations and Controls*, General Atomics Project 7600, GA-A21894, November 1994.

helium flow around the turbine. It is a fast-acting, but thermodynamically inefficient, means for controlling electrical load. Helium inventory is slow-acting means for controlling electrical load. Changing density of the helium maintains the same gas velocities and blade versus gas velocity angles so that efficiency is constant with load but involves slow response and pumping losses in removing and restoring the helium to the primary. The flow to the inventory storage system is extracted from the high pressure side of the compressor and return flow is to the low pressure side so that no separate helium pump is needed (except for startup). The rods are used to control reactor outlet temperature, and the intercooler secondary side flow (water cooled usually) is used to control reactor inlet temperature.

3.3.2.3 Helium purification systems

Helium purification systems contain a number of local controls for controlling the flow and temperature of the helium stream. In addition, the normal operation of these systems typically has two submodes: purification and regeneration. Helium purification systems have at least two trains so that one train can be online and processing the helium coolant and the other in regeneration to remove impurities from adsorption beds and ready them for re-use. Automatic controls for both normal purification and regeneration would involve on/off controls to redirect flows and transfer systems from one mode to the other and control algorithms to regulate temperatures, flows and chemical concentration in the purification and regeneration modes. Control schemes for the purification plants have not been found in the literature survey.

Moisture removal from the primary system is one of the safety functions required following a water ingress event.

3.3.2.4 Cooling systems

Controls for support cooling systems such as vessel cooling system, shutdown cooling system, component cooling system, and various balance of plant heater exchangers require normal controls similar to LWRs. Descriptions of the controls and instrumentation for these systems is not available however in the literature.

3.3.2.5 Potential NNGP heat transport systems controls

When this project was originally conceived, the concept for the NNGP was that the hydrogen production plant would be the only heat load. A combined cycle plant involving, for example, both electrical generation and hydrogen production was not planned. However, the plant design is still in a state of flux. A number of key design issues for the control system, including the heat load configuration, are undecided. The control issues depend significantly on the plant loop configuration.

As discussed in Chapter 5, proposed NNGP designs have shown considerable variety in the configuration of the heat transport systems. Designs involving intermediate loops for driving steam cycle, combined electrical load and chemical plant, and direct cycle gas turbines have been proposed. The range of possibilities does not lend itself to a useful general discussion of controls and protection. Each type of heat load (i.e., steam generator and turbine, gas turbine, or process heat plant) has a typical set of measured variables and control requirements independent of the other heat loads in a combined cycle plant. The combined cycle plant requires additional control logic to allocate the reactor heat source to the individual heat loads. The transient analysis of combined cycle plants must include all the transients each heat load can initiate and the impact on the heat load itself and on the rest of the plant. The complexity the load results in complexity in the controls and protection.

4. PROTECTION AND CONTROL SYSTEMS OF OPERATIONAL HTGRS

4.1 HTGR Descriptions

This chapter discusses the design of the reactor systems and their control and protection systems for a representative group of existing or proposed designs. The designs are selected to cover a range of design variations and different countries. Those systems which have more complete documentation in the open literature are also given preference.

4.2 Modular High Temperature Gas Reactor—MHTGR

4.2.1 Reactor system design

This section provides a summary of the instrumentation and control features of the modular high temperature gas-cooled reactor (MHTGR). The section discusses the plant design and operation in sufficient detail that the instrumentation and control features can be understood. Because the MHTGR design is significantly different from the operating light-water reactors (LWRs) which have been previously licensed in the United States, the NRC was involved early on in design reviews. As part of their participation, the NRC prepared a preliminary safety evaluation review⁸ of MHTGR pre-application design report. Issues from the NRC review are discussed at the end of the section.

The MHTGR is a modular high temperature gas-cooled reactor (HTGR) design whose development was primarily supported by the U.S. Department of Energy (DOE) based on many years of domestic and international gas-cooled reactor research and experience. Reference documents addressing design benefits, fuel characteristics, high temperature materials development, regulatory documents, safety assessments, etc., number in the thousands for this extensively studied reactor. The *Conceptual Design Summary Report—Modular HTGR Plant*⁹ is a good basic reference for the plant design.

The objective of the development was a safe, economic electric power generation option. The design was guided by specific user requirements that addressed safety, performance, availability, and economics.¹⁰ Safety and protection of the public were high-level requirements.

The MHTGR was originally conceived as four 350 MW(t) prismatic core reactor modules cooled by helium. The reactor fuel design used TRISO fuel particles in hexagonal prismatic fuel form as shown in Figs. 2 through 4 of Chapter 2. Both fissile and fertile tri-isotropic (TRISO) coated fuel particles are used. The initial fuel design used thorium in the fertile particles. A later design variation used natural uranium. Heat removal from the helium coolant in each reactor module was accomplished by a steam generator. The steam lines for four reactors were coupled to a steam header. The two steam turbine-generators were connected to the steam header to produce a net electrical output of 538 MW(e). Later design concepts raised the power of each module to 450 MW(t) and variations incorporated Brayton cycle gas turbines for higher thermal efficiency either via a direct cycle or through an intermediate helium loop. The Brayton cycle design is called the gas turbine, modular helium reactor, GT-MHR. Potential benefits included plant simplification and potentially better economics.

The characterization of the reactor systems that follow refer to the 350 MW(t) modules as initially proposed. Major specifications are shown in Table 5. Each of the four reactor modules in a power block is

⁸*Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, December 1995.

⁹*Conceptual Design Summary Report Modular HTGR Plant (Reference Modular High-Temperature Gas-Cooled Reactor Plant)*, DOE-HTGR-87-092, September 1987.

¹⁰*Utility/User Requirements for the Modular High Temperature Gas-Cooled Reactor Plant*, Gas-Cooled Reactor Associates (GCRA), GCRA-002, Rev. 3, June 1987.

identical. A typical MHTGR single module is shown in Fig. 1 from the preceding chapter. Each steel reactor pressure vessel contains subsystems for the reactor core, neutron control, and reactor internals. The annular fuel region of the core is contained within inner and outer graphite reflector regions. Control rods are contained in the reflector regions. A reserve shutdown system permits the addition of boron neutron absorber pellets into 12 channels in the center region of the core.

Table 5. MHTGR design parameters

[DOE-HTGR-97-092, *Conceptual Design Summary Report Modular HTGR Plant*]

REACTOR MODULE DESIGN PARAMETERS	
Item	Parameter
Configuration description	Side-by-side (SBS)
Heat transport system	
Modules per station	4
Power per module	350 MW(t)
Coolant and pressure at rated power	Helium at 6.39 MPa (925 psia) at circular discharge
Cold helium temperature	259°C (498°F) at circulator discharge
Hot helium temperature	687°C (1268°F) at core exit
Core helium flow rate	157.1 kg/s (1,246,000 lb/h)
Core helium pressure drop	34.5 kPa (5.0 psi)
Feedwater temperature/pressure	193°C/21.0 MPa (380°F/3,000 psia)
Steam temperature/pressure	541°C/17.3 MPa (1005°/2,515 psia)
Vessel material	Low alloy steel, manganese–molybdenum SA533 Grade B, Class 1
Reactor vessel overall height	22 m (72 ft)
Reactor vessel outside diameter	6.8 m (22.4 ft)
Plant design lifetime	40 year
Design basis operation	80 percent capacity factor
Number of components per module	
Steam generators	1
Main circulators	1, electric motor-driven
Shutdown cooling heat exchangers	1
Shutdown circulators	1, electric motor –driven
Control rods	30 (6 inner, 24 outer reflector rods)
Reserve shutdown channels	12 (inner row of core fuel elements)
Core and fuel cycle	
Fuel element	Prismatic hex-block, 36.0 cm across flats × 79.3 cm height
Active core configuration	66-column annulus, 10-blocks high
Fissile material	Uranium oxycarbide
Power density	5.9 W/cm ³
Coolant volume fraction	0.19
Average enrichment	19.9 percent U-235
Power peak/average axial ratio	1.4:1
Fertile material	ThO ₂
Initial core loading, kg: U/Th	1,726/2,346
Equilibrium reload, kg: U/Th	1,030/706
Equilibrium burnup, MW-d/ton	92,200

The reactor pressure vessel is connected to a steam generator vessel by a concentric cross-duct. Each reactor module is housed in a cylindrical concrete underground enclosure (silo). The plant itself comprises the four silos plus adjacent structures for reactor services, fuel storage and handling systems, and coolant purification and cleanup systems. A shutdown cooling system circulator and heat exchanger as described in Sect. 2.7.1 are mounted at the bottom of the reactor vessel. The reactor vessel is uninsulated with an air-cooled RCCS. A safety feature of the design is that core decay heat may be removed by purely passive systems via radiation and natural convection from the reactor vessel to the concrete enclosure and to the environs in the event that forced circulation and heat transport to the balance of plant is lost.

The steam generator vessel contains the single stage axial flow main coolant circulator mounted at the top and a vertical helical coil heat exchanger as described in Sect. 2.4.1 and shown in Figs. 9 through 11. A conventional turbine generator receives the steam generated by the reactor module and converts it to electrical energy. The power conversion from steam to electricity was to be carried out with two identical, independent 300 MW(e) turbine generators. The systems were cross connected at a common feedwater header and steam generators outlet steam header. A turbine cycle configuration and heat balance diagram are shown in Fig. 19.

Several support systems are part of the turbine generator system. These include the feedwater and condensate system, main steam and turbine bypass system, startup and shutdown system, steam and water dump system, turbine plant cooling water system, heat rejection system, and other turbine plant systems.

4.2.2 Current status

The MHTGR is an advanced reactor concept that was developed under a cooperative arrangement with the utilities, the nuclear industry, and government. A licensing plan¹¹ was submitted to the U.S. Nuclear Regulatory Commission (NRC) in 1986 that proposed a schedule of licensing activities prior to the submittal of an application. This document recognized the value of early and frequent interaction between the NRC staff and the reactor developers to develop regulatory criteria and the conceptual design configuration. The standard process at the time was for the applicant to submit a complete preliminary design to the NRC for review. The MHTGR design was in many ways fundamentally different from operating LWRs (e.g., passive heat removal systems, reliance on fuel particle integrity as a primary fission product barrier, high temperature metals, etc.). A close early involvement of the NRC might lead to a more efficient review process. A Preliminary Safety Information Document (PSID)¹² with numerous revisions was submitted to help support the initial review of the concept to provide a basis for concluding that the standard MHTGR was licensable; identify interfaces between the primary systems, secondary systems, and the environment; and to show compliance with dose and risk criteria. The applicant interacted extensively with NRC staff, Advisory Committee on Reactor Safeguards (ACRS), and Oak Ridge National Laboratory and Brookhaven National Laboratory contractors.

The NRC issued the draft Pre-Application Safety Evaluation Report (PSER) on the MHTGR design in 1989.¹³ General conclusions of the draft SER¹⁴ were that the MHTGR had the potential to have a high level of safety, exceed the safety level of current LWRs, and meet or exceed NRC safety goals. Important aspects of the design found to be technically acceptable by the NRC at the time included the absence of a traditional pressure-retaining containment structure, use of a mechanistic source term, and the absence of a need for an emergency evacuation/shelter plan for the public.

¹¹*Licensing Plan for the Standard HTGR*, DOE-HTGR-85001, Rev. 3, February 1986.

¹²*Preliminary Safety Information Document for the Standard MHTGR*, HTGR-86-024, 1986.

¹³*Draft Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, March 1989.

¹⁴As noted in, *The Licensing Experience of the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, F. A. Siladay, J. C. Cunliffe, and L. P. Walker, General Atomics, GA-A19455, p. 11, September 1988.

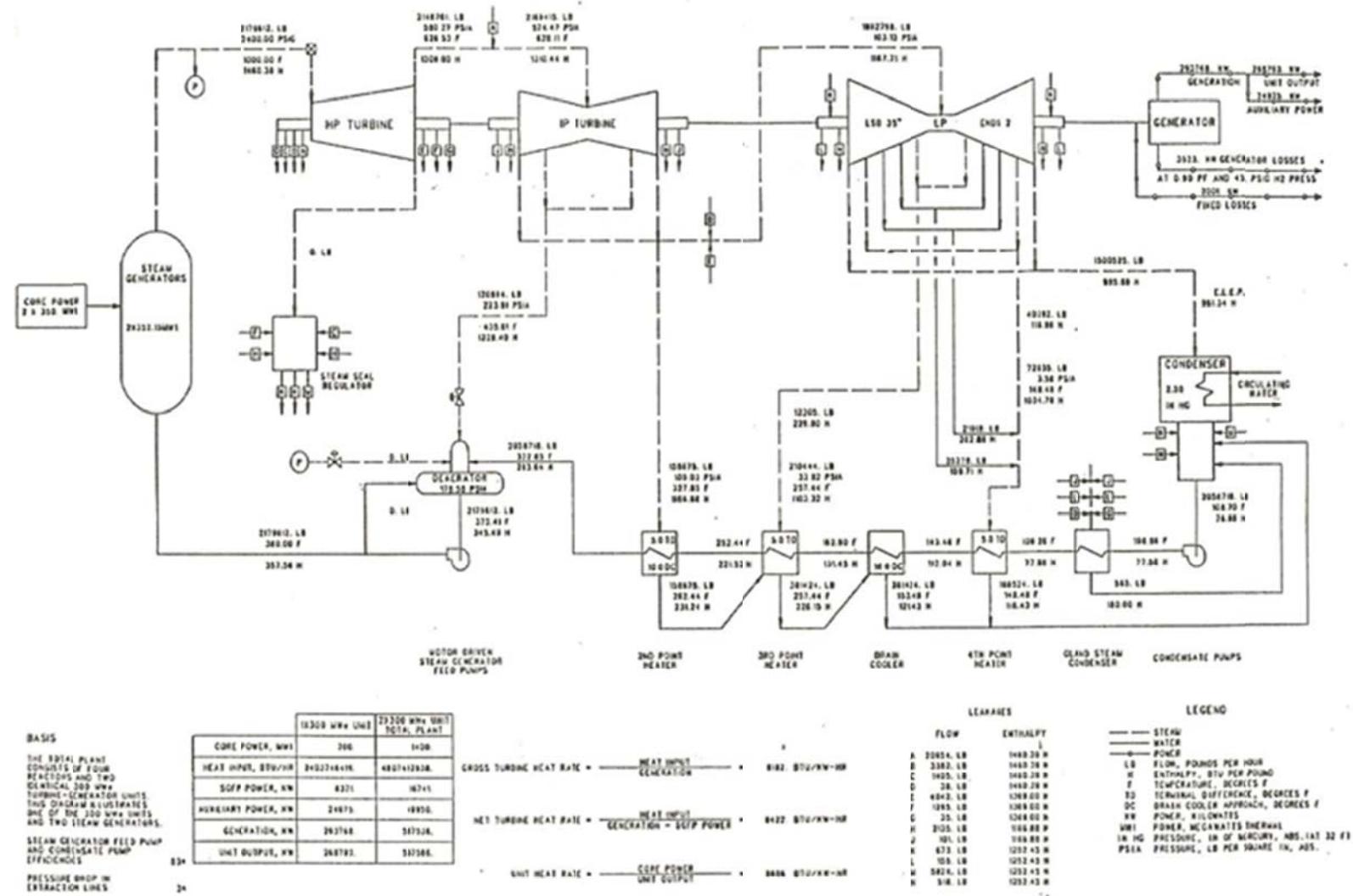


Fig. 19. Turbine generator configuration and heat balance.

[DOE-HTGR-87-092, Conceptual Design Summary Report Modular HTGR Plant]

Subsequently, additional information relevant to the pre-application review, including applicant reports, reports on evolutionary LWRs and other advanced reactors relevant to the MHTGR, and NRC guidance led to revisions to the draft PSER. The draft of the final PSER was published in December 1995.¹⁵

The MHTGR design presented a number of interesting design, safety, and operational considerations to the NRC, who, during this period of time, was also reviewing other evolutionary LWR designs and advanced reactor concepts. Ten advanced reactor policy issues were presented to the Commission in SECY-93-092, of which eight were pertinent to the MHTGR. These were:

1. accident evaluation,
2. source term,
3. containment,
4. emergency planning,
5. operating staffing and function,
6. residual heat removal,
7. control room and remote shutdown area design, and
8. safety classification of structures, systems, and components.

Discussions of these issues are summarized in Sect. 4.2.6 of this report.

4.2.3 Plant protection, instrumentation, and control systems

The design of the MHTGR provides for interconnected and integrated automatic control of the four reactor modules and two turbogenerator systems that comprise the plant. Automatic control is used for normal operations and for abnormal events; no operator actions are required to shut down the reactor for event categories included in the safety analysis. The plant safety/protection function is provided by separate, redundant safety-related instrumentation and control components. The plant is to be controlled by an operator and an assistant from the main control room. Additional monitoring and control capabilities are provided at a remote shutdown area room in the reactor service building and in plant protection and instrumentation system rooms in each reactor building. A description of the protection and I&C systems for the MHTGR is summarized in the NRC's draft PSER¹⁶ as well as concerns resulting from the staff review of the PSID. An overview of this NRC assessment is provided in this section.

MHTGR plant protection and automatic control are provided by the partly safety-related plant protection and instrumentation system (PPIS); the plant control, data, and instrumentation system (PCDIS); and the miscellaneous control and instrumentation group (MCIG).

The MHTGR instrumentation and control system has several novel features compared with the existing reactor fleet.

- All four reactor modules and the two turbine generators are monitored and controlled from a single control room via a modular, distributed control system that allows load to be allocated automatically among the reactor modules and the two turbine generators.
- An independent, redundant, and fully automated protection system, including a remote shutdown area is provided. The safety-related portions of the system (reactor trip and main coolant loop shutdown) are fully automatic; no safety-related operation actions are necessary or are even available in the control room.
- Most of the PPIS circuitry is contained in reactor module equipment rooms. The control room is not deemed as safety-related by the applicant.

¹⁵*Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, December 1995.

¹⁶*Draft Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, March 1989.

- Control room operator actions are not viewed as safety related but as a monitoring function and performance of plant mission management activities.
- Manual initiations of protective functions may be carried out in the remote shutdown area (RSA) or reactor module PPIS equipment rooms.
- The control room, RSA room, and reactor module PPIS rooms are designed to limit operator exposures during accident conditions.

4.2.3.1 Plant protection and instrumentation system

The PPIS indicates plant status and automatically actuates safety-related control systems and investment protection control systems. It consists of the safety protection, special nuclear area instrumentation, and investment protection subsystems.

Safety protection system

The safety protection subsystem initiates a reactor trip and shuts down the main cooling system. Specifically, the subsystem initiates:

- a reactor trip with the outer control rods,
- a reactor trip utilizing the reserve shutdown control equipment—a diverse trip system, and
- a main loop shutdown and isolation of main steam to protect against water ingress events and to protect major secondary-side equipment.

This subsystem is safety related. The safety protection system has the capability to sense plant process variables, detect abnormal plant conditions, and initiate protective actions. The scope of the system begins with process protection sensors and extends to the inputs of actuated systems. The system mitigates the consequences of design basis events to protect the public health and safety and to ensure that equipment and structure damage limits are not exceeded. Redundancy is employed within the safety protection system of each module. Each module has a separate and independent, remote multiplexed, centrally controlled, microprocessor-based safety protection system. As originally planned, separate and independent safety protection system operator interfaces for each reactor module were to be provided in the plants remote shutdown building. Ultimately, this capability would likely have been extended to the main control room at the request of the NRC. Its architecture consists of multiple separate and redundant optical-digital-data pathways from the remote multiplex units that communicate with four separate, redundant computers that make up the four-channel protection systems for each module, as shown in Fig. 20. Two-out-of-four coincidence logic initiates a protective action.

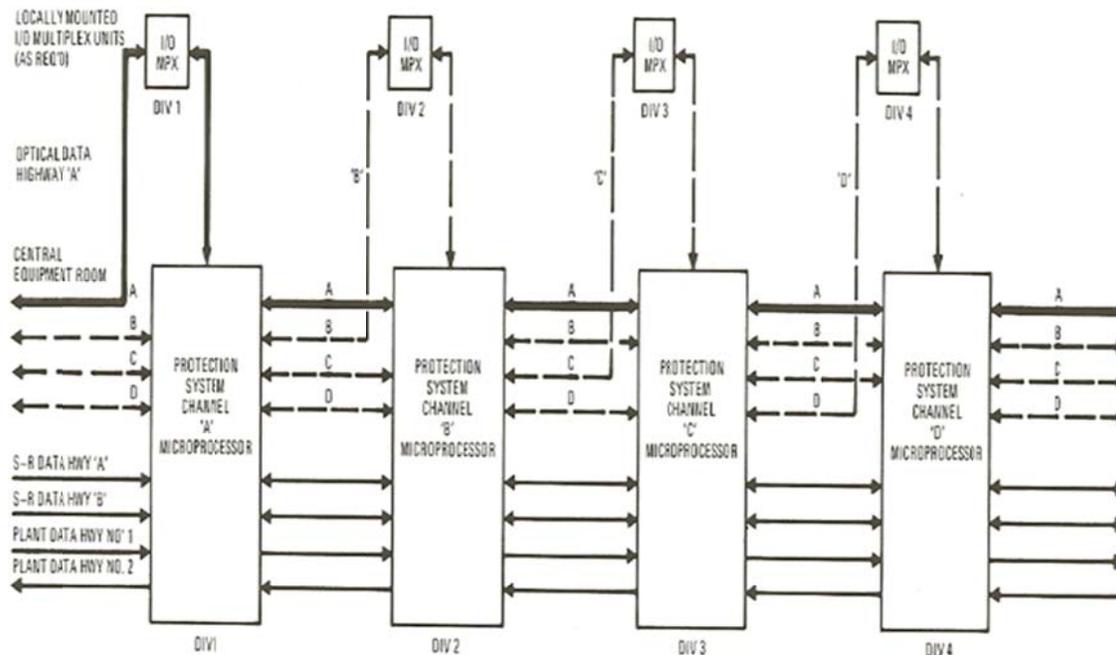


Fig. 20. Protection system data buses.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

The first protective action is the trip of a reactor module's outer control rods, which can occur for safety-related or nonsafety-related plant conditions. Safety-related conditions are:

- neutron flux to helium mass flow ratio—high,
- primary coolant pressure—high, and
- primary coolant pressure—low (bypassed on low neutron flux).

Nonsafety-related conditions for which the safety protection system actuates are:

- primary coolant moisture concentration—high,
- steam generator helium inlet temperature—high,
- main loop shutdown/main steam isolation trip signal, and
- manual actuation.

A reactor trip signal also notifies the plant data, control, and instrumentation system to initiate a feedwater flow reduction and ramp down of the steam supply system.

The second protective action is actuate the reserve shutdown control equipment, which occurs if the outer control rod trip system fails when commanded or if there is a positive reactivity condition due to water ingress into the core that exceeds the negative reactivity of the outer control rods. Safety-related conditions are:

- neutron flux to main circulator speed—high (with a time delay to allow for outer rods to trip),
- primary coolant pressure—high, and
- manual actuation (a nonsafety-related condition).

The reserve shutdown control equipment initiates when the actuation signal causes fusible links to be energized and open, which causes hoppers of borated pellets above the core to empty their contents into empty channels in fuel columns adjacent to the inner reflector and adding negative reactivity to the core. The negative reactivity of the reserve shutdown system is sufficient alone to maintain required level of subcriticality at cold shutdown and maximum water ingress.

The third protective action is the main loop shutdown and main steam isolation. This main steam isolation/steam generator isolation limits chemical attack on the fuel from water ingress to the core from a steam generator leak and protects the turbine from low-temperature, low-quality steam. The main loop shutdown protects steam generator components from high primary system temperature effects. The loop shutdown occurs when the main circulator receives a trip signal and feedwater block valves are signaled to close. Concurrently the main steam isolation valves shut off the secondary coolant system loop.

Conditions requiring main loop shutdown are:

- primary coolant pressure—high (safety-related condition),
- circulator speed high or low compared to a programmed setpoint (a nonsafety-related condition),
- steam generator isolation and dump signal (a nonsafety-related condition), and
- manual actuation (a nonsafety-related condition).

Conditions requiring main steam isolation are:

- main loop shutdown (safety-related condition),
- main steam low temperature (a nonsafety-related condition), and
- manual actuation (a nonsafety-related condition).

Special nuclear area instrumentation subsystem

The functions of the nonsafety-related (as proposed) special nuclear area instrumentation subsystem include:

- primary system pressure relief block valve closure interlock,
- protection subsystem information displays, and
- postaccident monitoring instrumentation.

Investment protection subsystem

The investment protection subsystem monitors plant conditions and initiates protective actions to limit plant investment risk. It was proposed as a nonsafety system whose functions include:

- reactor trip with inner control rods,
- steam generator isolation and dump,
- shutdown cooling system initiation,
- primary coolant pumpdown, and
- shutdown cooling heat exchanger isolation.

Operator interfaces for safety protection equipment for each reactor module in plant protection and instrumentation system equipment rooms and remote shutdown areas/rooms. An operator may initiate reactor trips and main cooling system shutdown from the remote shutdown areas, separate from the main control room. In the proposed design, manual inputs (e.g., manual reactor trips) to the safety protection system cannot be made from the main control room; however, a normal shutdown can be accomplished from the main control room. The operator interfaces are separate and independent of all other plant instrumentation and controls.

The NRC staff voiced several concerns during their review of the preapplication safety information document to be examined in more detail when the full application is submitted. These included the means for an operator to manually trip the reactor, ensuring independence of the protection system from the control system, nonsafety classification of certain equipment, such as investment protection trip functions that are common to the safety-protection trip functions, the block valve closure interlock system, steam generator dump and isolation valves, and system monitoring equipment.

4.2.3.2 Plant control, data, and instrumentation system

The nonsafety-related plant control, data, and instrumentation system is a network of integrated, hierarchical digital computers and control and monitoring instrumentation that permits the modular reactor units and two turbine generators to be operated and controlled from startup to power operation to normal shutdown. It is comprised of four subsystems: (1) plant supervisory control subsystem (see Figs. 21 and 22 for overview and configuration information), (2) nuclear steam supply system control subsystem, (3) energy conversion area control subsystem, and (4) data management subsystem. The descriptions provided below were extracted from the Preliminary Safety Information Document for the Standard MHTGR¹⁷. Changes in various design changes may have superseded some of the information presented here; however, the basic policies and philosophy should still illustrate principles of the systems.

¹⁷*Preliminary Safety Information Document for the Standard MHTGR*, HTGR-86-024, Vol. 3, Section 7.3.

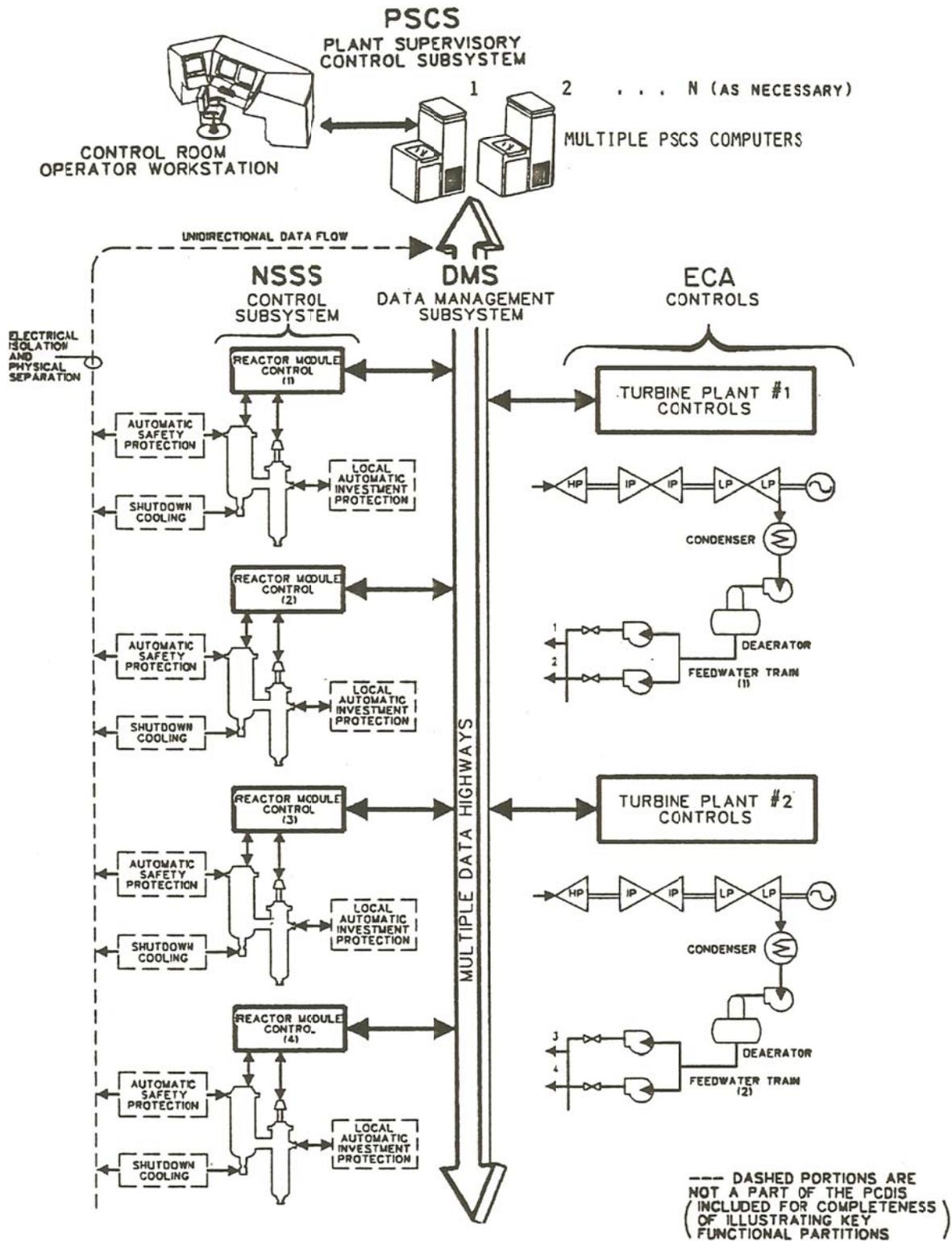


Fig. 21. Plant supervisory control subsystem control overview.

[DOE-HTGR-87-092, Conceptual Design Summary Report Modular HTGR Plant]

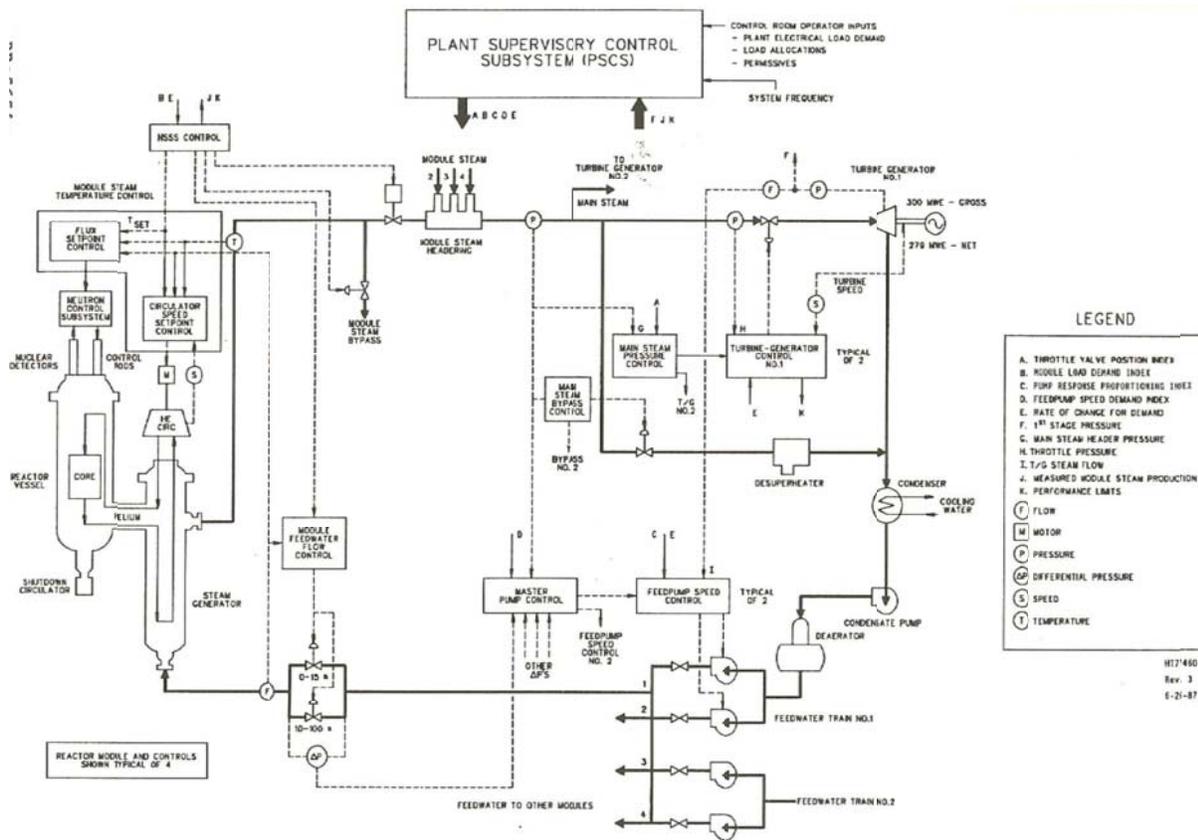


Fig. 22. Plant control and interface configuration.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

Plant supervisory control subsystem

The plant supervisory control subsystem (PSCS) coordinates plant control during operation, shutdown, refueling, and startup/shutdown. The PSCS determines how to divide overall plant load demand to individual reactor modules and turbine generators. It determines main steam and feedwater flow rates necessary to meet load maneuvers that may arise from the plant operator, grid operator, or reactor module or plant conditions. The PSCS computers manage the plant through selection of the necessary mode of plant operation and control strategy for best operation of the reactor modules and turbine generators independently at various power levels and then validates appropriate plant response. The PSCS has startup/shutdown, normal operation, refueling, shutdown, and abnormal operating modes. The control strategies associated with each operating mode are briefly described.

PSCS startup/shutdown

Table 6 summarizes the PSCS control strategy during plant startup and shutdown. Reactor module startup from depressurized shutdown consists of bringing the modules up to minimum stable operating conditions sequentially through series of operator checkpoints several times during the startup. These checkpoints are underlined in the table.

Load levels for the modules are raised in parallel to a common average level at ramp rates of +0.5% per minute. Modules are connected to the main steam header one at a time. The logic for shutdowns is the

reverse of startups. For shutdowns, the modules are shutdown in a parallel manner at incremental levels. Modules are disconnected from the main steam header one at a time.

Table 6. PCSC control strategy for normal startup or shutdown

[HTGR-86-024, *Preliminary Safety Information Document for the Standard MHTGR*]

<p>OBJECTIVE: SEQUENTIALLY MANEUVER REACTOR MODULES (incrementally if in parallel) TO STABLE OPERATING CONDITIONS.</p> <p>(underlined items below are operator permissives required to continue automatically.)</p> <ul style="list-style-type: none">o CONFIRM AUXILIARY SYSTEMS IN SERVICE AND INITIAL CONDITIONS MET (pressurization, etc.)o REQUEST <u>MODULE STARTUP</u>o MONITOR <u>SUBCRITICALITY</u> TESTS AND CONDITIONSo INDICATE ACHIEVEMENT OF <u>CRITICALITY</u> TO OPERATORo ASCERTAIN <u>PROPER FEEDWATER CHEMISTRY</u>o REQUEST <u>MODULE STEAM PRODUCTION</u>o CONFIRM ESTABLISHMENT OF <u>REQUIRED</u> MODULE <u>STEAM</u> AND MAIN STEAM HEADER <u>CONDITIONS</u> (e.g., pressure, temperature, etc.) FOR MODULE HEADERINGo REQUEST CONNECTION TO MAIN STEAM HEADER AND INCREASE MAIN STEAM LOAD INDEXo REQUEST ESTABLISHMENT OF TURBINE SEALS, CONDENSER VACUUM AND <u>TURNING GEAR OPERATION</u>

PSCS normal operation

Table 7 summarizes the PSCS control strategy during normal plant power generation (25–100% load). The primary control function is to allocate main steam flow (secondary side) demands and feedwater flow (primary side) demands to the energy conversion area and nuclear steam supply control subsystems, respectively. The PSCS calculates the main steam demand equivalent of the generator electrical demand, from which an algorithm calculates feedwater demand. These are continuously apportioned equally among the available turbine generators and reactor modules through another algorithm.

Table 7. PCSC control strategy for normal startup or shutdown

[HTGR-86-024, *Preliminary Safety Information Document for the Standard MHTGR*]

OBJECTIVE:	MANEUVER ALL MODULES IN PARALLEL FROM 25 PERCENT TO 100 PERCENT RATED LOAD AFTER OPERATOR PERMISSIVES ARE ACKNOWLEDGED.
STRATEGY:	<ul style="list-style-type: none">o CONVERT PLANT OUTPUT DEMAND (MWe or percent capacity) INTO TOTAL FEEDWATER AND MAIN STEAM DEMANDSo DETERMINE LOAD DEMANDS AND RATES OF LOAD CHANGE RELATIVE TO<ul style="list-style-type: none"><u>design rated</u> plant capacity if all modules are unconstrained<u>available</u> plant capacity if any modules are constrainedo EQUALLY ALLOCATE INDIVIDUAL REACTOR MODULE FEEDWATER AND MAIN STEAM ADMISSION DEMANDS (FOR AVAILABLE REACTOR MODULES AND T-G's)o IF - ANY MODULES ARE CONSTRAINED and<ul style="list-style-type: none">IF - THE PLANT LOAD CHANGE RATE REQUIRES MODULE LOAD CHANGES AT RATES EXCEEDING THOSE USED TO MEET 15 PERCENT STEP LOAD INCREASESTHEN - DECREASE THE PLANT LOAD CHANGE RATE TO THAT RATE ACHIEVABLE BY THE UNCONSTRAINED MODULES

PSCS refueling

The PSCS does not perform any refueling control functions. Control room operator-initiated functions that could add positive reactivity to a shutdown module are deactivated.

PSCS shutdown

The PSCS primarily performs monitoring functions for portions of the plant that are shutdown to ensure that the reactor is maintained in a shutdown condition, core geometry is maintained, neutronic measurements are acceptable, and decay heat removal functions are provided.

PSCS abnormal operating modes

Table 8 summarizes the PSCS control strategy during abnormal power generation during which the PSCS coordinates continuous plant operation during and following transient conditions associated with problems with major reactor module or turbine generator systems or components. The PSCS implement control strategies for reloading the plant once problems have been corrected. The PSCS is capable of recovering from generator load rejects and turbine trips (except on low condenser vacuum) from any power level without requiring a reactor trip, even if reactor modules or turbine generators are constrained for some reason.

Table 8. PCSC control strategy for normal startup or shutdown

[HTGR-86-024, *Preliminary Safety Information Document for the Standard MHTGR*]

OBJECTIVE:	MAINTAIN POWER GENERATION UNLESS INVESTMENT PROTECTION IS CHALLENGED OR COMPROMISED.
STRATEGY:	
o IF	- REACTOR POWER IS GREATER THAN HEAT SINK CAPABILITY (e.g., turbine trip, feedwater reduction, etc.)
THEN	- INITIALLY DECREASE REACTOR MODULE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK
AND	- FOR A TURBINE TRIP, EVENTUALLY INCREASE ALL LOAD INDICES IF AT LEAST ONE TURBINE IS AVAILABLE
o IF	- REACTOR POWER IS LESS THAN HEAT SINK CAPABILITY (e.g., module trip, etc.)
THEN	- ASCERTAIN PLANT ABILITY TO MAINTAIN THE ORIGINAL PLANT OUTPUT
AND	- EVENTUALLY INCREASE REACTOR MODULE LOAD INDICES TO COMPENSATE FOR REDUCED PLANT OUTPUT
OTHERWISE	- REDUCE TURBINE LOAD INDEX TO ACHIEVE AN AUTOMATIC LOAD RUNBACK

Nuclear steam supply system control subsystem

Each reactor module has its own nuclear steam supply system (NSSS) control subsystem that controls reactor conditions and supply of steam to the main steam header. The NSSS control subsystem responds to demands from the PSCS and then controls its feedwater flow demand (primary system demand) to meet its load demand. Figure 23 shows the control functions and interfaces of the NSSS control subsystem. The NSSS control subsystem performs its function by:

1. following the mission set by the PSCS (with plant operator concurrence), including startups and shutdowns;
2. monitoring conditions required for the NSSS to be operable;
3. determining the strategy to be used to produce the module's steam requirements;
4. implementing the chosen control strategy; and
5. displaying information on the NSSS status and conditions.

The major functions of the NSSS control subsystem are to manage module feedwater flow control demand, circulator speed control, power characterization, main steam temperature control, and main steam pressure during startup. The NSSS control subsystem reactor module control loops are configured to accommodate feedwater, reactor module, and turbine trips. In addition, the control loops minimize transient extremes to protect plant equipment and optimize NSSS availability.

NSSS feedback control algorithms are proportional plus integral plus derivative expressions (PID) or proportional plus derivative (PD). The result of this feedback algorithm may be summed with a feed forward signal that is a function of the reactor module load setpoint. The sum of the compensation output and the feed forward signal are passed through limiter logic to provide high, low, and/or rate limits. The output from the limiter is sent to the manipulated variable (dependent variable). If at a limit, a signal is sent to the PID to force it to track such that the sum of the compensation output and the feed forward satisfy the limit condition. A number of special control schemes were devised for specific situations. The

special controls schemes altered the normal settings for ramp rates, feedback gains, etc., to improve system response in the special event. The complexity of these system and potential for unintended functions were not analyzed.

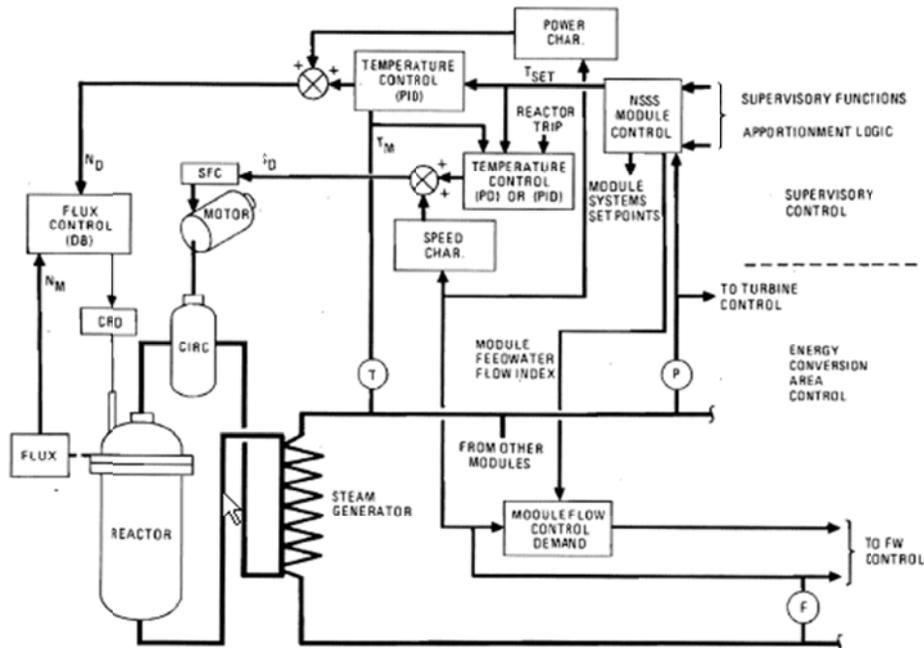


Fig. 23. NSSS control subsystem functions and interfaces.

[HTGR-86-024, Preliminary Safety Information Document for the Standard MHTGR]

The NSSS control subsystem provides startup/shutdown, normal operation, refueling, shutdown, and abnormal operation functions.

NSSS startup/shutdown

Startup/shutdown covers operating conditions in the 0–25% module load range. The NSSS control system has the capability of allowing the hot water and steam from startup and shutdown operations to bypass the main turbines and passed to a flash tank. Each module has its own bypass.

While in startup or shutdown, the module main steam isolation check valve is closed so that other modules may continue to operate.

Hot water and steam temperatures range from 27°C (liquid) to 541°C (superheated steam) by the NSSS control subsystem control of reactor power and circulator speed. Once at temperature, the pressure is raised slightly above the main steam header pressure through a slow closure of the bypass valve and a slow opening of the isolation check valve.

Special NSSS control loop gains are used during startup and shutdown to allow automatic control with outlet steam conditions below rated values and feedwater flow less than 25%. Automatic control is maintained during final stages of steam generator and turbine warmup during startup and in the initial stage of steam generator cooldown during shutdown. Except for certain safety checks, operation is fully automated.

NSSS normal operation

Main steam header pressure response is fast relative to reactor module thermal response during normal operation, so that pressure changes are typically small. Because of the main steam header pressure controller compensation speed, pressure response is largely decoupled from steam temperature in transient conditions. Main steam temperature is controlled by manipulating reactor power and circulator speed. Even in large load changes, main steam temperature deviations are negligible an hour later.

Following a trip of a reactor module, special steam temperature controls limit thermal transients in the steam generator by ramping down the main steam temperature setpoint at $0.2^{\circ}\text{C}/\text{s}$ down to the saturation temperature, then transferring the circulator speed to normal feed forward demand through a linear ramp with 30-s time constant. The time to transfer heat from the primary to secondary system is tightly controlled by the NSSS control subsystem. The NSSS control subsystem has runback and bypass functions to allow operation of remaining reactor modules in case of trips in others. If one or more reactor trips occur, the feedwater flow to the tripped modules is ramped back to 15% in less than a minute. Simultaneously, the PSCS reacts and causes the turbine load to also ramp back, making the turbine load compatible with the loss of flow from the tripped modules.

Figures 24 and 25 show MHTGR module response to a reactor trip and turbine trip, respectively.

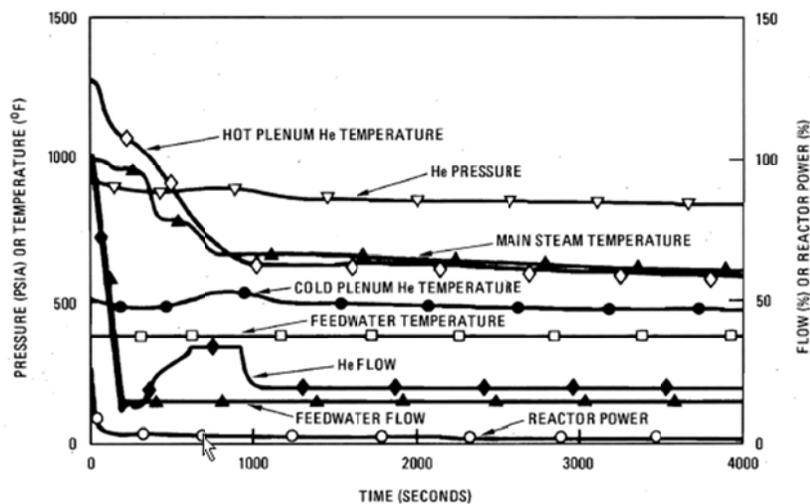


Fig. 24. MHTGR module response to reactor trip.

[HTGR-86-024, *Preliminary Safety Information Document for the Standard MHTGR*]

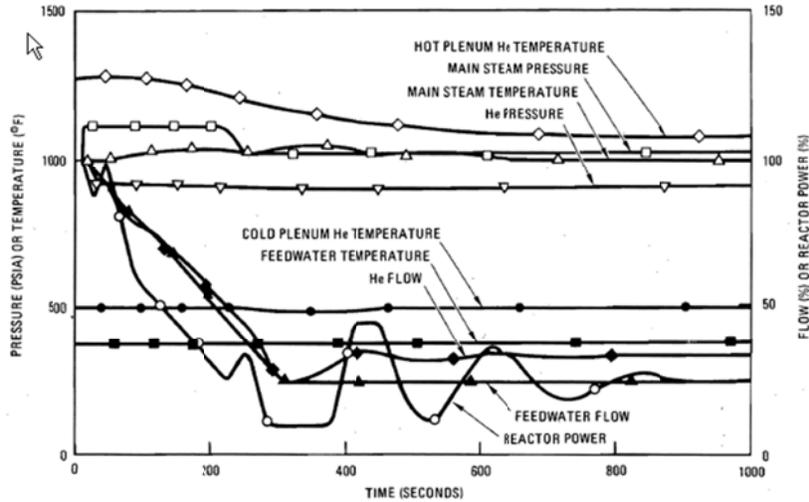


Fig. 25. MHTGR module response to turbine trip.

[HTGR-86-024, *Preliminary Safety Information Document for the Standard MHTGR*]

Energy conversion area control subsystem

The energy conversion area control subsystem provides monitoring and control for electrical power generation. The data management subsystem provides the data communication between the subsystems.

The plant control systems are to provide complete, computerized, automatic control of the plant using hardware platforms characterized as redundant and fault tolerant.

The NRC staff voiced several concerns during their review of the preapplication safety information document to be examined in more detail when the real application is submitted. These included: (1) the interconnected control of the four reactor modules and two turbine generators, since this is a configuration new to the industry with the goal of maintaining some power production even with the shutdown of a reactor module or a turbine generator; (2) isolation between the normal plant control system and the safety-related plant protection and instrumentation system; and (3) failures of the nonsafety control systems that put the plant outside of event category II sequences. The NRC staff concluded that the design could be implemented in an acceptable manner.

4.2.4 Miscellaneous control and instrumentation group

The miscellaneous control and instrumentation group systems provide additional data to the operator and for retention. These systems are (1) the NSSS analytical instrumentation system, (2) radiation monitoring system, (3) seismic monitoring system, (4) meteorological monitoring system, and (5) the first detection and alarm system. The NRC concluded that further review of these nonsafety-related systems was not needed for the pre-application design review stage.

4.2.5 Safety evaluation

The MHTGR was designed to be a safe, economical plant that follows principles of defense-in-depth in meeting requirements from its plant owners and the regulator. The discussion that follows is summarized

from the applicants' assessments as described in the Conceptual Design Summary Report for the MHTGR.¹⁸ The function of protection systems in the safety evaluation is discussed.

Four goals of the plant design were established:

- Goal 1: maintain safe plant operations,
- Goal 2: maintain plant protection,
- Goal 3: maintain control of radionuclide release, and
- Goal 4: maintain emergency preparedness.

In recent history, other gas-cooled reactors have been highly successful in complying with NRC requirements for Goals 1 and 2. The applicant noted that the MHTGR was also designed to use similar high-quality fuel so that radionuclide release probabilities and amounts are low during normal operation or accident situations. To accomplish Goal 3, radionuclides are to be retained within the fuel pellets, with high confidence and with minimal reliance on active safety systems or operator actions. This is to be accomplished by the specification of the size of the reactor core, its shape, and power density. The vessel type also plays a principal role in the elimination of active systems to remove decay heat under both pressurized and depressurized conditions. The particle fuel coatings also effectively retain fission products under a wide range of accident conditions, serving as the primary containment boundary for fission products. Thus, assurance of safety is based on assurance of fuel particle integrity. If this is proven, secondary mitigation measures or barriers are not necessary under normal or accident conditions. That is, assuring the integrity of the fuel particles ensures that safety criteria are met and can reduce the requirements associated with Goal 4.

The MHTGR includes analysis of structures and components for an operating basis earthquake of 0.15 g and a safe shutdown earthquake of 0.3 g for a range of soil types varying from uniform rock with a high shear wave velocity, soft soil with a low shear wave velocity, to a varying condition with softer soil at the surface and harder soil below. Site specific analyses will be required but are expected to be bounded by the conditions above. Effects on the reactor silo and vessel system, reactor core and core supports, and reactor cavity cooling system structures and components were assessed, and the plant was concluded to possess adequate seismic capability down to an event frequency of 5E-7 per year.

The MHTGR has been analyzed to assure the adequacy of the design to control accidental radionuclide releases to within the limits of regulatory criteria, including EPA's Protective Action Guide (PAG) limits. Design basis events (DBEs) were specified and evaluated that considered the mechanistic response of the plant. These serious, but rare, events might be expected over the lifetimes of several hundred like plants, but would be highly unlikely at any one plant. Nonmechanistic responses known as safety-related design conditions (SRDCs) are also considered in which DBEs are analyzed without taking mitigating effects of nonsafety-related types into account.

The safety performance of the MHTGR is based on the ability of TRISO coated particle fuel to effectively retain fission products. This is assured if functions to control heat generation, remove core heat, and protect against chemical attack of the fuel are maintained during normal operation and under transient conditions represented by DBEs and SRDCs.

4.2.5.1 Control heat generation events

The ability to control heat generation was evaluated through two events: (1) loss of normal cooling from the heat transport system with a failure to scram and (2) unplanned control rod withdrawal of an outer reflector control rod group of three rods.

¹⁸*Conceptual Design Summary Report Modular HTGR Plant (Reference Modular High-Temperature Gas-Cooled Reactor Plant, DOE-HTGR-87-092, September 1987.*

For the loss of normal cooling event, the core temperature rises which causes the reactor to go subcritical due to the negative fuel temperature coefficient. Core power drops to about 33% in less than 1 minute. The reserve shutdown system actuates after about 56 seconds due to core power/circulator speed ratio exceeding its trip point for 50 seconds. The reserve shutdown system quickly reduces core power to decay heat levels. With no forced circulation, decay heat causes core temperatures to rise to a peak maximum temperature of 1296°C after almost 4 days. System pressure peaks at about 1009 psia, which is below the actuation pressure for the pressure relief system. In this example, the pressure boundary integrity is retained, temperatures are below the onset of fuel particle failure, and no radionuclides are released.

For the unplanned control rod withdrawal, core power increases and core temperature rises. The negative fuel temperature coefficient counteracts the reactivity increase from the rod withdrawal. A reactor trip occurs after about 99 seconds on high core power/flow ratio and outer rods drop. Peak core power is about 147% at about 100 seconds. During this excursion, fuel temperature peaks at about 1394°C, which is below the threshold of fuel damage. There are no radionuclide releases.

4.2.5.2 Control core heat removal events

A depressurization accident is the limiting event for challenging the ability to remove core heat. A helium leak of 12.7 square inches located at the top of the steam generator vessel corresponding to a pressure relief train is assumed. The primary system depressurizes in minutes. After about 20 seconds, a reactor trip signal is received on low pressure. The nonsafety related shutdown cooling system is assumed to fail. Heat is removed from the core by radiation and conduction to the reactor vessel and from there by radiation and convection to the reactor cavity cooling system panels and from there to the environs via natural circulation. This is an entirely passive cooling process. No systems actively operate or change state.

Because of the thermal inertia of the core, maximum core temperatures occur after about 80 hours. Figure 26 shows the effect of this transient on core temperatures. The maximum fuel particle temperature is just over 1600°C. After about 80 hours, the core heat removal exceeds the core heat generation and the reactor core begins cooling. Fuel particle temperatures remain below the point at which gross failure of the silicon carbide layer occurs; however some fuel particle failure is expected above 1600°C. For this example, there is a loss of the primary system pressure boundary and leakage of fission products to the reactor building and the environs. Approximately 160 curies of ^{131}I , the limiting radionuclide, are expected to be released from the core. Approximately 26 curies are expected to be released to the reactor building. Approximately 1 curie is expected to be released to the environment. The cumulative offsite dose to the thyroid of a person at the exclusion area boundary of the plant is estimated to be 0.36 rem at 30 days. (The 10 CFR 100 limit is 300 rem; the PAG limit is 5 rem.)

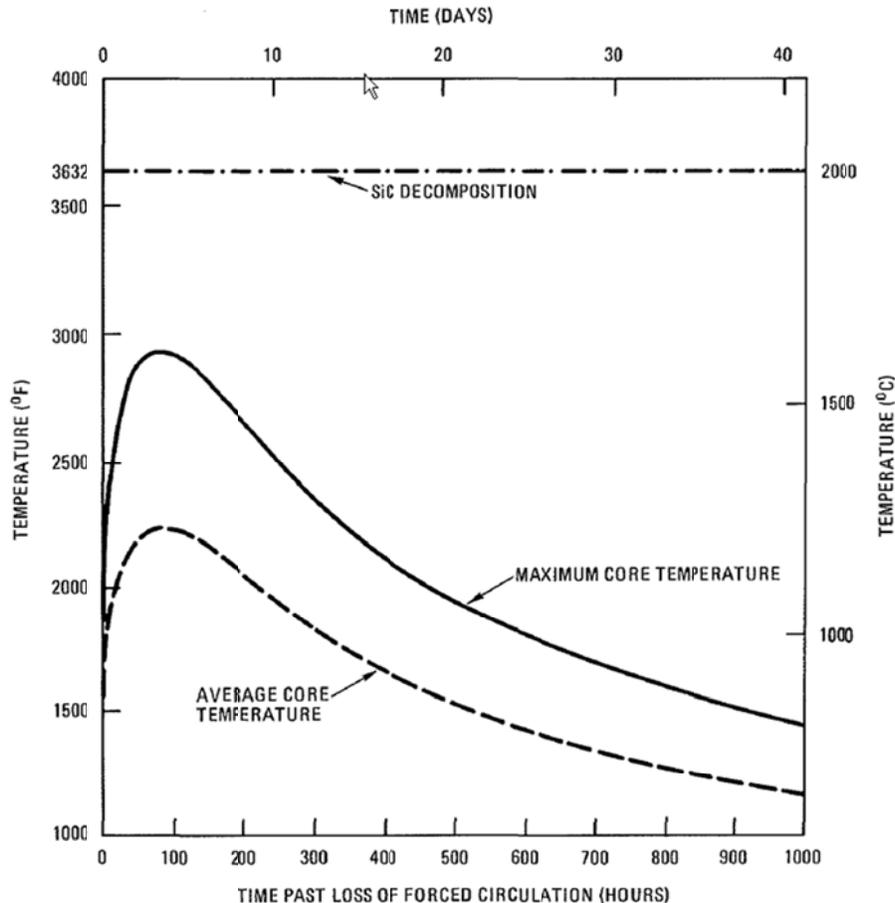


Fig. 26. Core temperatures during depressurized conduction cooldown.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

4.2.5.3 Control chemical attack events

The limiting event for controlling chemical attack is a depressurized conduction cooldown with moisture ingress. This could occur if a steam generator tube ruptures. After the tube rupture, a high-power/flow ratio limit is exceeded as a result of a power increase resulting from the moisture entering the core, which causes a reactor trip. The nonsafety-related moisture monitoring system is assumed to fail. Primary system pressure increases, and a reserve shutdown system actuation occurs on high pressure. The nonsafety-related shutdown cooling system is assumed to fail. The main coolant system and the steam generator isolate automatically; however, the steam generator dump system is assumed to fail, which provides a source of about 9000 lbm of steam to the primary system. The heatup of moisture in the primary system in the core causes primary system pressure to increase which activates the pressure relief system about 6 minutes into the accident. The relief valve is assumed to cycle once or twice and then fail open, resulting in a depressurized system.

The graphite core components, including the fuel, are subject to chemical attack from the moisture. This occurs mostly in the hotter lower sections of the core; however, oxidation is not expected to be enough to create concerns with structural integrity. Some fission products are expected to be released from fuel particles that have defective coatings and undergo hydrolysis. Fission product release is also expected due to coating degradation from high temperatures. The fission products migrate to the reactor building and

environs. Iodine-131 is again the limiting radionuclide. In this accident, about 50 curies are estimated to be released to the reactor building and about 5 curies are expected to be released to the environment. The cumulative offsite dose to the thyroid of a person at the exclusion area boundary of the plant is estimated to be 4.8 rem at 30 days. (The 10 CFR 100 limit is 300 rem; the PAG limit is 5 rem.)

Probabilistic risk assessment (PRA)

A PRA of the MHTGR was conducted. The applicant stated that the expected reactor behavior is “extraordinarily benign,” with limited offsite releases predicted even for extremely unlikely accidents. The design met risk limits of NRC safety goals with substantial margin. The design met user requirements “of no need for public sheltering or evacuation based on the Protection Action Guideline (PAG) does for emergency planning.”¹⁹ Accident frequencies of greater than one per 10⁷ years were considered. External events such as loss of offsite power and earthquakes that could affect multiple plant systems were included in the PRA. The methodology included initiating event selection, event trees, fault trees, common mode failures, transient radionuclide transport and dose, and uncertainty analysis.

The PRA indicated that the overall safety of the MHTGR, which relies on passive features and high integrity fuel, is not dependent on active systems and operator responses. The applicant noted that “no accident scenarios of meaningful probability were identified that could compromise the fuel and lead [to] gross releases.”²⁰ Radionuclide releases in all cases stemmed from manufacturing defects in the fuel made apparent in stresses during accident conditions.

Figures 27 and 28 are dose curves for the whole body gamma dose and thyroid dose consequences, respectively, at the exclusion area boundary showing the probability of exceeding specified doses considering all release categories for four accident types:

- DF: forced convection cooldowns under dry conditions.
- WF: forced convection cooldowns under wet conditions,
- DC: conduction cooldowns under dry conditions, and
- WF: conduction cooldowns under wet conditions.

¹⁹*Ibid.* p. 8–15.

²⁰*Ibid.* p. 8–16.

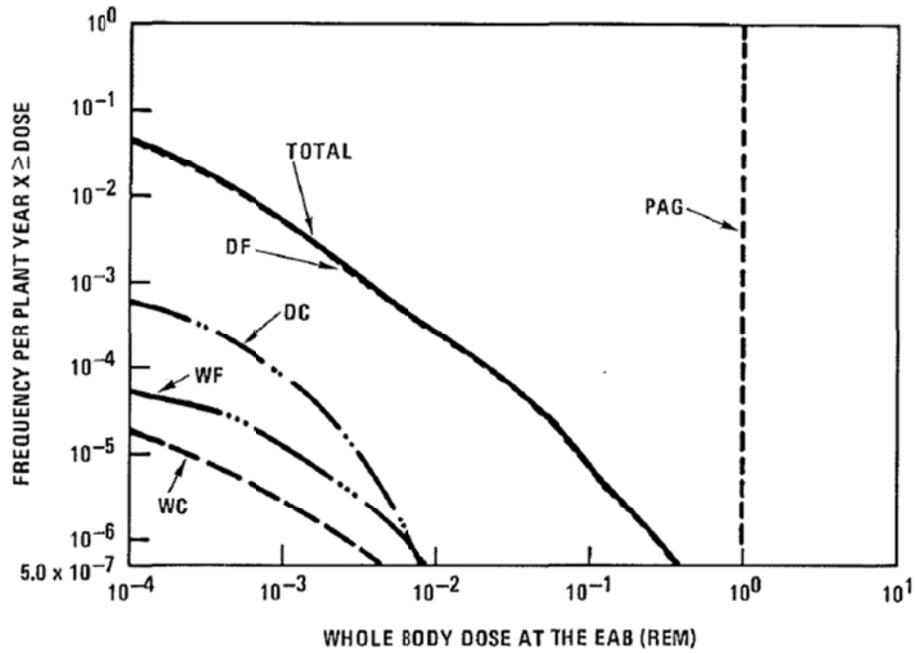


Fig. 27. Cumulative frequency for whole body dose.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

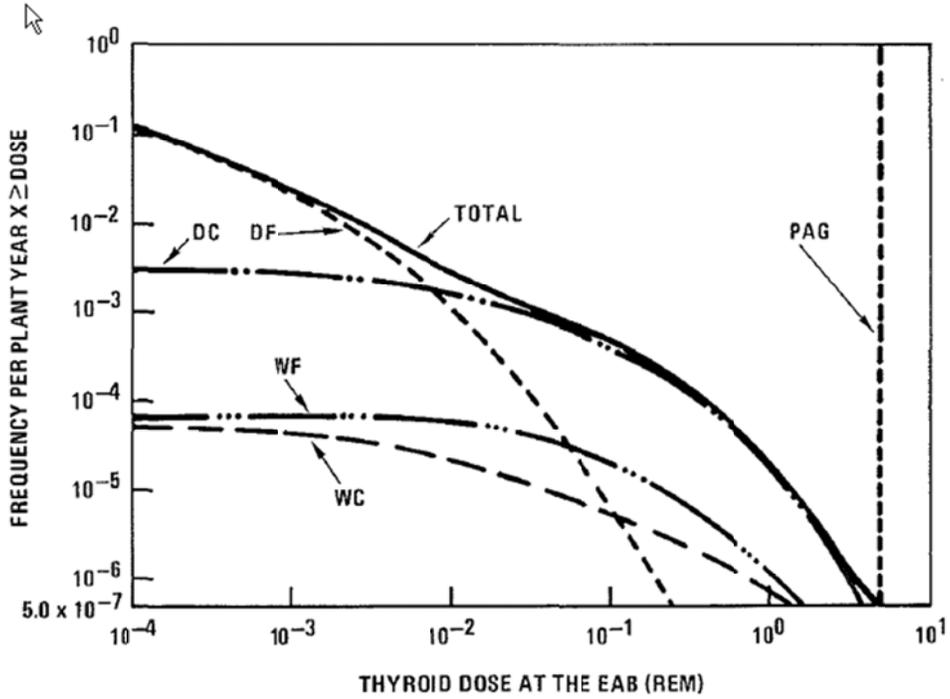


Fig. 28. Cumulative frequency for thyroid dose.

[DOE-HTGR-87-092, *Conceptual Design Summary Report Modular HTGR Plant*]

Figure 27 shows that an accidental release resulting in a whole body gamma dose at the exclusion area boundary above the 1 rem PAG limit is a rare occurrence, with an expected frequency less than 5×10^{-7} per year. For the thyroid, the dose is expected to be less than the 5 rem PAG limit, a rare occurrence with about the same frequency.

4.2.6 Concerns from a regulatory perspective

A Pre-Application Safety Information Document (PSID) for the MHTGR²¹ was first submitted to the NRC in 1986 to foster a concurrent sharing of design information and regulatory concerns early in the design process, so that potential regulatory concerns that resulted in design modifications could be made early on, and to inform NRC staff of areas in which regulatory infrastructure may need to be developed or strengthened. This document was amended many times to address questions or comments from NRC staff and to make improvements to the design.

The NRC staff performed a review of the PSID to identify potential licensability issues associated with the preliminary design and documented their review in a draft pre-application safety evaluation report in 1989.²² Subsequently, the Commission made policy decisions on advanced reactors and additional applicant reports to address technical issues about the MHTGR design. A revised draft of the Pre-Application Safety Evaluation Report was published in December 1995 to reflect these additional developments.²³ A summary of the licensability and policy issues noted in this NUREG will be discussed briefly. The NRC staff also commented on the applicant's proposed technology development plan for issues that were not resolved at the time of the pre-application submittal or during its review. These conclusions will also be noted briefly.

Nine licensability issues for the MHTGR were noted in the 1995 PSER. They are:

- *Fuel performance*—The MHTGR fuel is very similar to the fuel used for Fort St. Vrain; however, the applicant specified a much higher level of fuel performance for the MHTGR. Fuel performance is an integral element of the plant's safety. Its quality and performance must be demonstrated for NRC staff to make a determination on the fuel.
- *Fission products transport computer codes*—The staff noted that additional work will be needed to satisfy their concerns regarding modeling of fission product transport pathways.
- *Source term*—The source term is interrelated with fuel performance, fission product transport, and containment performance in accident dose estimates. The staff requested additional work in this area.
- *Unconventional containment*—The containment for the MHTGR will not be the conventional, leak-tight, light-water reactor containment. High containment pressures will be relieved by direct venting to the atmosphere, with the expectation that there will be few fission products released due to the fuel particle fission product containment capability. The staff requested additional information on the containment performance under certain accident conditions.
- *Safety classification of systems*—The NRC staff noted a number of systems it believed should be classified as safety systems. This issue may be resolved during the design acceptance review.

²¹*Preliminary Safety Information Document for the Standard MHTGR*, HTGR-86-024, February 1989 (Amendment 10).

²²*Draft Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG 1338, February 1989.

²³*Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, December 1995.

- *Completely passive system for ultimate heat sink*—The RCCS is a completely passive system and unique in the industry (at the time of the pre-application review). The staff noted their concerns on the reliability and capability of this single system to ensure core cooling. There may also be post-9/11 vulnerabilities; for example, the close proximity of all RCCS intakes and exhausts may make them more vulnerable to attack.
- *Reactor vessel neutron flux embrittlement*—Potential neutron flux embrittlement of reactor vessel is a staff concern.
- *Reactor vessel elevated service temperature*—The staff is concerned that certain loss of forced coolant flow or conduction cooldown events could result in exceeding the reactor vessel and appurtenances materials temperature limits. At the time, an ASME code case inquiry was submitted to the ASME Code Committee, which would have to be reviewed and approved by the NRC staff. The staff expressed concerns on the expected frequencies of high-temperature events.
- *Applied technology designation*—The staff noted that the applied technology designation of much of the MHTGR technology raised legal and policy issues for the NRC. In the intervening years, HTGR documents have had the applied technology classification generically removed. This may be a minor issue now.

The staff noted that the fuel performance issue was of principal importance (as well as the applied technology designation). Several of the other concerns follow from the concern with fuel performance; therefore, if fuel performance is demonstrated, other performance issues would be expected to be demonstrated as well.

Advanced reactor designs, including the MHTGR and evolutionary LWR designs, were noted by the NRC staff to have potential policy issues to ensure that they meet the same level of safety or protection as current LWRs. Advanced reactor design issues applicable to the MHTGR are:

- accident selection and evaluation,
- containment performance,
- control room and remote shutdown area design,
- emergency planning,
- operator staffing and function,
- residual heat removal,
- safety classification, and
- source term.

Several policy issues for evolutionary LWRs and passive advanced LWRs are also potentially applicable to the MHTGR and require further consideration by the applicant. There are:

- anticipated transient without scram,
- control room alarm reliability,
- control room habitability,
- common mode failures in digital I&C systems,
- definition of passive failures,
- electric distribution,
- equipment survivability,
- fire protection,
- industry codes and standards,
- level of detail,
- elimination of operating basis earthquake,
- prototype,
- radionuclide attenuation,

- regulatory treatment of nonsafety systems,
- reliability assurance program,
- role of the passive plant control room operator,
- safe shutdown requirements,
- severe accident design alternatives,
- site specific PRAs and analysis of external events,
- station blackout, and
- tornado design basis.

The applicant noted that several technology development plans were needed to demonstrate the performance and safety claims made in its PSID. Plans to study fuel and fission products, graphite materials, metals, and verify and validate reactor physics issues were proposed.

NRC staff comments on the reactor technology development plan for the MHTGR were principally on the fuel and the performance of the RCCS. The staff was concerned with fuel performance, its manufacture, quality control, and statistics associated with the testing and noted the need for the technology development plan to address these needs. Efforts to demonstrate fuel performance were felt to be too narrowly focused. The staff also noted the need to demonstrate the reliability and performance of the reactor cavity cooling system, possibly by testing a prototype.

4.3 High Temperature Engineering Test Reactor (HTTR)—Japan

4.3.1 Reactor system design

This section provides a summary of the instrumentation and control features of the modular high temperature gas cooled reactor Japanese HTTR design. It discusses the features and operation of the full plant in sufficient detail that the instrumentation and control features of the plant can be understood.

The HTTR^{24,25} is the first HTGR in Japan. It is a helium gas-cooled and graphite-moderated test reactor with 30 MW thermal power and outlet coolant temperature of 850°C at the rated operation and 950°C in high temperature test operation. The HTTR uses pin-in-block type fuel assembly and is capable of demonstrating nuclear process heat utilization. The purposes of the HTTR are establishment of the HTGR and nuclear heat utilization technologies, development and analysis of innovative high temperature new technologies, and demonstration of safe HTGR operations and safety characteristics. Major specifications are shown in Table 9.

²⁴ *Design of High Temperature Engineering Test Reactor (HTTR)*, JAERI 1332, 1994, http://htr.jaea.go.jp/research/jaeri_1332.html.

²⁵ *Present Status HTGR Research and Development*, JAERI, 2004, http://htr.jaea.go.jp/eng/index_top_eng.html.

Table 9. HTTR design parameters

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Thermal Power	30MW
Outlet coolant temperature	850°C/950°C
Inlet coolant temperature	395°C
Fuel	Low enriched UO ₂
Fuel element type	Prismatic block
Direction of coolant flow	Downward flow
Pressure vessel	Steel
Number of main cooling loop	1
Heat removal	Intermediate heat exchanger (IHX) Pressurized water cooler (PWC)
Primary coolant pressure	4MPa
Containment type	Steel containment
Plant lifetime	About 20 years

Current status²⁶

The HTTR achieved initial criticality on November 10, 1998. Power ascension tests were conducted over the next few years. In December 2001, the reactor reached operation at its normal full power (30 MW) and coolant outlet temperature (850°C). In February 2002, the HTTR received its preoperational test certificate (operating permit) from the Japanese government for normal (850°C) operation, after which safety demonstration tests were conducted. The maximum design operating temperature of 950°C was achieved in April 2004. Subsequently, the HTTR received its operating permit for the high temperature (950°C) test operation mode.

Fuel

The HTTR uses prismatic fuel elements of hexagonal blocks. The active core is 2.9 m in height and 2.3 m in diameter. It consists of 30 fuel columns and 7 control rod guide columns. The active core is surrounded by columns for replaceable reflectors, 9 additional control guide columns, and irradiation test columns. Permanent reflectors surround the active core and the replaceable reflector columns. A view of the pressure vessel and core is shown in Fig. 29 below; major nuclear and thermohydraulic specifications are also provided in Fig. 29.

²⁶ Seigo Fujikawa et al., "Achievement of Reactor-Outlet Coolant Temperature of 950°C in HTTR," *Journal of Nuclear Science and Technology*, **41**(12), pp. 1245–1254 (December 2004).

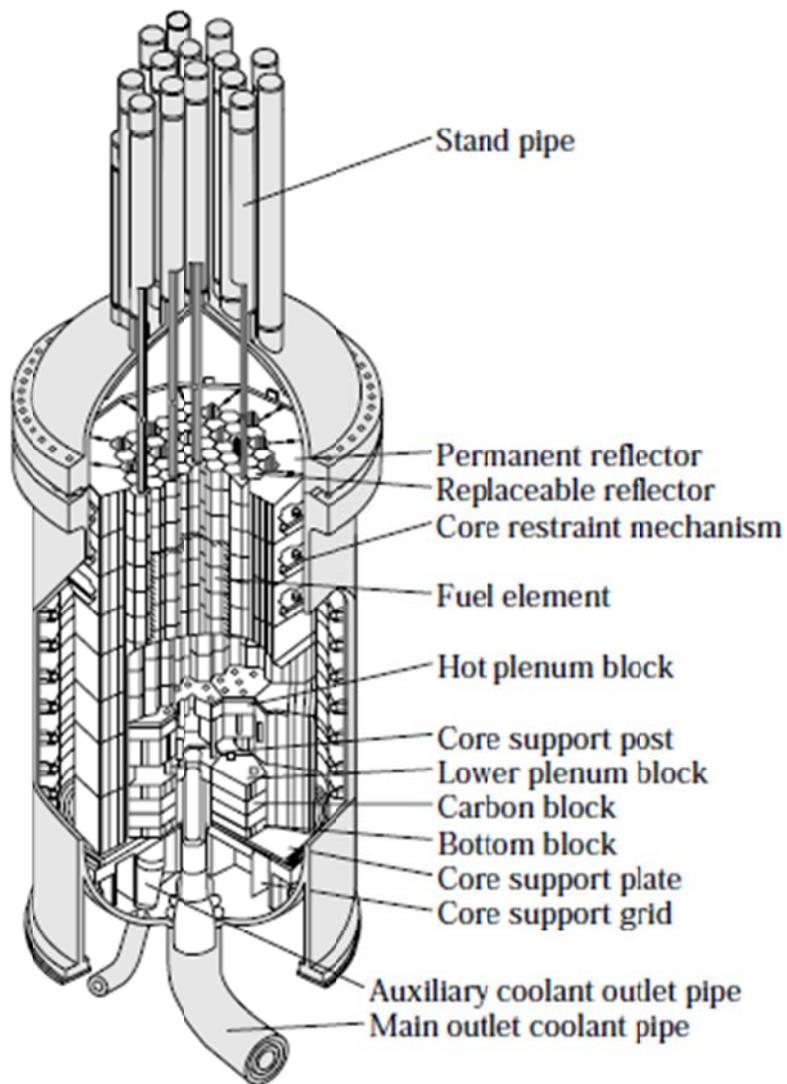


Fig. 29. HTTR pressure vessel and core.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Table 10. HTTR design parameters

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Thermal power	30MW
Core diameter	2.3m
Core height	2.9m
Average power density	2.5W/cm ³
Fuel loading	off-load, 1 batch
Nuclear	
Excess reactivity	15% Δk
Uranium enrichment	3~10wt%
Average	about 6wt%
Fuel burn up (average)	22GW d/t
Reactivity coefficient	
Fuel temperature coefficient	$-(1.5 \text{ to } 4.6) \times 10^{-5} \Delta k/k/^{\circ}C$
Moderator temperature coefficient	$-(17.1 \text{ to } 0.99) \times 10^{-5} \Delta k/k/^{\circ}C$
Power coefficient	$-(2.4 \text{ to } 4.0) \times 10^{-3} \Delta k/k/MW$
Prompt neutron lifetime	0.67~0.70ms
Effective delayed neutron fraction	0.0047~0.0065
Thermal-hydraulic	
Total coolant flow	10.2kg/s (950°C Operation)
Inlet coolant temperature	395°C
Outlet coolant temperature	950°C (Max.)
Power peaking factor	
Radial	1.1
Axial	1.7
Effective core coolant flow rate	88%
Max. fuel temperature	1492°C

Fuel assemblies consist of fuel rods and hexagonal graphite blocks 360 mm across flats and 580 mm in height as shown in the Fig. 30 below. TRISO-coated fuel particles with UO₂ kernels with about 6% by weight average enrichment and 600 μm in diameter are dispersed in the graphite matrix and sintered to form a fuel compact. Fuel compacts are contained in a fuel rod made of graphite that is 34 mm in diameter and 577 mm in length. Fuel rods are inserted into vertical holes in the graphite blocks. Helium gas flows through gaps between the holes and the rods.

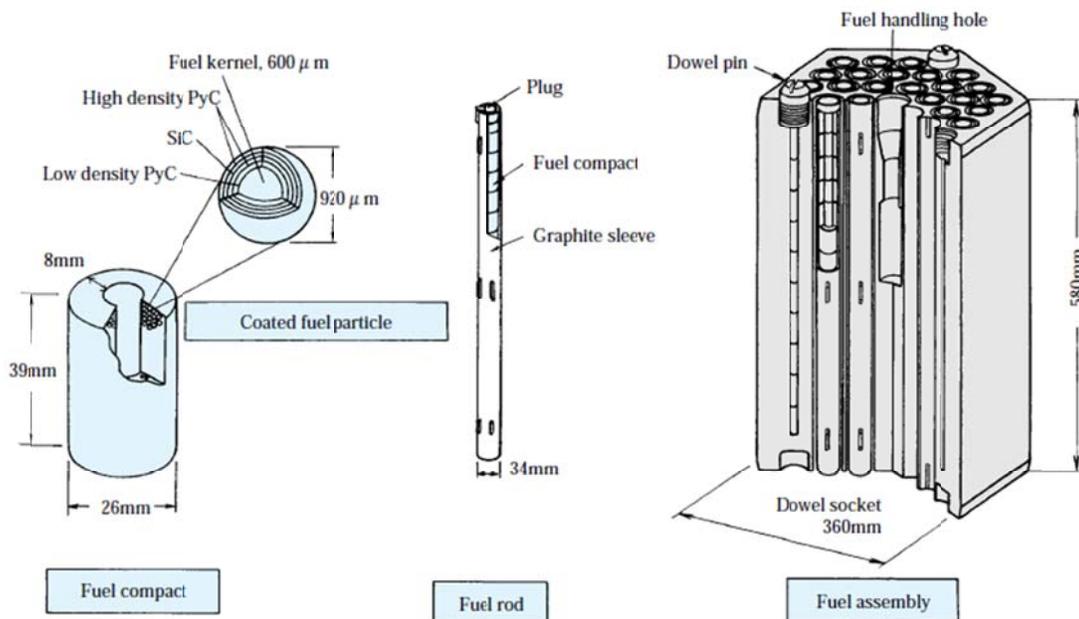


Fig. 30. HTTR fuel.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

A design requirement is for the fuel to retain fission products within the fuel particles to limit their release to the primary coolant during normal operation and abnormal conditions. Fuel temperature is limited to below 1495°C during normal conditions and 1600°C under abnormal transient conditions. Fuel burnup is limited to 33 GWd/t for the first fuel loading. Kunitomi²⁷ reported that fuel temperature limit in excess of 1600°C for anticipated operational occurrences was originally sought but was not approved by the regulatory authority due to lack of experience with the fuel in Japan. Kunitomi also reported that research activities to test fuel at high burnup to confirm fission product retention and demonstrate fuel performance at temperatures higher than 1600°C would be necessary, as well as a better fuel failure model.

Reactor internals

The reactor internals consist of graphite core-support structures, metallic core support structures, and other components as shown in Fig. 31. The graphite support structures consist of hot plenum blocks, core bottom structures, core support posts, etc. The hot plenum blocks provide lateral and vertical positioning and support of the core array. The blocks contain flow paths which guide the primary coolant from the outlet of the fuel columns and distribute it into the hot plenum beneath the hot plenum blocks. The core support posts are designed so as to support the core and hot plenum block arrays which form the hot plenum. The permanent reflector is a graphite structure surrounding the replaceable reflector and control rod guide column located in the circumference of the core. The metallic core support structures are composed of core support plates, a core support grid, and core restraint mechanisms. The core support plate and the core support grid are placed below the thermal insulation layers.

²⁷Kazuhiro Kunitomi and Shusaku Shiozawa, "Safety Design," *Nuclear Engineering and Design*, **233**, pp. 4558 (2004).

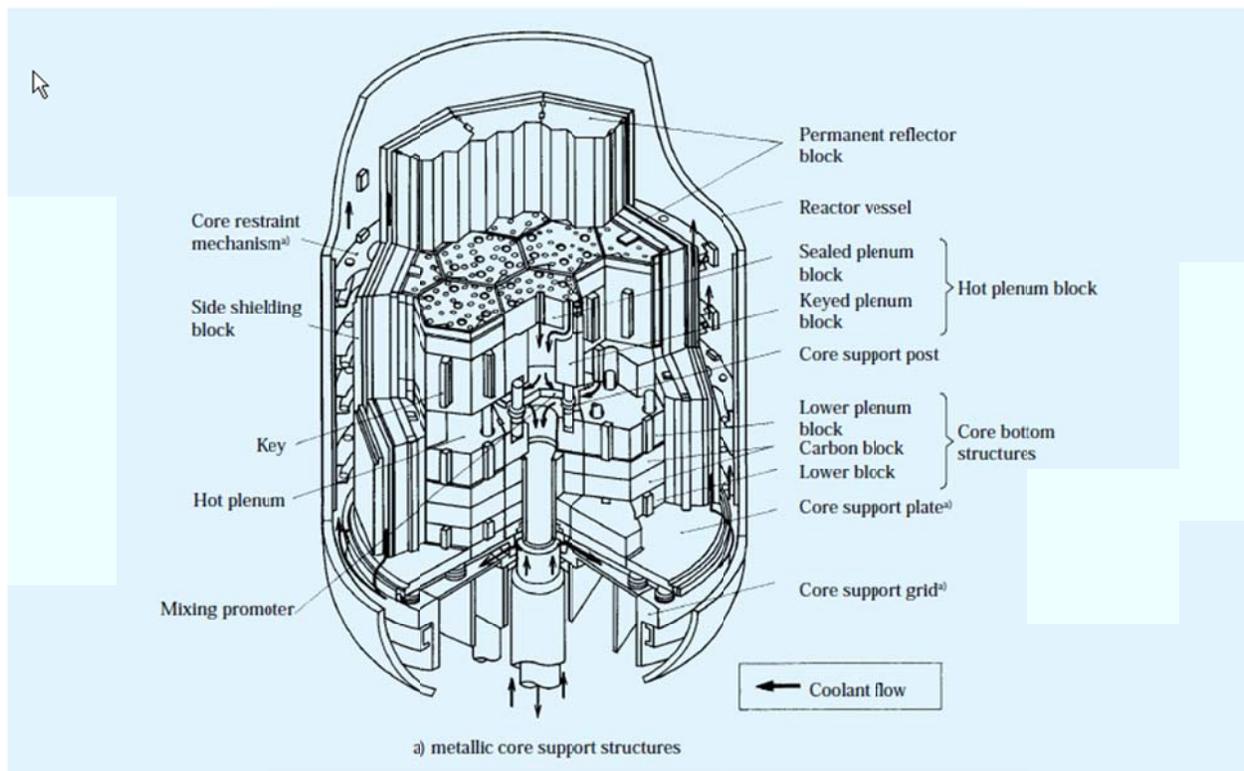


Fig. 31. HTTR reactor internals.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Reactivity control system

A control rod for the HTTR is illustrated in Fig. 32. The control rods are individually supported by control rod drive mechanisms located in stand pipes connected to the hemispherical top lid of the reactor pressure vessel. The control rods are inserted into the channels in the active core and replaceable reflector regions. Reactor shutdown is made by first inserting nine pairs of control rods into the reflector region and then by inserting the other seven pairs of the control rods into the active core region after the temperature there is reduced (typically, 40 minutes later) so that the control rods do not exceed their design temperature limit. If needed, the control rods in the active core region can be inserted immediately; however, if they exceed 900°C they must be replaced before the reactor is restarted. Reserve shutdown capability is provided by insertion of B₄C pellets into the holes in the control rod guide blocks.

Reactivity pressure vessel

The reactor pressure vessel (RPV) shown in Fig. 33 is 13.2 m in inner height and 5.5 m in diameter. It is fabricated from 2-1/4 Cr-1 Mo steel and consists of a vertical cylinder, a hemispherical top lid, and a bottom dome. There are 31 stand pipes for the control rod and irradiation columns welded to the top lid. A stand pipe closure is installed on the top of each stand pipe, which is removed during refueling. Thermal shields are installed on the inner surface of the top lid to protect against high temperatures in accident conditions.

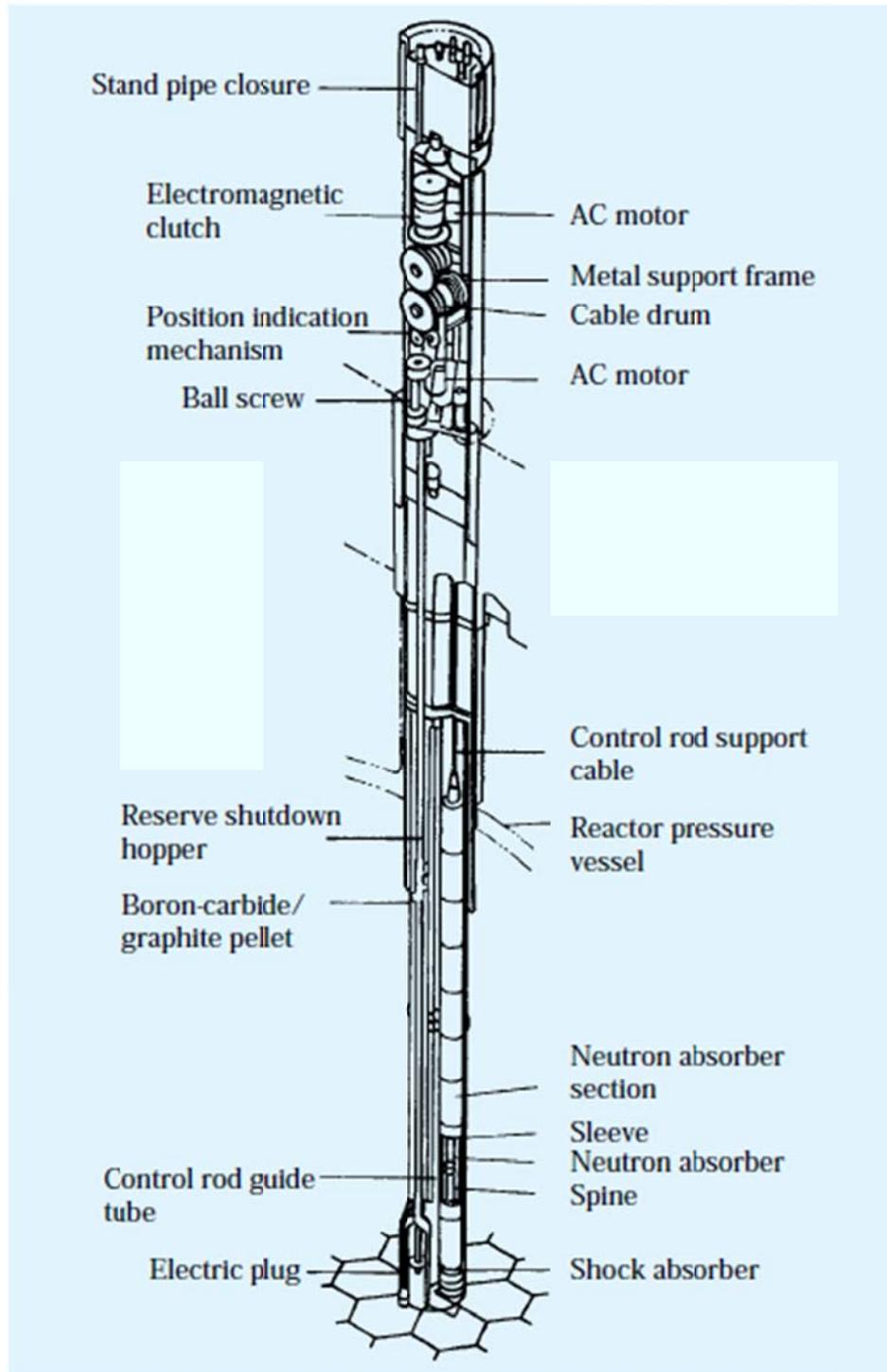


Fig. 32. HTTR control rod.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

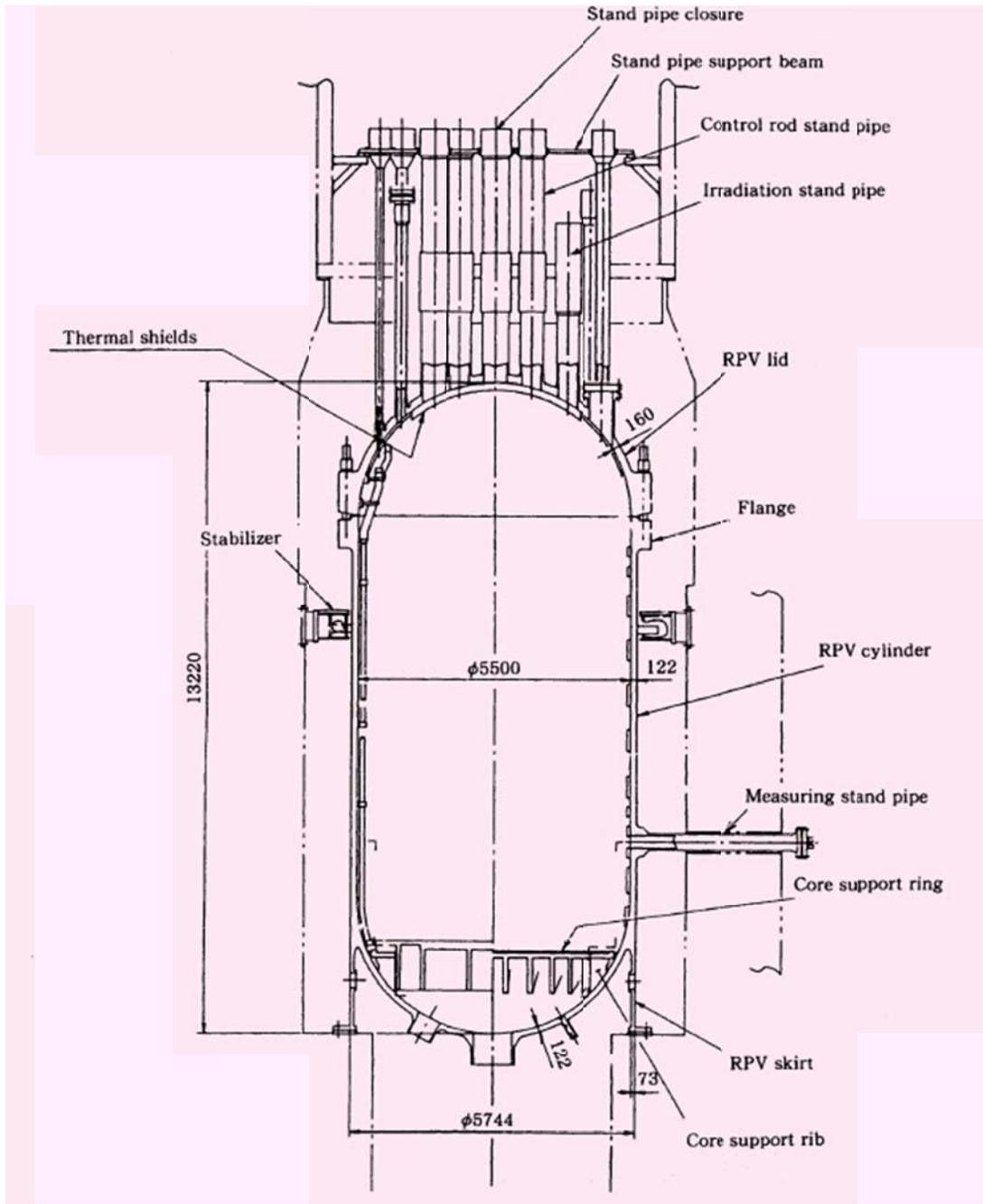


Fig. 33. Reactor pressure vessel.

[JAERI 1332, Design of High Temperature Engineering Test Reactor (HTTR), 1994]

4.3.2 Reactor cooling system

Main cooling system

The main cooling system (MCS) of the HTTR is composed of a primary cooling system (PCS), and secondary helium cooling system (SHCS), and a pressurized water cooling system (PWCS) as shown in

Fig. 34. The PCS removes heat from the core via gas circulators and two heat exchangers—a helium–helium intermediate heat exchanger (IHX) and a primary pressurized water cooler (PPWC). Primary helium gas is transferred from the core to the IHX and the PPWC through a primary concentric hot gas duct. The SHCS, composed of the secondary pressurized water cooler (SPWC) and a gas circulator, removes heat from the primary gas through the IHX. The PWCS consists of an air cooler and water pumps. The air cooler cools the pressurized water for both the PPWC and the SPWC and transfers the heat from the reactor core to the final heat sink, which is the atmosphere. The HTTR is operated in two loading modes. One is a parallel loaded operation in which the IHX and the PPWC are operated simultaneously. Their heat removal rates are 10 MW and 20 MW, respectively. The other is a single-loaded operation in which the reactor is cooled by the PPWC of 30 MW.

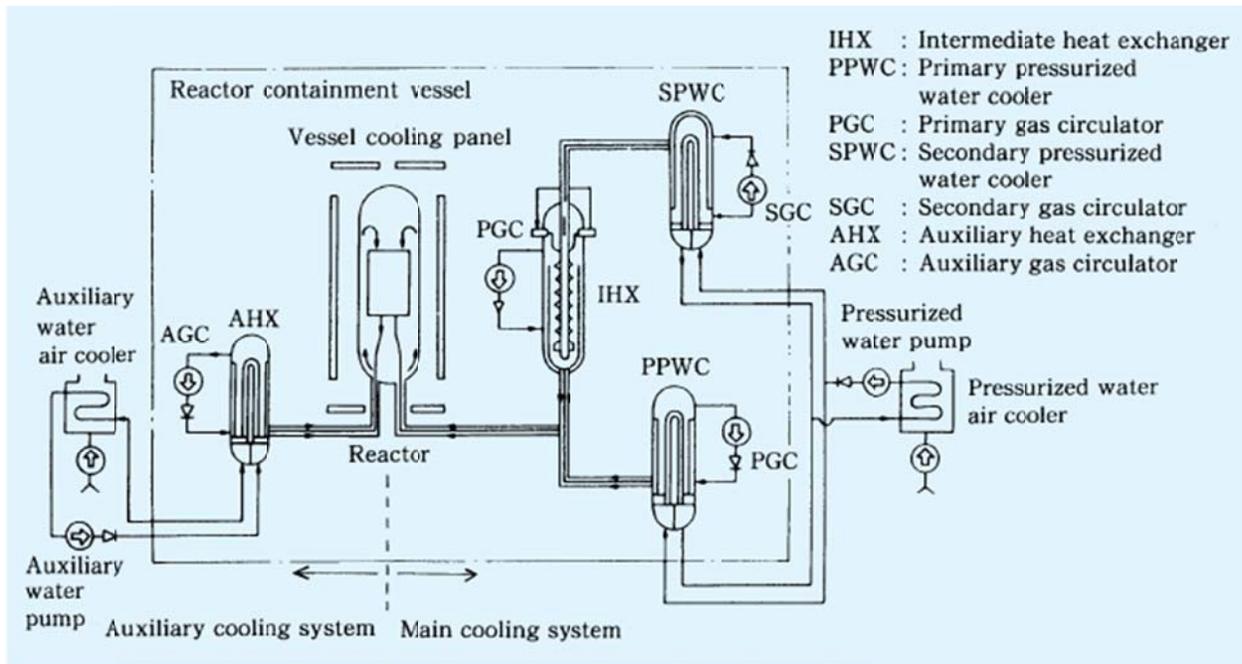


Fig. 34. Main cooling system.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

A need for the capability to detect helium coolant leakage from the primary system promptly was cited (Kumitomi) to prevent small leakage from developing into large leakage. Counting “on-off” movements of a supply valve to determine excessive leakage was the planned approach; the reactor would be shutdown immediately if a high number of valve cycles was observed. Acoustic sensors were attached on primary system components to see if the time differences of correlated sensor data could better locate leakage points. A better system was recommended for future Japanese HTGRs.

Helium purification systems are installed for primary coolant system and the secondary coolant systems. These systems reduce impurities in the coolant, such as hydrogen, carbon monoxide, moisture, etc., and fission products (in the primary system).

High temperature components

The pressure boundaries of the main components, such as the IHX, PPWC, SPWC, an auxiliary heat exchanger (AHX), and the primary concentric hot gas duct, operate at a temperature of about 400°C. The

pressure boundary between the primary and secondary helium gas, such as the liner of the concentric hot gas duct and the heat transfer tubes of the IHX, is in service at a temperature of up to about 900°C. To ensure integrity at high temperatures, high temperature metallic materials are used. Countermeasures to protect against the high-temperature effects and reliable high temperature structural design guidelines were established. Austenitic stainless steels are used for heat transfer tubes of the PPWC, AHX, and SPWC. A heat-resistance superalloy, Hastelloy XR, is used for the heat transfer tubes of the IHX and other reactor coolant boundaries in service at the high temperature level of 950°C. Co-axial double wall structures for high temperature piping and shells of the heat exchangers separate the heat resisting and pressure retaining boundaries in order to reduce the temperatures of the pressure retaining boundary. Also, a low pressure difference between the primary and secondary coolants is maintained to reduce pressure loads acting on the heat transfer tubes of the IHX.

4.3.3 Engineered safety features

Auxiliary cooling system

The auxiliary cooling system (ACS) consists mainly of the auxiliary heat exchanger (AHX), auxiliary gas circulators, and an air cooler. The system starts automatically when the reactor is scrammed and the MCS is stopped in abnormal events. Core cooling by forced circulation is possible with the ACS. Redundant active components (circulators, water pumps and valves, etc.) are provided.

Vessel, cooling system

The vessel cooling system (VCS) consists of upper, lower, and side cooling panels, heat removal adjustment panels around the RPV, and cooling water circulation systems. The VCS is used as a residual heat removal system when the forced circulation by the MCS cannot be maintained due to the rupture of the inner pipe or both pipes in the concentric hot gas duct. Being an ESF system, there are two complete, independent trains backed up with an emergency power supply.

Containment structure

The containment structure consists of a reactor containment vessel (CV), service area (SA), and an emergency air purification system, which reduce the release of fission products to the environment during postulated accidents. Specifications of the reactor containment vessel are shown in the Table 11. A containment structure was not originally envisioned by the designer (ref: Kunitomi) but this idea was dropped because of the extra time (~2 years) that it would take to support the elimination of the containment vessel. A public acceptance problem with a “no-containment” concept was also foreseen.

Table 11. Containment specifications

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Containment type	Steel containment
Maximum service pressure	0.4MPa
Maximum service temperature	150°C
Major size	
Inner diameter	18.5m
Overall height	30.3m
Body thickness	30mm
Top lid thickness	38mm
Refueling hatch diameter	8.5m
Maintenance hatch diameter	2.4m
Personal air lock diameter	2.5m
Free volume	2800m ³
Material	Carbon steel
Maximum leak rate	Less than 0.1% per day at room temperature and 0.9 times as high as maximum service pressure

4.3.4 Instrumentation and control system

Instrumentation system

The instrumentation system consists of a (1) nuclear instrumentation, (2) control rod position instrumentation, (3) core differential pressure instrumentation, (4) in-core temperature monitoring, and (5) fuel failure detection system.

The nuclear instrumentation system is composed of an in-core wide range power monitoring system (WRMS) and an ex-core power range monitoring system (PRMS) as shown in Fig. 35. The WRMS is used to measure neutron flux from 10^{-8} to 30% of rated power. The system is a postaccident monitor under accident conditions; therefore, the neutron detector was designed for high radiation and temperatures of 600°C. Three fission chambers are installed in the permanent reflector blocks through standpipes and are not exposed to the higher temperatures of the mid-core.

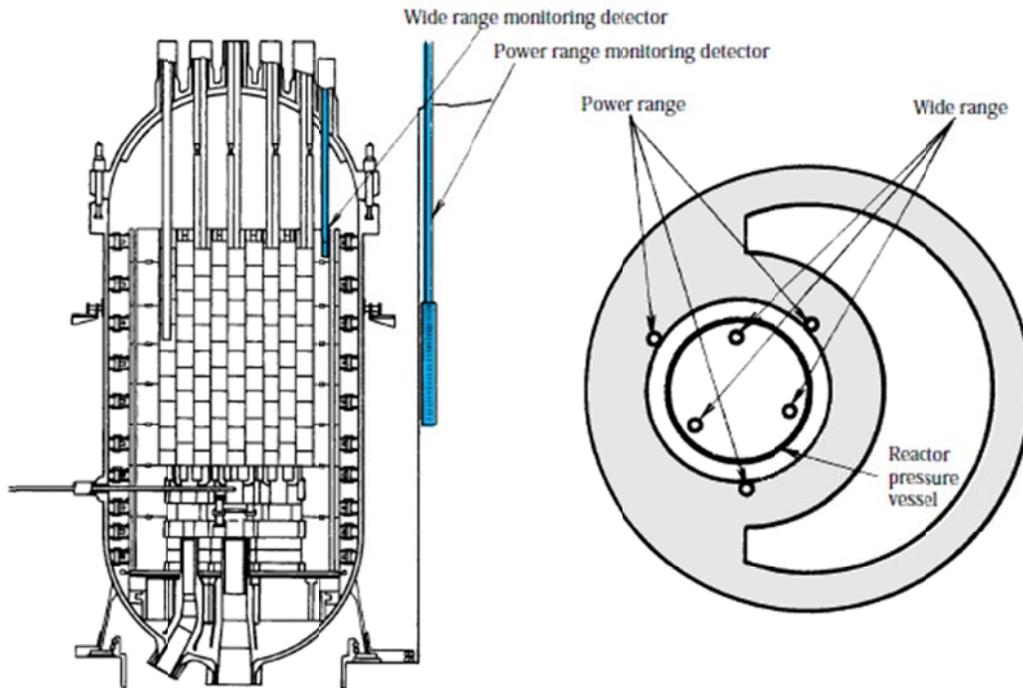


Fig. 35. Nuclear instrumentation.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

The PRMS is used to measure neutron flux from 0.1 to 120% of rated power and is also a sensor for the reactor power control system. Because of the high temperature and high flux level in the core, the detectors are located on the outside of the reactor vessel. The detectors have a high sensitivity to be able to detect neutron flux at a very low level.

The control rod position instrumentation system monitors the position of 16 pairs of control rods. Their position is measured by encoder systems in the control rod drive mechanism. The instrumentation signals are used for the reactor control system and the safety protection system.

The core differential pressure instrumentation detects a decrease in primary coolant flow in the reactor core based on differential pressures between the inlet and outlet of the core. This signal is used for the safety protection system.

The in-core temperature monitoring system uses seven N-type thermocouples arranged in the hot plenum blocks below the reactor core as shown in Fig. 36. (Another article²⁸ states that “Four thermocouples are arranged at each hot plenum block....”) These sensors withstand temperatures above 1000°C; sheath coating materials were developed in order to avoid carburization by carbon deposits. Long-term performance of the thermocouples was not specified.

²⁸Saito et al., “Instrumentation and Control System Design,” *Nuclear Engineering and Design*, **233**, pp. 125–133 (2004).

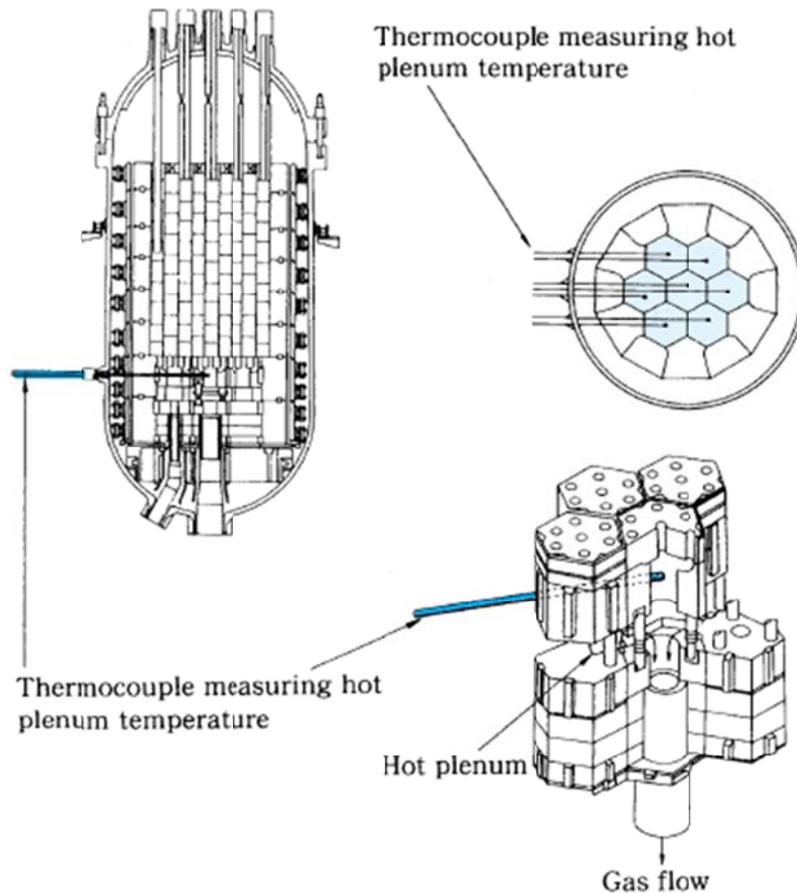


Fig. 36. Nuclear instrumentation.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

The fuel failure detection system is composed of precipitators, a pre-amp, control box, etc. The system is used to detect beta rays radiated from short-lived fission products such as ^{88}Kr , ^{89}Kr , and ^{138}Xe from failed fuel particles. The design requirement for HTTR initial fuel failure fraction in the coating layers of the particle fuel shall be less than 0.2%; the fuel failure detection system is able to detect 0.02% fuel failure.

Reactor control system

The reactor control system of the HTTR is designed to assure high stability and reasonably damped characteristics against the various disturbances during operation. The system consists of the operational mode selector, reactor power control, and plant control systems. The mode switch selects several operational modes, such as rated power operation, high temperature test operation, safety demonstration test operation, irradiation test operation, etc. A plant dynamic analysis of the operating conditions of the HTTR was carried out in order to design plant's control system²⁹ as noted by Saito³⁰. The simulation

²⁹Y. Shimakawa et al., "The Plant Dynamics Analysis Code ASURA for the High Temperature Engineering Test Reactor (HTTR)," presented at the *Specialists Meeting on Uncertainties in Physics Calculations for Gas Cooled Reactors*, Villigen, Switzerland, May 9–11, 1990.

³⁰Kenji Saito et al., "Instrumentation and Control System Design," *Nuclear Engineering and Design*, **233**, pp. 125–133 (2004).

code, ASURA, was used to examine reactor power transients, thermal transients, coolant flow transients and response of the reactor control and protection system.

The reactor power control system consists of the power control and reactor outlet coolant temperature control devices. Per Saito, the signals from each channel of the power range monitoring instrumentation are fed to three microprocessor-based controllers. If there is a deviation, between the process and setpoints, a pair of control rods is signaled to insert or withdraw at variable speed, depending on the deviation. A control rod pattern interlock is used to prevent abnormal power distribution.

The reactor outlet coolant temperature control instrumentation illustrated in Fig. 37 is used at full power. In case of a deviation, the control system gives a demand to the power control system and changes the coolant outlet temperature by moving the control rods.

The plant control system controls the plant parameters such as the reactor inlet coolant temperature, the primary coolant flow rate and pressure, and differential pressure between the PCS and the PWCS or SHCS as shown in the Fig. 38 (from Saito).

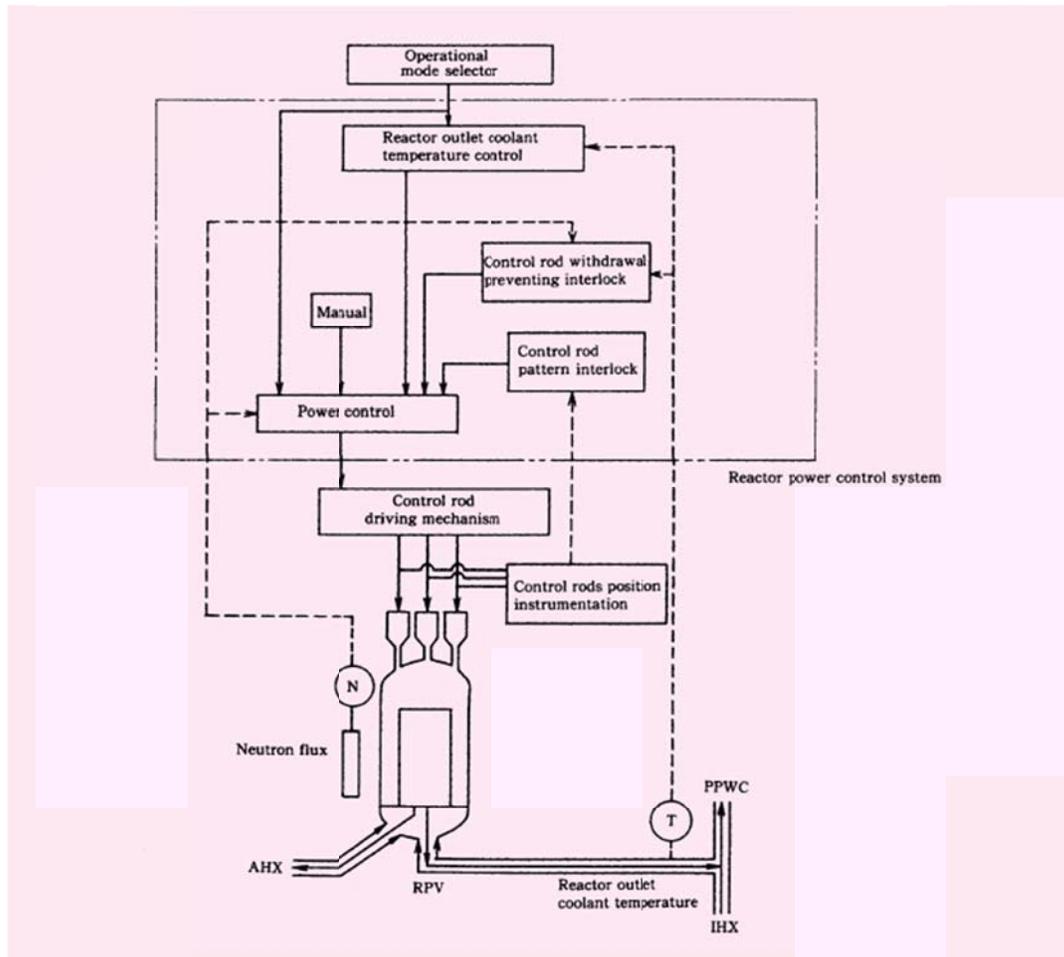


Fig. 37. Reactor coolant outlet temperature control instrumentation.

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

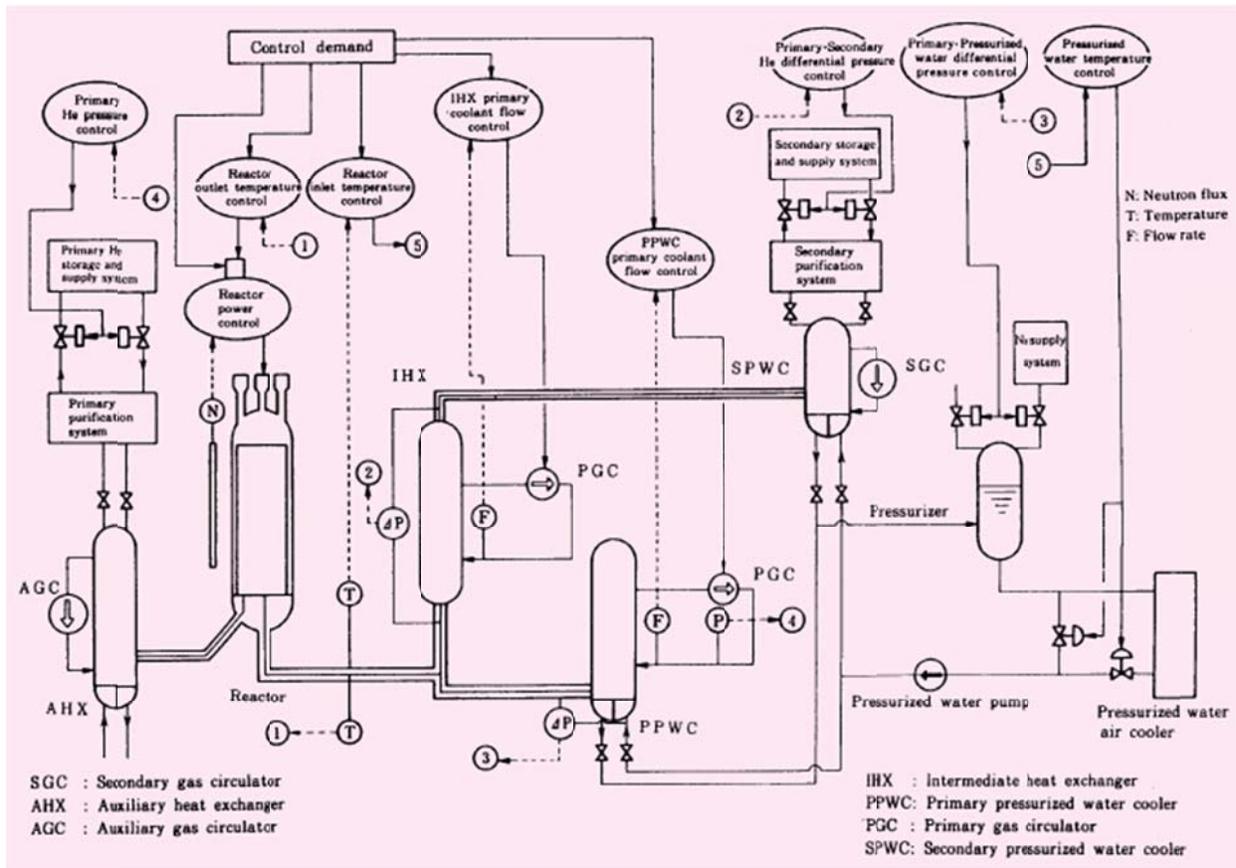


Fig. 38. Reactor coolant outlet temperature control instrumentation.

The reactor inlet coolant temperature control system is used in the power range from 30–100%. It is cascade connected with the pressurized water temperature control system. In case of a deviation, the reactor coolant inlet temperature is controlled by adjusting the pressurized water cooler inlet temperature of the pressurized water. (Saito)

The intermediate heat exchanger primary coolant flow rate control system works by maintaining a constant coolant flow rate in the intermediate heat exchanger by adjusting the helium gas circulator. (Saito)

The primary pressurized water cooler primary coolant flow rate control system maintains a constant value of the primary coolant flow rate in the primary pressurized water cooler by adjusting the three helium gas circulators. (Saito)

The primary helium pressure control system controls the primary helium pressure by cycling the valves of the helium storage and supply system for the primary system. (Saito)

The primary-secondary helium differential pressure control system controls the differential pressure between the primary and secondary helium by cycling the valves of the secondary helium storage and supply system. The secondary system is maintained at a higher pressure than the primary system to prevent release of fission products into the secondary system. (Saito)

The primary pressurized water differential pressure control system controls the differential pressure between the primary helium and pressurized water by cycling valves in the pressurized water system

pressurizer. The pressurized water pressure is maintained lower than the primary helium to prevent water ingress to the primary helium. (Saito)

The pressurized water temperature control system controls the inlet pressurized water temperature of pressurized water cooler by adjusting the flow rate of water in the air cooler by means of a bypass flow control valve and cooler outlet flow control valve. The demand signal is given by the reactor inlet coolant temperature control system. (Saito)

Safety protection system

The safety protection system consists of the reactor protection and engineered safety features actuating systems. It is designed with 2 out of 3 circuit logic and 2 trains. The multiple channels are separated physically as reasonable achievable. Safety protection function is maintained if the signal also provides a reactor control function and the reactor control system malfunctions. The signals in the safety protection system are listed in Table 12 below. The reactor protection system automatically initiates a reactor scram by inserting the control rods. The engineered safety features actuating system is designed to ensure the integrity of the core, the reactor coolant pressure boundary, and the containment vessel pressure boundary against unexpected conditions during abnormal operational transients and accidents.

Table 12. Reactor scram and engineered safety features actuation signals

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Reactor scram signals in reactor protection system		Engineered safety features		Signals	
WRMS	high	CV isolation	CV pressure	high	
PRMS	high		CV radioactivity	high	
IHX primary coolant flow rate	low		Primary/pressurized water differential pressure	low	
PPWC He flow rate	low		Primary purification flow rate	high	
Primary coolant radioactivity	high		SA radioactivity	high	
IHX outlet primary coolant temperature	high		Manual		
Reactor outlet temperature	low		ACS startup	Reactor scram	
Core differential pressure	low	Manual			
PPWC pressurized water flow rate	high	Auxiliary water iso	Primary/auxiliary water differential pressure	low	
Primary/pressurized water differential pressure	low		Manual		
Primary/pressurized water differential pressure	low				
Primary/secondary He differential pressure	large				
Secondary He flow rate	low				
Seismic acceleration	large				
Primary coolant high humidity	high				
Manual					

4.3.5 Safety and demonstration tests planned in HTTR²⁶

The test schedule for safety demonstration tests for the HTTR documented in JAERI-Tech 2005-015 began in 2002 and continued through 2006 as shown in Table 13. The tests included reactivity insertion tests through control rod withdrawal, coolant flow reduction tests by tripping one or more gas circulators, and partial flow loss of coolant tests. Additional tests planned at the time of the JAERI-Tech 2005-0015 report included loss of all forced cooling and loss of vessel cooling.

Table 13. Safety demonstration test schedule

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Fiscal Year	2002	2003	2004	2005	2006
Duration of HTTR Operation for Safety Demonstration Tests					
Safety Demonstration Tests	SR-0: 30% SR-1: 50%	SR-2: 60%	SR-3: 80%	SR-4: 30%	S3C-1, SV-1 <i>will start after obtaining new licences.</i>
<u>Phase I Tests</u> SR: Reactivity Insertion Test SF: Partial Flow Loss of Coolant Test S1C: 1 Gas Circulator Trip Test S2C: 2 Gas Circulators Trip Test		SF-1: 60%	SF-2: 80%	SF-3: 100%	
<u>Phase II Tests</u> S3C: 3 Gas Circulators Trip Test SV: Vessel Cooling System Stop Test	S1C-1: 30%	S2C-1: 30% S1C-2: 60% S2C-2: 60%	S1C-3: 80% S2C-3: 80%	S1C-4: 100% S2C-4: 100% S1C-5: 30%	

4.3.6 Safety evaluation

A negative temperature coefficient of reactivity, large core heat capacity, and inert helium coolant are safety characteristics of the HTTR. Events to be evaluated, design basis events (DBEs), are selected for anticipated operational occurrences (AOOs), accidents, major accidents, and hypothetical accidents. These events include conditions beyond normal operation resulting from a single failure or malfunction, or a single operator error anticipated to occur during the lifetime of the reactor facility, as well as one that may occur with a similar frequency as the above, which may result in unplanned operating conditions. Accidents in this category are beyond AOOs but are considered due to the large release potential of very low frequency events.

Criteria for AOOs are as follows:

- maximum fuel temperature shall not exceed 1600°C;
- maximum reactor pressure boundary pressure shall not exceed 110% of normal maximum pressure in service; and

- maximum temperatures of the reactor pressure boundary shall not exceed 500°C for RPV and primary piping, etc., made of 2-1/4 Cr–1 Mo steel; 600°C for PPWC heat transfer tubes, etc., made of austenitic stainless steel; and 980°C for IHX heat transfer tubes, etc., made of Hastelloy XR alloy.

Some reactor facilities could be damaged by postulated accidents; however, it shall be confirmed that the core has no chance of damage and the barrier against fission product release is designed properly to prevent a spread of the influence of radiation around the site. Criteria for these accidents are:

- The reactor shall not be seriously damaged and sufficient cooling capacity for residual heat removal shall be maintained. Fuel compacts are held in the graphite blocks, and the support post has the strength required to support the core.
- The pressure of the reactor pressure boundary (except for the boundary between the primary and the secondary helium gas) shall be under 1.2 times as high as the maximum pressure in normal service, and the primary/secondary helium gas boundary shall not fail. The IHX transfer tube shall not be in creep buckling.
- Maximum temperatures of the reactor pressure boundary shall not exceed 550°C for RPV and primary piping, etc., made of 2-1/4 Cr–1 Mo steel; 650°C for PPWC heat transfer tubes, etc., made of austenitic stainless steel; and 1000°C for IHX heat transfer tubes, etc., made of Hastelloy XR alloy, per code.
- The pressure on the containment vessel boundary shall not exceed the maximum pressure during normal operation, by MITI (Japan Ministry of International Trade and Industry) standard.
- There shall be no risk of a significant radiation exposure to the public per the guidelines for the reactor siting evaluation.

Abnormal events, which are classified into AOOs and accidents, are summarized in the Figs. 39 and 40.

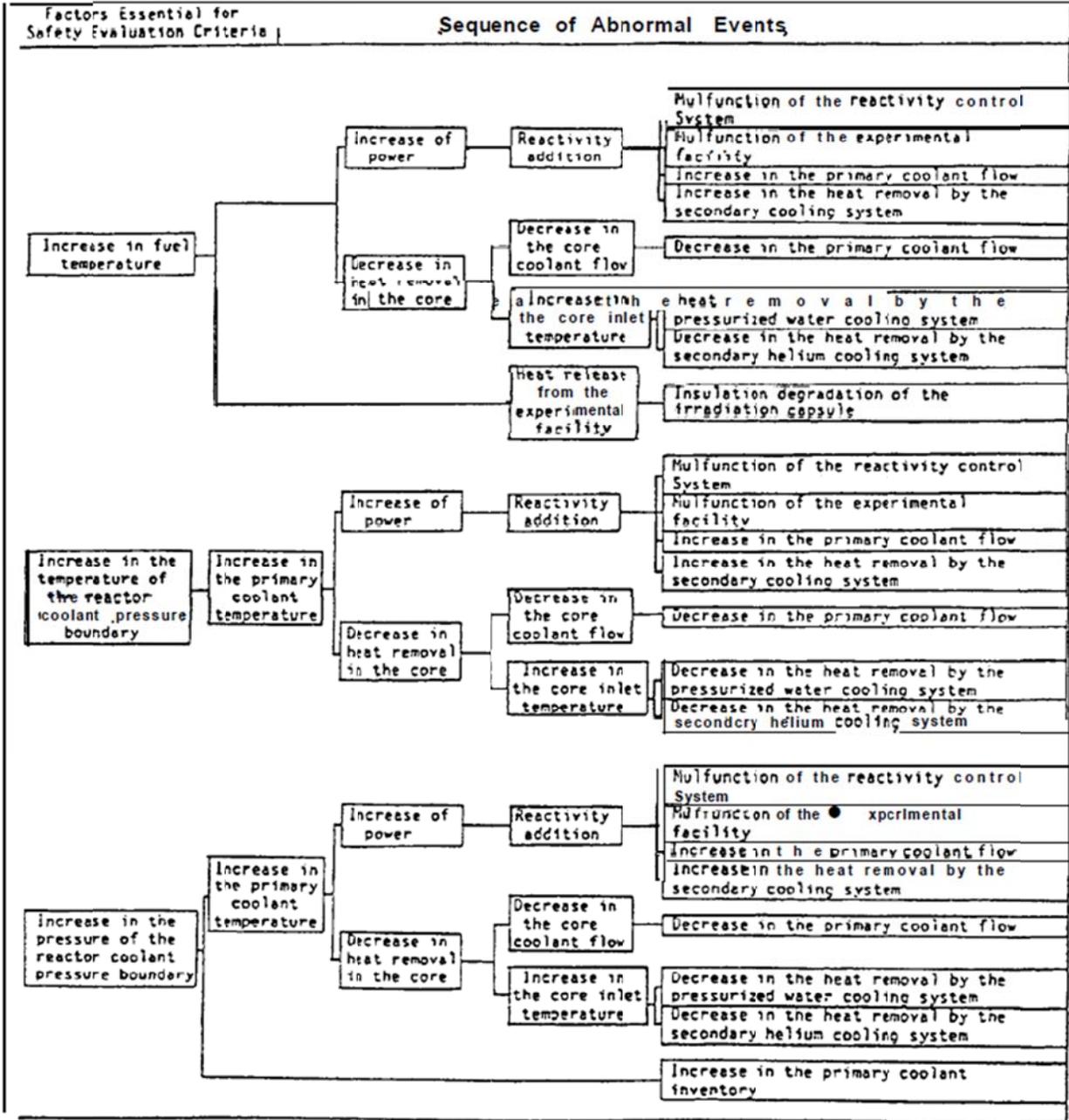


Fig. 39. Sequence of abnormal events.

Table 14. Postulated events classified into AOOs

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

- | |
|---|
| <ul style="list-style-type: none">(1) Abnormal change in the reactivity or power distribution in the core<ul style="list-style-type: none">1) Abnormal CR withdrawal during subcritical condition2) Abnormal CR withdrawal during rated power operation(2) Abnormal change in heat generation or heat removal in core (including abnormal change in pressure or inventory of primary coolant)<ul style="list-style-type: none">1) Decrease in primary coolant flow rate2) Increase in primary coolant flow rate3) Decrease in heat removal by secondary cooling system4) Increase in heat removal by secondary cooling system(3) Loss of off-site electric power(4) Transient during irradiation test(5) Transient during safety demonstration test |
|---|

Table 15. Postulated events classified into accidents

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

- | |
|---|
| <ul style="list-style-type: none">(1) Channel blockage in standard fuel element(2) Failure of inner pipe of the primary concentric hot gas duct(3) Failure of inner pipe of the secondary concentric hot gas duct(4) Rupture of secondary concentric hot gas duct(5) Rupture of pipe in PWCS(6) Rupture of primary concentric hot gas duct (depressurization accident)(7) Failure of PPWC heat transfer tube(8) Failure of primary helium purification system(9) Failure of gaseous radwaste treatment system(10) Failure of sweep gas pipe in irradiation test equipment(11) Channel blockage in fuel failure test specimen(12) Rupture of stand pipe |
|---|

The various AOOs and accidents were evaluated at worst-case operating conditions for these events. Single failures of active systems were also incorporated into the safety analyses. Tables 16 and 17 show the consideration of single failures in the analyses of AOOs and accidents, respectively.

Table 16. Single failures consideration for AOOs

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Events of AOO	System expected to work							
	Reactor protection system	CR system	ACS	VCS	Emergency power feeder	Frequency converter of PGC	CR pattern interlock	Pressurized water pump trip by means of high temperature of PWC inlet pressurized water
Abnormal CR withdrawal during subcritical condition	—	—	—	—	—	—	—	—
Abnormal CR withdrawal during rated power operation	—	—	—	—	—	—	●	—
Stop of PGC for IHX	△	⊙	●	⊙	—	⊙	—	—
Opening of exhaust valve of primary helium storage and supply system	△	⊙	●	⊙	—	⊙	—	—
Increase in revolution of PGC for IHX	—	—	—	—	—	—	—	—
Increase in revolution of PGC for PPWC	—	—	—	—	—	—	—	—
Opening of supply valve of primary helium storage and supply system	△	⊙	●	⊙	—	⊙	—	—
Opening of bypass flow control valve of air cooler	△	⊙	●	⊙	—	⊙	—	△
Opening of exhaust valve of secondary helium storage and supply system	△	⊙	●	⊙	—	⊙	—	—
Increase in heat removal by secondary cooling system	—	—	—	—	—	—	—	—
Loss of off-site electric power	△	⊙	●	⊙	△	⊙	—	—
Abnormal reactivity insertion by movement of irradiation specimen	—	—	—	—	—	—	—	—
Deterioration of insulation material in irradiation capsule	—	—	—	—	—	—	—	—
Transient during safety demonstration test	△	⊙	●	⊙	—	⊙	—	—

⊙ means the system expected to work.

△ means the system of which the work does not influence the result of analysis even if single failure is assumed.

● means the system of which the work influences the result of analysis if single failure is assumed.

Table 17. Single failures consideration for accidents

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Systems or components Events of accident	System expected to work									
	Reactor protection system	CR system	ACS	VCS	Isolation valve of the CV	Isolation valve of the PWCS	Emergency air purification system	Emergency power feeder	Frequency converter of PGC	Ventilation system for experimental equipment
Channel blockage in standard fuel element	—	—	—	—	—	—	—	—	—	—
Failure of inner pipe of primary concentric hot gas duct	△	○	—	●	—	—	—	△	○	—
Failure of inner pipe of secondary concentric hot gas duct	△	○	●	○	—	—	—	△	○	—
Rupture of secondary concentric hot gas duct	△	○	●	○	—	—	—	△	○	—
Rupture of pipe in PWCS	△	○	●	○	—	—	—	△	○	—
Depressurization accident	△	○	—	●	△	—	●	△	○	—
Failure of PPWC heat transfer tube	△	○	●	○	—	△	—	△	○	—
Failure of primary helium purification system	—	—	—	—	△	—	●	△	—	—
Failure of gaseous radwaste treatment system	—	—	—	—	—	—	—	—	—	—
Failure of sweep gas pipe in irradiation test equipment	—	—	—	—	—	—	—	—	—	△
Channel blockage in fuel failure test specimen	—	—	—	—	—	—	—	—	—	—
Failure of stand pipe	△	○	—	●	△	—	●	△	—	—

○ means the system expected to work.

△ means the system of which the work does not influence the result of analysis even if single failure is assumed.

● means the system of which the work influences the result of analysis if single failure is assumed.

Initial conditions for normal reactor operation are shown in Table 18.

Table 18. Initial conditions for normal reactor operation

[JAERI 1332, *Design of High Temperature Engineering Test Reactor (HTTR)*, 1994]

Items		Standard reactor core (High temperature test operation)		Irradiation test core	
		Nominal value	Error	Nominal value	Error
Reactor power		30MWt	±2.5%	30MWt	±2.5%
Primary coolant temperature	Outlet	950°C	±17°C	850°C	±19°C
	Inlet	395°C	±2°C	395°C	±2°C
Primary coolant pressure		41kg/cm ²	±1.5kg/cm ²	41kg/cm ²	±1.5kg/cm ²

4.4 Arbeitsgemeinschaft Versuchsreaktor–AVR

4.4.1 Reactor system design²⁷

The AVR was an experimental reactor which operated from 1967 until 1988 at the Jülich Research Center in the Federal Republic of Germany. The AVR's mission was to demonstrate the concepts and safety features of the pebble bed high temperature reactor design. The AVR was a complete power plant equipped with a turbine generator and was connected to the electrical grid in normal operation. During its operation, a number of key reactor safety experiments were carried out to verify the pebble bed configuration and the inherent safety of the reactor concept, including a depressurized loss-of-forced circulation. The plant was the first demonstration of operation with continuous circulation of the fuel pebbles and online refueling. New fuel designs and fuel manufacturing techniques were tested in long-term service under prototypical power plant operating conditions. A number of advances in TRISO fuel reliability and fission product containment were first demonstrated by operation in the AVR.

The main features of the AVR reactor are shown in Fig. 41 and described in the following paragraphs. The main design parameters are summarized in Table 19.

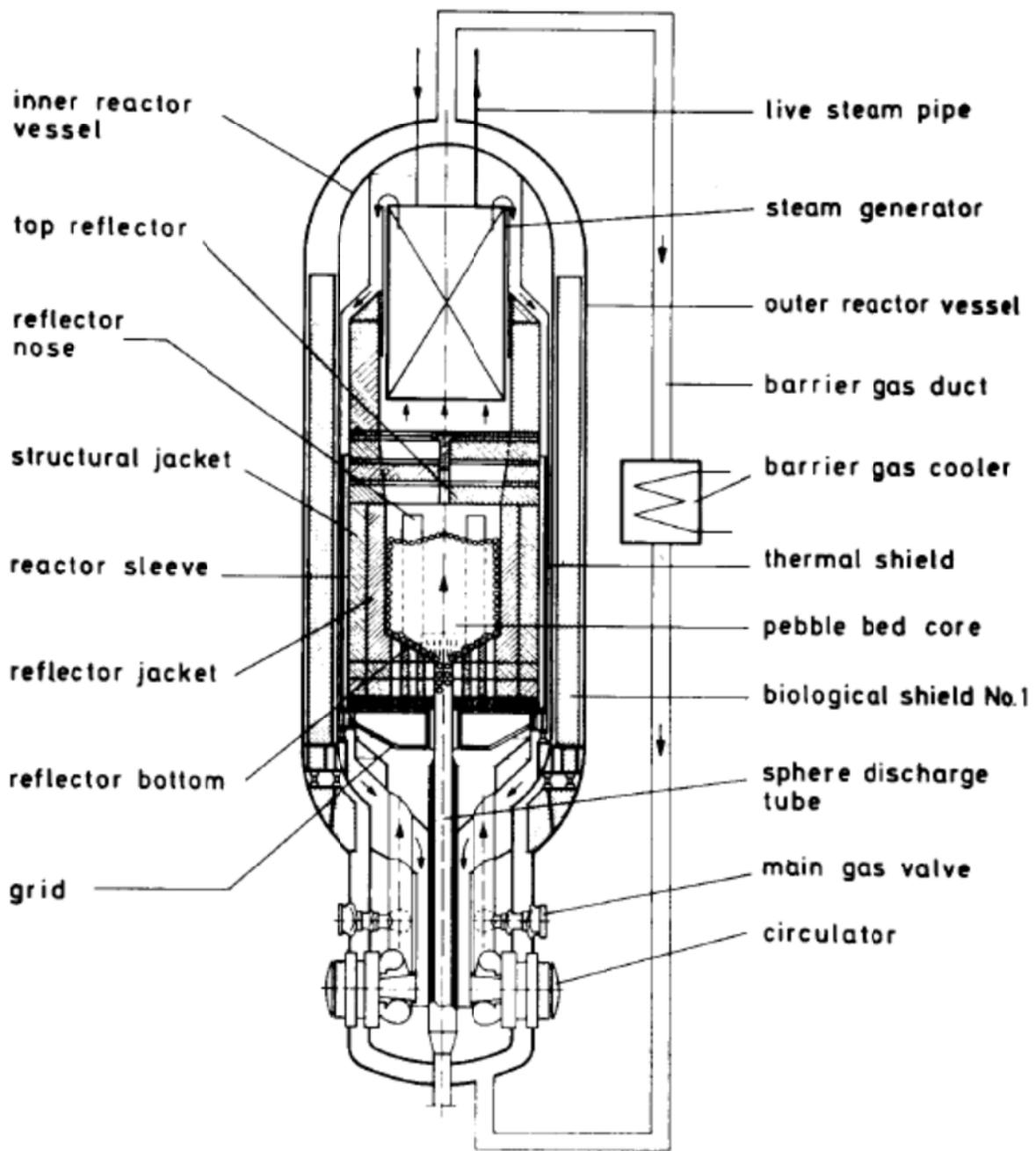


Fig. 41. Vertical cross section of AVR reactor.

[H. Knüfer, "Preliminary Operating Experiences with the AVR at an Average Hot-Gas Temperature of 950°C," *Nuclear Engineering and Design*, 34 pp. 73-83 (1975)].

Table 19. Main design characteristics and safety concept

Main Design Data	AVR
Core <ul style="list-style-type: none"> - Power - Power density - Pressure - Core inlet temperature - Core outlet temperature - Core diameter - Core pebble volume height 	46 MW(t) 2.6 MW/m ³ 10.8 bar 275°C 950°C 3 m ~2.8 m
Fuel <ul style="list-style-type: none"> - Fuel pebble diameter - Fuel particle diameter - Fuel - Fuel particle coating 	6 cm 0.6 mm 1981–1988 low enriched uranium UO ₂ 1967–1981 uranium and thorium carbide TRISO and BISO
Coolant circulator <ul style="list-style-type: none"> - Number of circulators - Speed - Mass flow 	2 400–4400 RPM 13 kg/s at 4400 RPM
Steam generator <ul style="list-style-type: none"> - Number of SGs - Type - Feedwater temperature - Outlet steam temperature - Steam flow 	One subdivided into four parallel Once through, helical coil 115°C 505°C 15.6 kg/s
Turbine <ul style="list-style-type: none"> - Livesteam pressure - Inlet steam temperature - Turbine speed - Electrical power (gross) 	72 bar 500°C 3000 RPM 15 MW(e)
Safety Concept <ul style="list-style-type: none"> Reactivity control <ul style="list-style-type: none"> - Temperature coefficient - Excess reactivity - Shutdown rods Decay heat removal Safety enclosure Water ingress control Air ingress control Reactor protection system <ul style="list-style-type: none"> - Criteria - Actions 	Inherent negative thermal feedback Temperature reactivity coefficient $-9 \times 10^{-5}/^{\circ}\text{C}$ 1.2×10^{-2} 4 shutdown rods in reflector (no control rods) Steam generator cooling for normal decay heat Passive wall conduction No separate shutdown cooling system Seal gap cooler for component protection Fuel elements Inner and outer pressure vessel Gas-tight containment Four parallel steam generator sections to limit water volume from leak Water reactivity coefficient ($+4 \times 10^{-6}/\text{kg water}$) Volume limitation of sealed containment Pressure, flow rate, flux, moisture Reactor shutdown—cold shutdown (steam generator isolation, relief)

The AVR core region is cylindrical with a diameter of 3 m and a core region height of 3.5 m. The reactor core consists of a bed of approximately 100,000 spherical fuel elements or pebbles, each 6 cm in diameter. Both BISO and TRISO fuel particle coatings were experimentally tested in the core. The pebble level within core region is approximately 2.8 m. In later years, the more successful TRISO particles, of the type shown in Fig. 2, were used more often. The fuel enrichment and fertile material also was changed over time for different fuel cycle experiments. Earlier fuel was highly enriched uranium and thorium carbide; later fuel was low-enriched uranium dioxide.

The core is completely surrounded by a 50-cm-thick graphite layer which serves as a reflector. The reflector in turn is enclosed in an insulating carbon brick layer. Both the graphite reflector and the carbon brick layers contain cooling gas channels. Four vertical “noses” in graphite reflector extend radially into the core region as shown in Fig. 42.

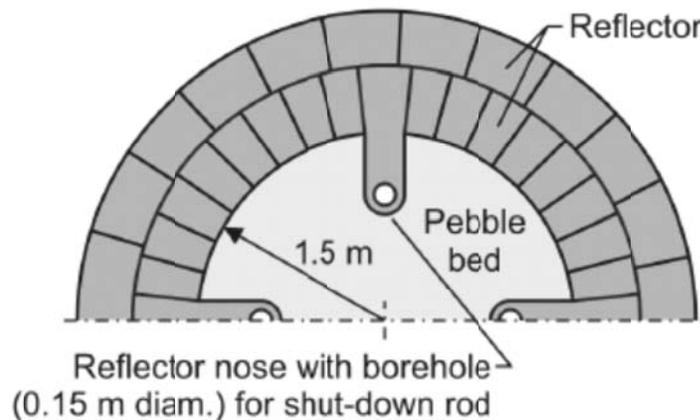


Fig. 42. AVR reflector with graphite “nose” extending into pebble bed.

[Rainer Moormann, *A Safety Re-Evaluation of the AVR Pebble Bed Reactor Operation and Its Consequences for Future HTR Concepts*, Technical Report, Jul-4275, ISSN 0944-2952, <http://www.fz-juelich.de/zb/juwel>].

Each nose encloses a drilled bore for insertion of a shutdown rod. The shutdown rods are inserted from the bottom of the core. Each shutdown rod is coupled to a heavier counter balance rod by means of a rod drive clutch and a rack and pinion gear. When the rod drive clutch is released by a reactor trip, the force of gravity pulls the counter balance rod down and the pinion gear simultaneously drives the absorber rod up into the core. The housing of each of the shutdown and counter balancing rods has four 9-m-long tubes welded onto the reactor vessel. The shutdown rods themselves consist of concentric metal tubes with a boron carbide filling between. The shutdown rods can completely shut the reactor from a hot critical to a cold critical state. They also provide for the required 0.5% of k-effective shutdown margin in the cold subcritical state for long-term shut down. The cold critical state implies a mean moderator temperature of 130°C sustained by an auxiliary oil fired heater.

4.4.2 Heat transport loop

The heat generated in the core is removed by the circulating helium coolant pressurized to 10 bar in normal operation. Two helium circulators below the core maintain the primary gas flow. Each circulator consists of an asynchronous motor and a clutched rotor; the sleeve bearings are oil lubricated. The motor is driven by a frequency transformer with a frequency range of 400 to 4400 min⁻¹ which permitted variable speed and flow in the circulator. A gas-filled, labyrinth-packed seal prevents the leakage of bearing oil into the primary cooling circuit and the motor’s crankshaft housing. The mean temperature of

helium leaving the core was set at 850°C in the initial operating design. Later the operating temperature was raised to 950°C. The helium flows upward through the core, then through holes in the radiation shield to the steam generator and back down to the circulators via the outer annular region of the vessel. The helium leaving the steam generator cools the core barrel and the inner reactor vessel.

The steam generator is located above the core inside the reactor vessel. The steam generator is composed of four parallel Benson systems that can be isolated individually. The parallel systems divide the water inventory into four parts to reduce the amount of water ingress that can occur in the event of a tube leak. The support tubes are also water cooled. The heat transfer surfaces are divided into layers which are connected as shown in Fig. 43. A water injector (attenuator) is provided in the intermediate header outside the reactor vessel to control the steam temperature. In actual operation, the attenuation was not needed as steam temperature was adequately controlled by reactor power. The steam generator tubes are ferritic steel. Each of the four steam generator sections in the economizer and evaporator sections consists of 10 tubes per section (40 tubes total). The superheater sections have 5 tubes per section. The steam generator is shielded against the radiation from the core by a graphite reflector (50 cm thick) and two layers of carbon bricks (each 50 cm thick). The steam generator itself is inaccessible after construction. For this reason, each of the 60 steam generator tubes penetrates the reactor vessel upper head so that an individual failed tube could be plugged externally.

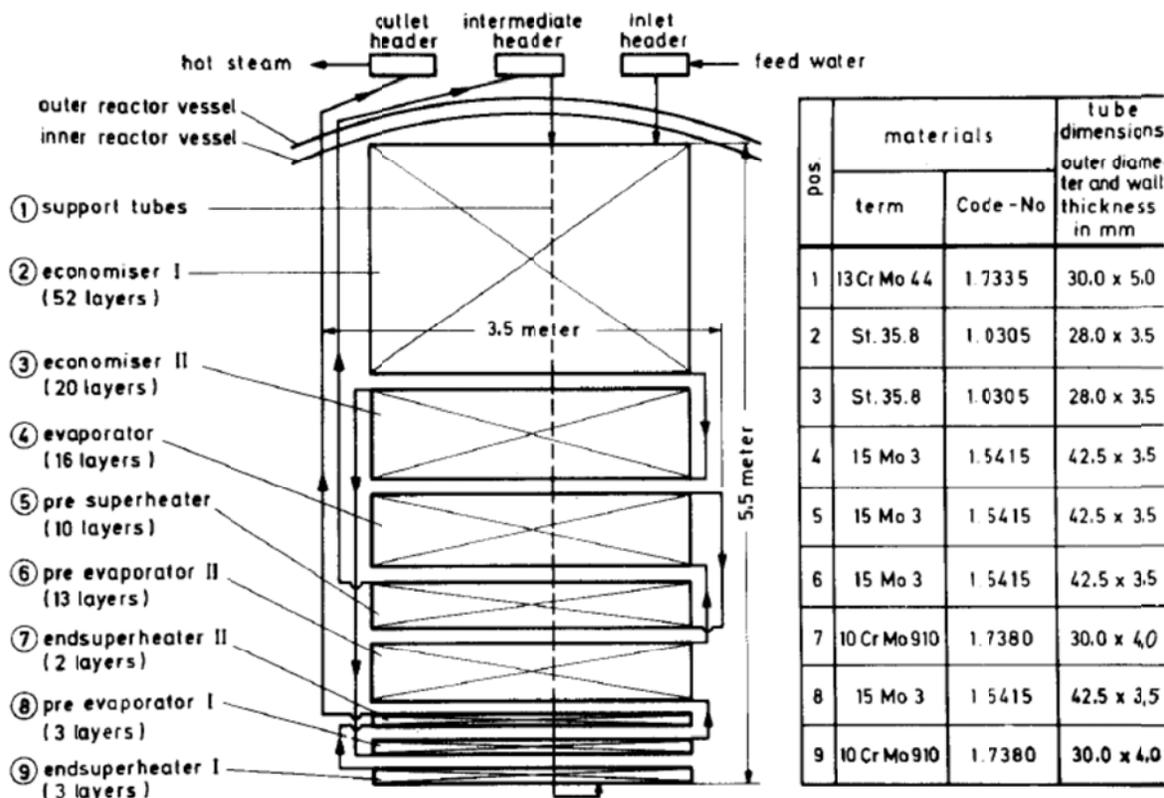


Fig. 43. Circuit diagram of the AVR steam generator with materials and dimensions.

[H. Knüfer, "Preliminary Operating Experiences with the AVR at an Average Hot-Gas Temperature of 950°C," *Nuclear Engineering and Design*, 34 pp. 73-83 (1975)].

An objective of the AVR development at the time of its design was to produce the same or higher steam temperature and pressure as produced in conventional fossil power plants, something not possible with light-water reactors because of the temperature limits of metal fuel cladding. The AVR steam generator produces superheated steam at temperature 505°C and pressure of 73 bar which then flows into a condensing turbine coupled to a synchronous electrical generator. This steam quality is comparable to conventional fossil powered boilers.

While the steam generator performed well, the design of the steam generator within the double reactor vessel proved to be problematic in a number of ways. The shielding did not prevent the steam generator tubes and corrosion products in the tubes from becoming irradiated by neutron fluence from the core. Circulation of the radioactive corrosion products and eroded tube material caused significant contamination in the balance of plant. High levels of radiation in the balance of plant complicated worker access and maintenance. Another problem with the design was that the steam generator developed a leak during an outage in May 1978 when the steam generator was being used for decay heat removal. The leak went undetected for some time. The leak resulted in a water ingress of 27 m³ of water into the pressure vessel which covered the helium circulators, fuel discharge tube, and the lower core region. While no radiation release or other serious consequences resulted from the event, the water ingress caused a lengthy outage. Fuel failures increased in the time following the restart which was attributed to water accelerating failure of weakened coatings.

4.4.3 Online refueling

The spherical shape of the AVR fuel pebbles means that the fuel is readily handled by automated mechanical conveyors thus permitting an online refueling system. The AVR was the first pebble-bed plant with an online refueling system. Figure 44 illustrates the main elements of the system. The refueling system inserts fuel pebbles into the top of the core via five delivery tubes. One tube is in the center of the other four and arranged symmetrically in the four quadrates of the core region. The fuel pebbles circulate downward by gravity. At the base of the core region, the fuel elements are channeled by a conical funnel to the bottom of the core where they are discharged through a long tube (15 m long, 50 cm diameter). A slotted rotating disk singulizer selects individual spheres. The fragment separator removes mechanically damaged pebbles and diverts them to the failed fuel storage containers. A dosing wheel contains measuring devices to detect the types of spheres (fuel, pure graphite, test, or poison spheres) and the burnup of the fuel pebbles. To determine burnup, the dosing wheel measures the Cs-137 radiation by means of a high-resolution photopeak gamma spectrometer. The gamma sensor is a Li-drifted germanium semiconductor detector. A computerized monitoring system compares the measured radiation spectrum with control data to measure the burnup and determine whether the fuel element should be transferred back into the core or discharged for storage.

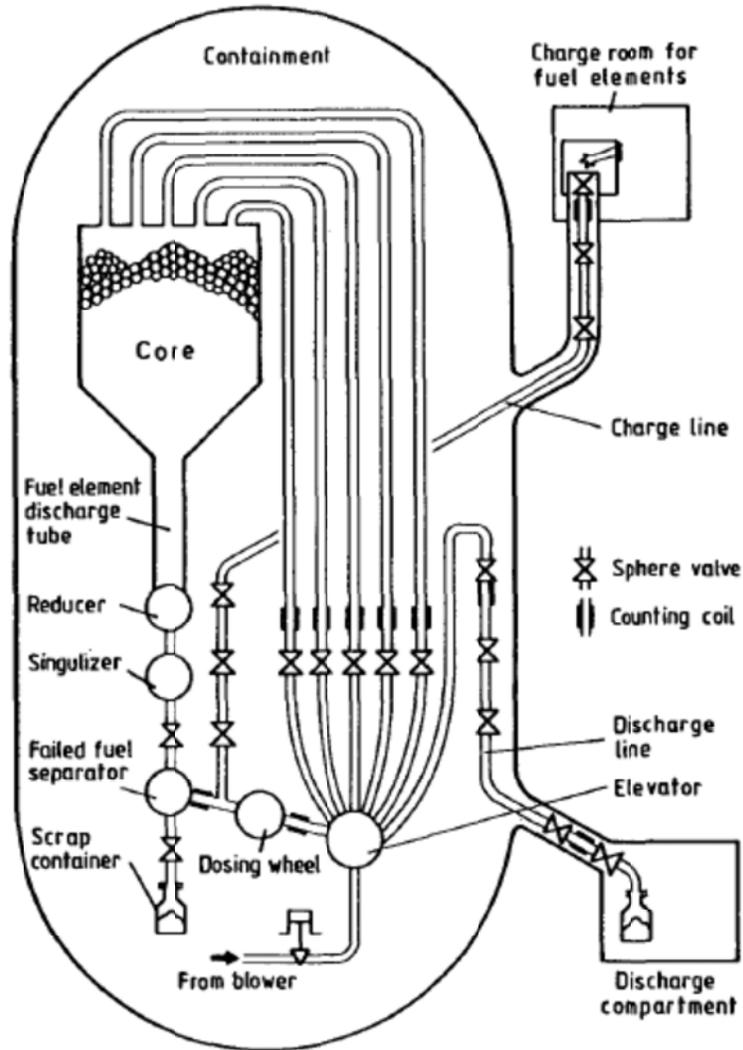


Fig. 44. Diagram of AVR online refueling system.

[E. Sauer, ed., *AVR-Experimental High Temperature Reactor-21 Years of Successful Operation for a Future Energy Technology*, Association of German Engineers (VDI), The Society for Energy Technologies, Dusseldorf GMBh, 1990].

One of the advantages of online refueling is that the number of fuel elements can be adjusted continuously during the reactor operation to account for burnup. No significant initial excess reactivity in the core is necessary to compensate for fissile material depletion as in fixed fuel cores. The need for burnable poisons and inserted control rods is reduced, which improves neutron economy thereby reducing the amount of fissile material needed for a given energy production. The AVR core is operated with the shutdown rods almost fully withdrawn. This configuration limits the reactivity available for uncontrolled rod withdrawal or other reactivity insertion events.

4.4.4 Containment

One of the goals of the AVR was to be a test bed for experimental fuel particle designs and coatings. Because of the uncertainty in the porosity of those fuels, the AVR was equipped with a double-wall

pressure vessel surrounded by gas tight containment as a precaution against radiation release from the unproven fuel particles. The system was designed for inward leakage through multiple barriers zones. The helium coolant in the inner pressure vessel was pressurized to 10 bar. The helium between the inner and outer reactor pressure vessels was divided into two barrier zones. Barrier zone 1 encompassed the circulators; Barrier zone 2 encompassed Barrier zone 1 and the remainder of the inner vessel. Barrier zone 1 was pressurized to 0.1 bar higher than the primary to ensure any circulator seal leakage went inward. Barrier zone 1 was pressurized to 0.1 bar higher than Barrier zone 2. The inner biological shield (shown in Fig. 45) is located in the cylindrical space between the two reactor vessels. Its shielding effect is sufficient to allow personnel to enter the containment, which houses the reactor vessels and auxiliary units, for any length of time during shutdown and for limited times for essential repairs during operation. The double vessel system is then surrounded by a safety containment and a concrete shell (150 cm thick). The concrete shell is simultaneously the reactor building and the outer biological shield. The containment vessel pressure is maintained at slightly less than atmospheric pressure to ensure inward leakage from the outside. The double vessel was expensive and proved unwieldy in maintenance. The steam generator was not accessible after initial commissioning.

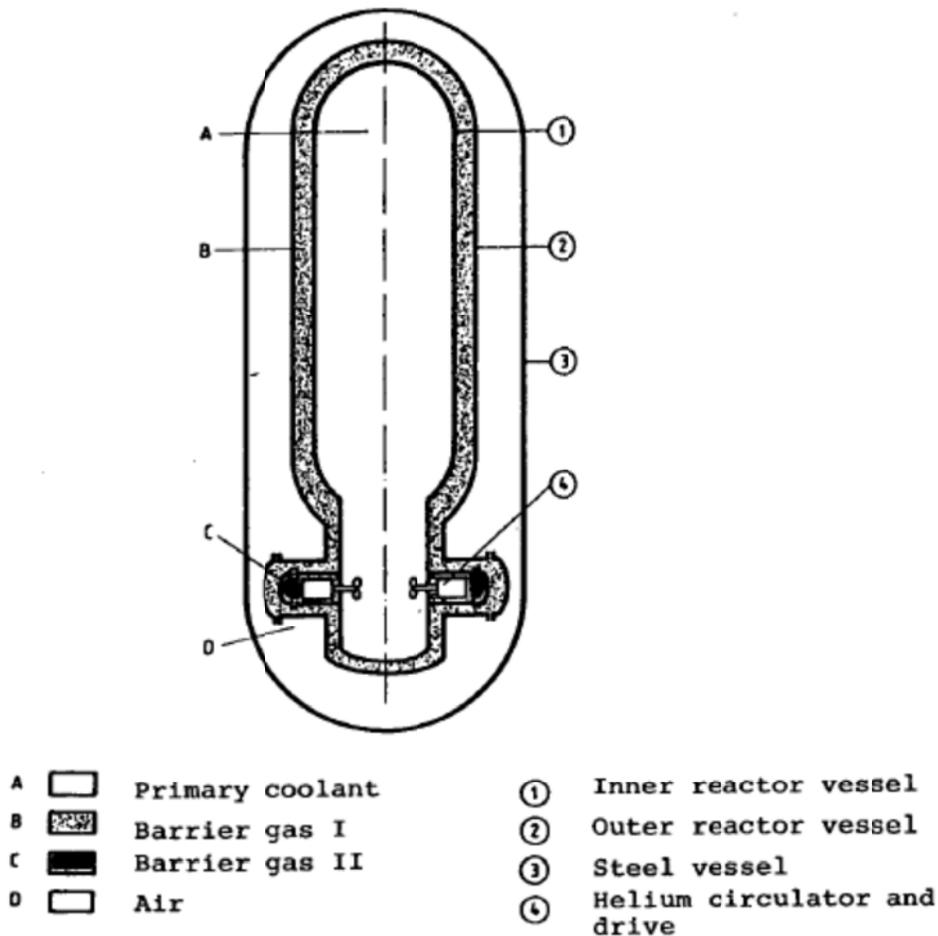


Fig. 45. AVR double pressure vessel and sealed containment.

4.4.5 Shutdown cooling system

The AVR did not use a separate active shutdown cooling system as described in Sect. 2.7.1 for decay heat removal. Following a normal shutdown, feedwater flow is maintained to the steam generator in water-cooling mode to provide core cooling. In the event of a failure of the secondary side cooling, passive cooling of the reactor by radiation and conduction through the vessel and containment walls is adequate to limit temperatures in the core and vessel to safe levels. The seal gap cooling is also a cooling system that aids heat removal from the vessel. However, this system was intended only to protect components in the gap such as the circulators and was not a safety system. The seal gap cooling system would normally be available but was not credited in protecting the core.

4.4.6 Helium purification plant

Small amounts of air and moisture enter the primary system through the addition of fresh fuel elements, small leaks in the cooling facilities, experimental ports, and through the course of maintenance and repair work to components of the primary circuit. The helium purification system continuously extracts a fraction of the flow to remove impurities from the coolant. The particulate matter is filtered in the gas precleaning stage which consists of two parallel gravel bed filters and coolers. The flow of $\sim 800 \text{ m}^3/\text{h}$ is generated by the pressure drop of the helium circulator across the core.

A bypass flow of $\sim 50 \text{ m}^3/\text{h}$ is drawn taken from this filtered and cooled helium and passed through two purification stages connected in series. The first stage consists of silica gel dryers and activated carbon adsorbers which are cooled with liquefied nitrogen. This stage is operated with a service life of $\sim 3,000$ hours to ensure that the noble fission product gases are retained. The next stage is a catalytic oxidation stage in which hydrogen and CO are first oxidized and again passed through activated carbon adsorbers cooled with liquefied nitrogen. These adsorbers are operated with a mean service life of approximately 10 days because main adsorbed gases are nitrogen and the oxidation products.

The purification plant is designed with two parallel full flow trains so that one train can be out of service for desorbing at all times. The gases from a loaded stage are desorbed by heating. The desorbed material is kept in temporary holding containers until short-lived inert gases are mostly decayed.

4.4.7 Current status

The AVR reactor was permanently shutdown at the end of 1988 after 21 years of operation. Dismantling and decontamination activities are underway to return the site to a “green field.” The history of the AVR reactor began in February 1959 when 16 German municipal electricity companies formed a subsidiary company, AVR, to build a prototype reactor. The objective of this association was to gain experience in the construction, operation, and especially the science, technique, and economics of the high temperature gas reactor (HTGR). In August 1959, Brown Boveri/Krupp was awarded the contract to design and build the reactor. Construction began in 1961 on the site of Jülich Research Center in Jülich, North Rhine-Westphalia, Federal Republic of Germany. The AVR attained first criticality in August 1966 and reached full power in early 1968. The AVR operated successfully for 21 years, and attained the highest temperatures (up to 1000°C) of any commercial nuclear power reactor up to that time.

4.4.8 Plant instrumentation and control systems

Normal operating instrumentation and control system

The AVR control inputs for the main heat transport system include:

- shutdown rod position,
- fuel pebble loading,

- helium circulator speed,
- steam turbine admission valve position, and
- feedwater flow control valve position.

The system also has a water spray into the intermediate steam header for controlling steam temperature, but this control was not needed.

The measured variables for the main heat transport loop of the plant include:

- neutron flux-source range,
- neutron flux-power range,
- helium coolant core inlet temperature,
- helium circulator differential pressure,
- helium circulator speed,
- helium coolant circulator outlet pressure,
- helium moisture concentration,
- temperatures at bottom reflector, side reflector and graphite nose projecting into reactor core,
- steam temperature,
- steam pressure, and
- feedwater flow.

The core outlet temperature is not directly measured because of the unreliability of thermocouples in the hot gas region of the core. The outlet temperature is derived from a heat balance measurement of power on the secondary side of the steam generator, the cold helium temperature, and a primary helium flow rate estimated from measured differential pressure of the helium and the helium circulator speed. Heat balance power on the secondary also is a derived quantity from steam and feedwater temperature and the feedwater flow.

Startup/shutdown

Normal startup

Two limitations on operation must be observed when starting from cold shutdown condition

1. Thermal stresses must be limited in the graphite bricks forming the core bridge between the core and steam generator. This is accomplished by limiting the heatup rate for the hot gas temperature to a maximum rate of 3°C/min.
2. Low flow boiling instabilities that could potentially cause tube failures must be avoided in the steam generator. To avoid boiling instabilities, steam production should only be initiated when the incoming helium has a mean temperature of more than 600°C. At lower temperature and power conditions, the steam generator is operated in a water-cooling model.

The start-up procedure can be divided into five steps:

1. From cold shutdown condition (130°C, all rods in), the reactor is brought to critical zero power level by withdrawing the shutdown rods. Approach to critical is monitored by the pulse counting source range neutron detectors.
2. The output is raised to neutron power of 12.5 MW on the power range detectors. At this output the steam generator can just barely be maintained in water-cooling mode.
3. By gradually withdrawing the shutdown rods, the core exit temperature is raised to 600°C at the rate of 3°C/min.
4. Once the temperature of 600°C is achieved, the evaporation in the steam generator is initiated by increasing the neutron power and reducing the feedwater mass flow. This flow and power

condition is sufficiently high to avoid boiling instability. At this point, a steam bypass valve is relieving steam directly to the condenser.

5. The cooling gas temperature and the steam temperature are set to the desired values using feedwater flow and helium circulator speed, the turbine is started up, and the generator is synchronized to the grid. The turbine load must be gradually increased to full power to limit material stresses in the turbine.

Altogether the startup takes approximately 4.5 hours from the commencement of withdrawing the rods until synchronization of the generator.

Normal shutdown process

The normal shutdown is initiated by switching off the helium circulators. This is the gentlest and slowest shutdown procedure. The rods remain in their withdrawn position. With heat removal reduced, the core gradually heats up which, in turn, reduces neutron power due to negative temperature feedback. The decay heat is initially sufficient to drive the core temperature high enough that the reactor becomes subcritical without the use of rods. Rods are driven into the core by rod drive motors after some time when the core has cooled down substantially. Delaying insertion protects the rods from thermal stresses.

The feed water mass flow is set at approximately 40%. This flow rate is sufficiently high to ensure that the steam is not produced by the steam generator and prevents boiling instabilities in the steam generator.

The helium circulators are restarted after about 3 hours gradually increasing the speed in steps. The steam generator runs in water-cooling mode for shutdown cooling with water dumped to the condenser by a water relief valve.

Normal operation

In normal operation of the heat transport system, the heat from the neutron reaction must be conveyed to the primary coolant and conducted through steam generator tubes to the secondary side coolant. The secondary coolant is evaporated and superheated in the steam generator. The steam is conveyed to the turbine and balance of plant for conversion to electricity and rejection to the heat sink. Each of these processes is a transmission of power which must be conducted in a coordinated fashion for stable operation. The AVR, being designed in the early 1960s, relied on the stability and thermal inertia of the heat transport processes to allow the operators to control the plant in manual (except turbine admission valve). In high-level terms, the goal was for the operators to use the three manually manipulated variables (circulator speed, feedwater valve, and reactivity) to hold three measured variables (secondary heat balance power, steam temperature, and core outlet temperature) to desired values. The turbine was equipped with an automatic pressure regulator which used the turbine admission valves to control steam pressure to a setpoint.

Unlike light-water nuclear power plants that control power with rods, load change in the AVR is accomplished primarily by changing the helium circulator speed using a variable frequency generator. An increase in helium flow causes the heat convected out of the core and heat convected into the steam generator to be simultaneously increased. Because of the large negative temperature coefficient, only a minor temperature change in the core and in the reflector is needed to raise or lower the neutron flux level. Consequently, an increase in circulator speed cools the core thus adding positive reactivity causing neutron power to rise. The rate of change of the load is determined by the maximum possible speed change of the helium circulators. Load reductions from 100 to 50% in 2 minutes were achieved. In principle, load increases are possible at the same rate of change. However, because of the thermal inertia of the core, neutron flux overshoots the steady state value before approaching equilibrium. On increasing load, the positive overshoot may exceed the high flux trip setpoint. Therefore, increasing ramps must approach equilibrium more slowly than decreasing ramps.

A given neutron power level can be achieved with a range of values of circulator speed and core outlet temperature depending on the reactivity in the core. To set the core outlet temperature to an operating point, the operating scheme for the AVR involved a coarse adjustment of core reactivity via the fuel pebble charging and precision regulation by the positioning of the shutdown rods. Maintaining core outlet temperature at constant value was the scheme by which burnup was accounted for in the control scheme. During normal power operation, the four shutdown rods are fully withdrawn or slightly inserted. (The rod insertion limit was such that the required shutdown margin was available to be inserted all times. The required shutdown margin at cold shutdown temperature, 130°, is 0.5% $\Delta k/k$.) The worth of the shutdown rods in excess of the required shutdown margin was permitted to be inserted for precise regulation of temperature. The rod insertion and fuel charging was used by the operator to maintain core outlet temperature at 950°C (raised from 850°C in 1975) using the estimated core outlet temperature. To maintain steady neutron flux, the circulator speed would have to be manually adjusted in concert with the fuel charging and rod positioning. Available literature does not give any indication of how closely temperature tracked the operating point. The reactor was described as “very stable.”

The steam produced by the steam generator is passed to the turbine which is equipped with automatic admission-pressure regulators. The pressure regulator is apparently the only automatic control in the AVR. This scheme, with the turbine responding to the steam load, is usually described as *reactor-following mode*. In this mode, the turbine controls pressure without regard to the electrical load demand or any feedback from the grid for voltage or frequency regulation. This scheme is common for base-loaded nuclear plants.

The feedwater flow is used to control steam temperature. An increase in feedwater flow causes a decrease in steam temperature in the once-through steam generator design. Secondary effects of a feedwater flow increase would also have to occur on the primary side. Helium temperature would decrease and neutron flux would increase with feedwater flow. Therefore, the operator would have to follow a feedwater flow adjustment with circulator speed and rod position changes to maintain the other measured variables at their setpoints. Apparently this task was not too onerous. The description of the steam temperature control by Ziermann states, “The system operates in such a stable manner that we are able to dispense with the planned temperature control by water injection.”³¹

Online refueling

The dual goals of control of online refueling are to use the fuel feed process for reactivity control to permit operation at the desired reactor conditions while simultaneously ensuring that the reactor can be shut down at any time and can be kept in a subcritical condition for as long as desired. To guarantee safe shutdown, the subcriticality of the shutdown reactor must be $>0.5\% \Delta k/k$ (licensing provision).

In reactivity control for the core, the fuel feed must account for burnup and continuously adjust total reactivity available in the fuel. Fuel charging is used for coarse control of helium outlet temperature.

As shown in Fig. 44, the refueling system has five delivery tubes to the core. One tube is in the center, and the other four are arranged symmetrically around the core. The distribution of fresh and used fuel to each of the five sectors of the core is used to flatten flux and temperature distributions in the core and reduce hot spots. The computerized burnup analyzer is programmed to determine the sector in which fuel pebble should be returned to optimize the flux distribution. The general scheme is to place fresh pebbles and pebbles with lower burnup in the outer zone and more depleted fuel in the center.

³¹ E. Ziermann, “Review of 21 Years of Power Operation of the AVR Experimental Nuclear Power Station in Jülich,” *AVR-Experimental High-Temperature Reactor—21 Years of Successful Operation for a Future Energy Technology*, Association of German Engineers (VDI), The Society for Energy Technologies, VDI-Verlag GmbH, Düsseldorf.

The fuel pebbles are removed via the fuel discharge tube at a rate of 300–500 pebbles/day fuel elevating unit. About 10% of the removed fuel is discharged to spent fuel.

Cold shutdown

Cold shutdown is a reference condition for the AVR defined by a mean moderator temperature 130°C and a subcriticality level that would be at least 0.5% $\Delta k/k$ at an infinitely long time after shutdown (after fission product poisons decayed to equilibrium condition). The cold shutdown state is the standby condition in which the reactor is ready to be brought to critical by withdrawing rods. During shutdown the fuel is not usually allowed to cool below 130°C. An auxiliary oil-fired heater sustains the temperature of 130°C if decay heat is not sufficient.

The reactor is monitored during cold shutdown by source range neutron detectors and temperature monitors. The source range detectors are pulse counting fission chambers located at midplane height outside the inner vessel behind the thermal shield. The thermal shield has a graphite window to improve the neutron permeability. Thermocouples in the reflector monitor of the moderator temperature.

Abnormal operating modes

Automatic reactor shutdown is enforced on the AVR for high-neutron flux, high rate of change of neutron flux, high- or low-helium pressure, high-moisture content in helium, and low-helium flow rate. Two types of automatic shutdown are used, scram and rod drive run-in. The scram method is the faster method. The rod driving method is slower but places less stress on equipment.

1. Scram

An automatic scram is initiated on high flux or high rate of change of flux. In the scram, the shutdown rods drop into position by releasing the rod drive clutch, power to the helium circulators is switched off, and the turbine is tripped. After the initial automatic reactor shutdown, the control rods are withdrawn half way under manual control to reduce thermal stresses in the control rods. The feedwater is reduced to approximately 40% to maintain reactor cooling. The steam generator goes into water cooling mode.

2. Driving the shutdown rods in

In all other automatic shutdowns from the reactor protection system, the shutdown rods are automatically driven into the core by the rod-drive motors in conjunction with switching off the helium circulators and shutting down of the turbine. After driving in the shutdown rods and achieving shutdown through temperature increase, the rods are withdrawn halfway again to reduce thermal stresses. The feedwater mass flow is set at about 40%. After approximately 3 hours, the helium circulators are restarted, gradually increasing the speed in steps to accelerate the heat dissipation. When decay heat has dropped and temperature of the core is sufficiently reduced, the shutdown rods may be reinserted to prevent recriticality.

4.4.9 Safety evaluation

The main safety functions of a nuclear power plant are to control reactivity, control heat removal, and limit release of radionuclides to less than licensed limits. One of the technical achievements of the AVR design is that it achieves its safety functions mainly through the inherent properties of the design, the materials used, and the fuel form. The key safety features of the AVR design are a small operational excess reactivity, a large negative temperature coefficient, inert gas coolant, the capability of the fuel particle coatings to withstand high temperature without releasing fission products, and a passive heat removal capability of the core, vessel, and containment that is sufficient for decay heat removal. In loss of cooling events, the combination of the small excess reactivity and large negative temperature coefficient stops the nuclear fission process with only a moderate temperature increase in the core even if the automatic rod shutdown system fails to insert rods. These design attributes mean that, for even the most

severe conceivable loss of cooling or reactivity insertion events, no active safety systems are needed to ensure integrity of the fuel and core. By comparison, a light-water reactor under postulated the loss of coolant accident without scram would result in fuel damage and other adverse consequences for the plant. For the AVR, this event is shown by mathematical simulation and by experiment not to have adverse consequences.

On the other hand, because of the high temperature of the core, air and water ingress events have the potential for chemical reaction of the fuel and moderator with the air or water and could result in core damage and fission product release. Recent re-evaluation of the performance of the AVR operational data at high temperature by Moormann may give reason to reflect on the safety evaluation of pebble bed reactor design.³² The arguments of Moormann are controversial among members of the HTGR community. Koster has responded to Moormann's re-evaluation of AVR safety and its implications for ESKOM's PBMR design in a point by point rebuttal.³³

In safety analysis, the evaluation method groups events into broad categories that are all protected by the same response. A limiting design basis case then demonstrates the safety of the plant for all the events in the class. In general, the safety evaluation events for the AVR include uncontrolled reactivity insertion events, loss of cooling events, and air and water ingress events which are discussed in the following sections.

Reactivity insertion events

Reactivity insertion events include uncontrolled rod withdrawal and overcooling events. The amount of potential reactivity is limited in the AVR design because of the online refueling to compensate for burnup. The event is detected by the high flux trip or high flux rate of change with a secondary signal from the high helium pressure trip. The response of the system is to scram the rods (on high flux) and to switch off the helium circulators. In the safety evaluation of this event, the transient is terminated safely even if the rods fail to scram. The increase in temperature of fuel and moderator from decreased flow is sufficient to shut down the reactor. The reactor remains subcritical for 24 hours until decay heat has decreased and xenon has decayed. The normal safety action for any of the detected trip functions includes stopping the circulators. The bounding event is the loss of forced circulation without a scram.

In September 1975, the AVR demonstrated experimentally that after a failure or normal stoppage of the helium circulator during power operation—even if the shutdown facility fails at the same time—the reactor shuts down automatically and remains subcritical for approximately 1 day.³⁴ The temperatures occurring in the fuel remain within the range of the temperatures prevailing during operation. In the experiment, the coolant flow was interrupted at full power by stopping the helium circulators, without inserting the shutdown rods. At the same time, the valves on the circulator discharge side were closed so as to prevent the natural convection that would have otherwise occurred. Following the trip of the circulators, the reactor shut down as the temperature rose due to the negative temperature coefficient of the reactivity. In the hours that followed, the generation of residual heat and natural convection led to a maximum temperature rise of 250 K in the originally cooler regions of the reactor and a drop in temperature in the hot zones. Calculations of the experiment estimated that the maximum temperature in the core following the event did not exceed the initial value. The reactor became critical again after about 15 hours (this point in time depends on the rod position, core cooling transients, and time-dependent variation in xenon concentration and was deliberately “advanced” in this experiment). The core stabilized

³²Rainer Moormann, *A Safety Re-Evaluation of the AVR Pebble Bed Reactor Operation and Its Consequences for Future HTR Concepts*, Technical Report, Jul-4275, ISSN 0944-2952, <http://www.fz-juelich.de/zb/juwel>.

³³Albert Koster, NEI Fuel and Fuel Cycle, “Pebble Bed Reactor—Safety in Perspective,” Friday, May 29, 2009.

³⁴K. Krüger, G. Ivens, and N. Kirch, “Operational Experience and Safety Experiments with the AVR Power Station,” *Nuclear Engineering and Design*, **109**, pp. 233–238 (1988).

a few hours later at a low-power level (in the kilowatt range). Figure 46 shows the measured response of AVR during the pressurized loss of flow without scram.

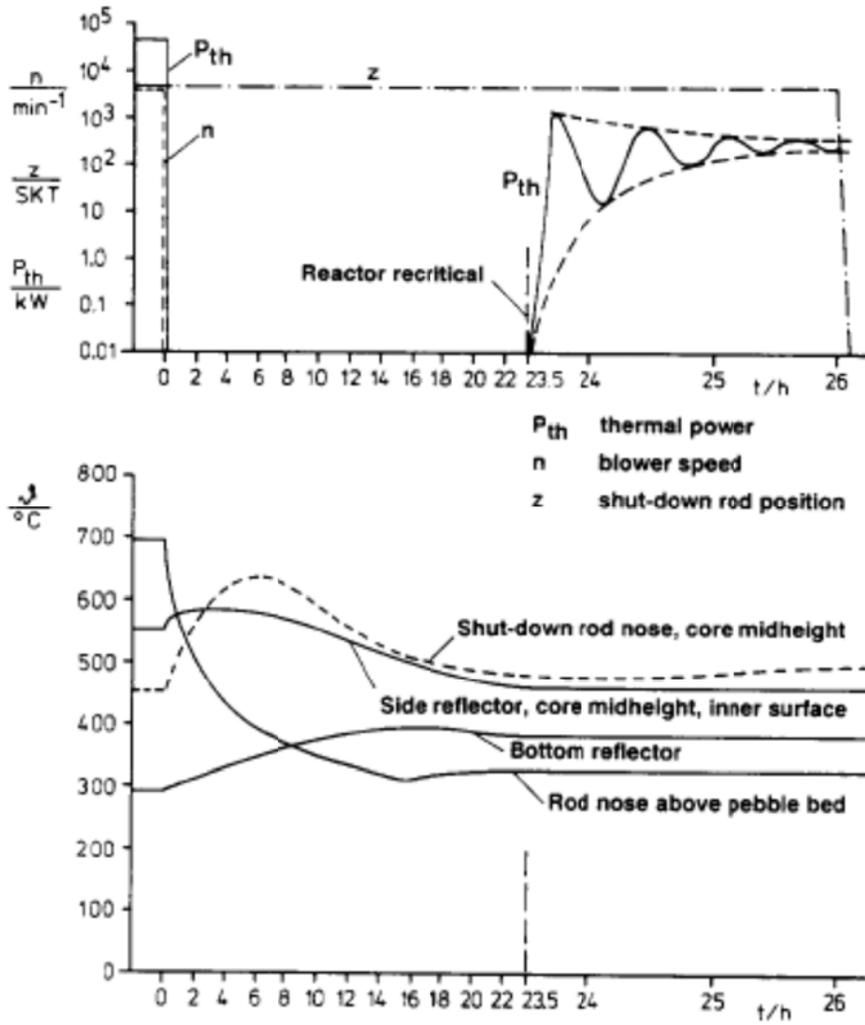


Fig. 46. Demonstration of inherently safe shutdown of the AVR.³⁵

Control of core heat removal events

The limiting case for loss of core heat removal event occurs when the helium coolant leaks from the primary system. In this event, all convective cooling from both natural and forced circulation in the core is lost. The normal response to this event is to detect the event by low pressure and to run the rods in and trip the circulators. The system must rely on radiation and conduction to cool the core. The licensing evaluation from this event shows that core temperatures do not exceed the temperatures at which fuel failures begin to occur (1600°C). This event is typically called the depressurized loss-of-flow event or DLOF. In light-water reactor terminology, the DLOF is equivalent to the loss-of-coolant accident without scram.

³⁵H. Gottaut and K. Krüger, "Results of Experiments at the AVR Reactor," *Nuclear Engineering and Design*, **121**, pp. 143–153 (1990).

In October 1988, the AVR demonstrated experimentally that, even in the event of loss-of-coolant helium without reactor scram, the reactor could remove decay heat.³⁶ The experiment was run with no actual decay heat. The reactor was maintained critical at low levels of power to simulate decay heat. The method was preferable because the heat generation could be terminated by tripping the rods if evidence of fuel failures was detected. The experiment was continued for 100 hours. The temperatures in the reactor fittings and in the reactor vessels soon drop down to moderate values after a brief rise. In this experiment, test pebbles for measuring temperature were added to the core fueling. The test pebbles contained fuse wire inserts which melted at different temperatures to aid in determining the maximum core temperature in the core. The majority of the wires showed that the temperatures were in the range of 1070 to 1085°C. The maximum fuel temperatures were higher than expected but well below critical values for damaging fuel particles. Figure 47 shows the measured temperatures for core and vessel.

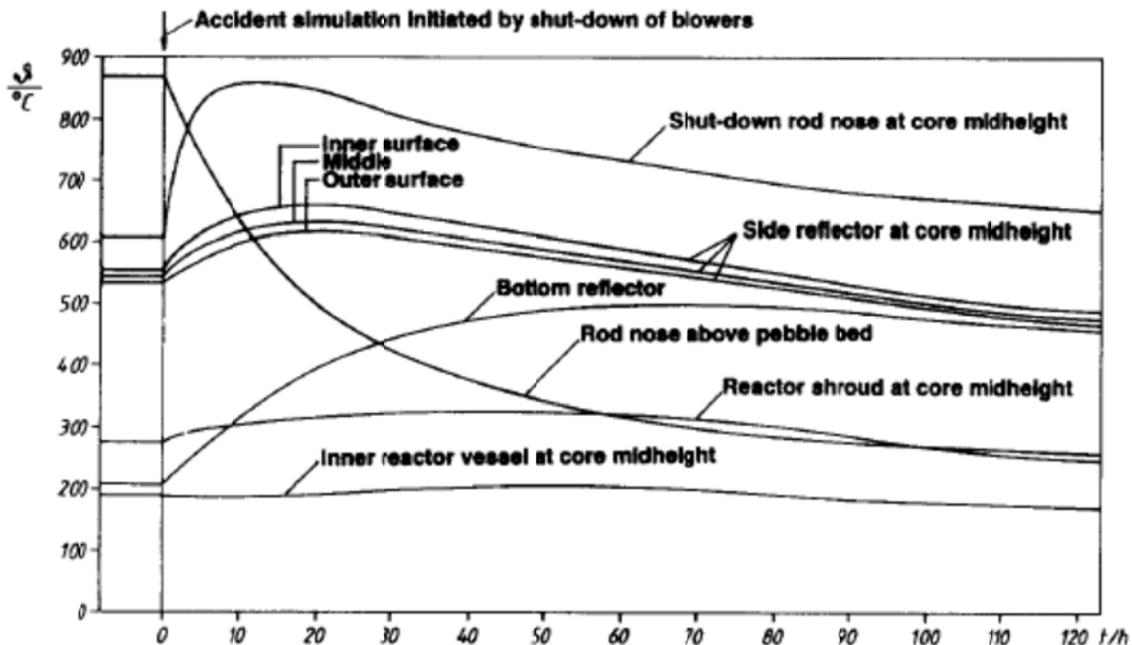


Fig. 47. Demonstration of decay heat removal in depressurized loss-of-flow event at AVR.³⁷

Control of water and air ingress events

The two main chemical attacks events for AVR are air and water ingress events. The strategy for preventing air ingress is the multiple barriers provided by the double pressure vessels and the sealed containment that must be breached for the core to have access to the open atmosphere. The entire primary coolant system and core are contained within the inner vessel. If the inner vessel fails, the first and second barrier zones of the outer vessel are filled with helium to prevent air from reaching the core. If the outer vessel fails, the sealed containment vessel contains a limited volume of air such that only small amount of oxygen is available to react with the core. No significant core damage results from failure of both inner and outer pressure vessels. Only if all three barriers are breached would the core potentially be exposed to the open atmosphere and sufficient oxygen to cause significant core damage. The AVR containment

³⁶ *Ibid.*, pp. 145–146.

³⁷ H. Gottaut and K. Krüger, *op cit.*, p. 146.

design with double vessel and containment is considered very safe with respect to air ingress events. In the event of air ingress, the event would accompany a loss of helium pressure which the system would detect. The progress of the event is limited by the air volume of the containment and is shown not to react sufficiently for fuel damage.

Water ingress is a more serious concern. Water reacts with the fuel potentially damaging the coatings of the fuel particles causing failure of the coatings and allowing the release of fission products. The event is protected in the AVR by detecting moisture and shutting down the reactor. A reactor shutdown with active cooling prevents damage to the fuel. Water does not react with graphite unless the temperature exceeds 1100°C. In the AVR, the volume of water ingress can also be limited by the four parallel steam generator circuits that allow a segment with a failed tube to be isolated. The remaining circuits remain available for the cooldown. Apparently, no discussion regarding the controls for the steam generator isolation have been found in the literature. Presumably, the isolation function is not automatic.

Depending on the core temperature distribution, local hot spots in the AVR may easily exceed 1100°C when core exit temperatures are 950°C. Temperatures in gas streams below the steam generator of up to 1100°C were measured in the melt wire temperature measurements of 1985. The AVR configuration with the steam generator directly above the core does not produce sufficient mixing to prevent hot streams from contacting steam generator tubes. Hot gas streams may lead to overheating of the steam generator tubes or other metallic components which may increase their failure rate and contribute the frequency of water ingress events.

Another major safety implication of water ingress lies in the potential for the formation of combustible gases. In the water gas reaction, a mixture of CO and H₂ is formed by interaction between steam and graphite. The rate of the reaction increases exponentially with temperature. To prevent an explosive gas mixture after depressurization, graphite surface temperatures must not exceed 1100–1200°C.

In contrast to all other major accident scenarios, the AVR design is not passively safe in a design basis water ingress accident. The event must be detected. The affected steam generator's tubes must be isolated, the core must be shutdown by rods rather than allowed to heatup, and active cooling of the core must be provided to reduce temperatures to below the reaction point. These active emergency measures are contrary to the passive measures required for other events. This category event remains one of the significant concerns for pebble bed designs with primary steam generators.

The AVR experienced a massive water ingress accident in May 1978 during a maintenance shutdown. A small leak, estimated between 1 to 3 mm², occurred in one of the superheater tubes. The indications of the leak were not immediately diagnosed. Approximately 27 m³ of water entered the core and flooded the lower part of the inner reactor vessel including the fuel element feeding device, the lower section of the fuel discharge tube and control rod mechanisms, the helium circulators, and nearly 6000 fuel elements. The consequences for the plant were not severe. Core temperatures were already low when large water amounts were present and, thus, the extent of the graphite/steam reaction remained limited. The accident, however, illustrates the vulnerability of the AVR design with the steam generator located in the same vessel and above the reactor to the water ingress accident.

The AVR was successfully operated after the 1978 event. The repair of the steam generator, removal of the water from the vessel, replacement and inspection of components was completed by July 1979. The plant started operation in August 1979 to dry the carbon material inside the core, and electrical power generation started again on August 30, 1979. It remains unknown whether the leak was caused by hot gas streams from core hot spots. Evidence suggests that a sufficient cooling of hot gas streams by mixing with bypass flows, as originally assumed in AVR design, did not occur.

4.5 Fort St. Vrain Reactor

The Fort St. Vrain reactor was the second commercial HTGR in the United States. The plant operated in Platteville, Colorado, beginning power operation in 1976 and ending operations in 1989.

4.5.1 Reactor system design

As with all the gas-cooled reactors in this summary, the coolant for the Fort St. Vrain plant was helium and the fuel was contained in TRISO particles. The fuel particles were embedded in rod-shaped fuel compacts and inserted in a prismatic carbon matrix. The fissile particles were highly enriched uranium and thorium. Fertile particles were thorium. Figure 48 shows the configuration of fuel particles, fuel rods, and prismatic fuel blocks in the Fort St. Vrain core.

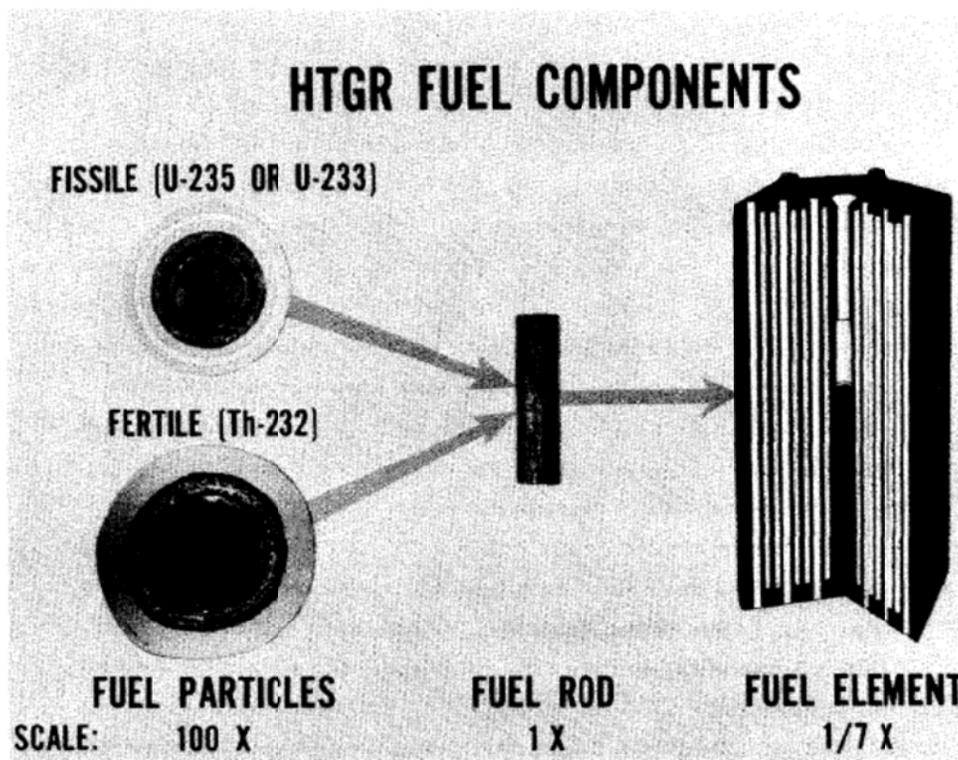


Fig. 48. Fort St. Vrain fuel showing fissile and fertile particles, fuel rod (compact of particles), and hexagonal matrix fuel element.

[“Experience with the Fort St. Vrain Reactor,” Walker]

The entire primary coolant system, active core, steam generators, and helium circulators were contained within the 32.3-m (106-foot) high prestressed concrete reactor vessel (PCRVR). On the primary side, helium at 4.78 MPa (693 psia) and 386.7°C (728°F) was discharged from four steam driven helium circulators and passed down through the core, heating to 767.2°C (1413°F). Heat was removed from the primary loop by a steam generator which was then conveyed to a conventional steam turbine for power conversion. The plant was rated at 842 MW(t) and 330 MW(e). The helium then passed through one of two identical loops, each having six parallel steam generators. After passing through the steam generators, the helium returned to the helium circulators to pass through the core again. Two helium circulators were

applied in each loop. Reheat steam from the high-pressure turbine drove the helium circulators, was reheated, and returned to the intermediate-pressure turbine. The circulators also had Pelton water turbine drives for use under emergency conditions when steam was not available. Figure 49 illustrates the arrangement of the components in the PCRV. Table 20 gives some of the system parameters for the Fort St. Vrain plant.

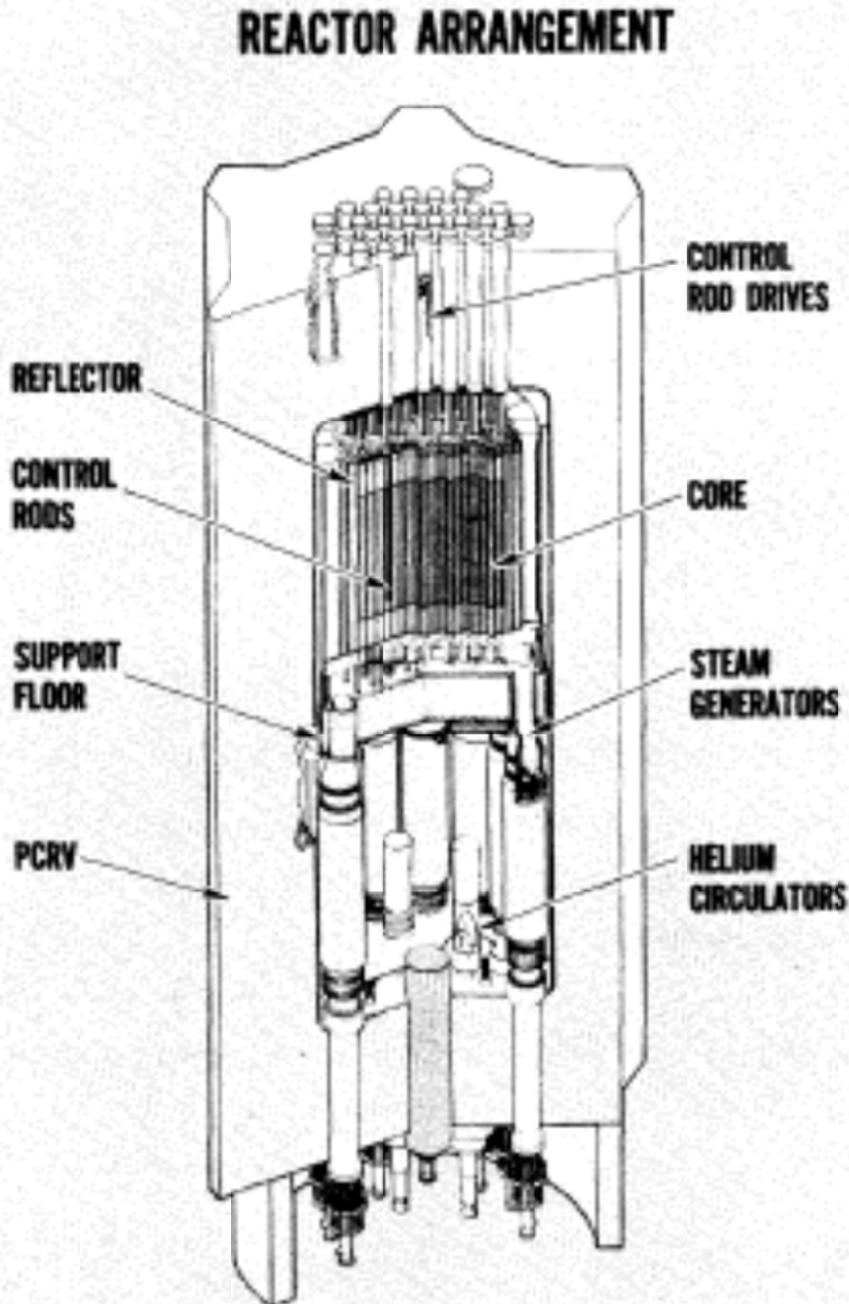


Fig. 49. Fort St. Vrain arrangement of components within the PCRV.

["Experience with the Fort St. Vrain Reactor." Walker]

Table 20. Fort St. Vrain design parameters

[“Fort. St. Vrain Experience,” H. L. Brey and H. G. Olson; “Fort St. Vrain Nuclear Generating Station Construction and Testing Experience,” A. L. Habush and R. F. Walker; “The HTGR: From Demonstration Experience to Co-Generation Applications,” C. L. Rickard and P. Fortescue; “Comparison of Predicted and Measured Parameters at the St. Vrain HTGR,” H. G. Olson, H. L. Brey, and K. R. Stroh; “Fort Saint Vrain Gas Cooled Reactor Operational Experience,” ORNL]

Reactor Design Parameters	
Item	Parameter
Reactor power [MW(t)]	842
Net reactor power [MW(e)]	330
Heat transport system	
Helium coolant pressure at rated power	4.78 MPa (693 psia)
Cold helium temperature	387°C (728°F) at circulator discharge
Hot helium temperature	767°C (1413°F) at core exit
Core helium flow rate	491.5 kg/s (3,898,000 lb/h)
Core helium pressure drop	96.5 kPa (14.0 psi)
Feedwater temperature	204°C (400°F)
Steam temperature/pressure	540°C/16.6 MPa (1000°/2,400 psig)
Reactor vessel internal height	22.9 m (75 ft)
Reactor vessel inner diameter	9.4 m (31 ft)
Loop description	
Loops	2
Steam generators per loop	6
Helium circulators per loop	2
Reactivity control	
Control rod pairs	37
Core and fuel cycle	
Fuel element	Prismatic hex-block, ~36 cm across flats × 79 cm height
Active core configuration	1,482 elements in 247 vertical columns; 37 flow-controlled regions
Fissile material	Uranium oxycarbide
Power density	6.3 W/cm ³
Average enrichment	93.15% ²³⁵ U
Power peak/average axial ratio	1.4:1
Fertile material	ThO ₂
Initial core loading, kg: ²³⁵ U/Th	721/15,905
Burnup limit, %FIMA fissile/fertile	20%/7%

On the secondary side, each loop contributed half the total output of the nuclear steam supply system. This produced steam at 16.55 MPa (2400 psig) and 532°C (991°F). After passing through the high-pressure turbine, steam passed to the helium circulators and then back to the steam generators for reheat to 524.4°C (976°F) before passing to the intermediate-pressure turbine. After the intermediate-pressure

turbine, the steam passed to the low-pressure turbine, then the condenser. The condensate system used a full-flow demineralizer, three low-pressure heaters, and a deaerator. Three boiler feed pumps (two turbine-driven and one motor-driven) directed the feedwater through two high-pressure heaters back to the steam generator modules to complete the secondary loop. ("Fort St. Vrain Experience," Brey and Olson). Figure 50 illustrates the configuration of the primary and secondary parts of the plant.

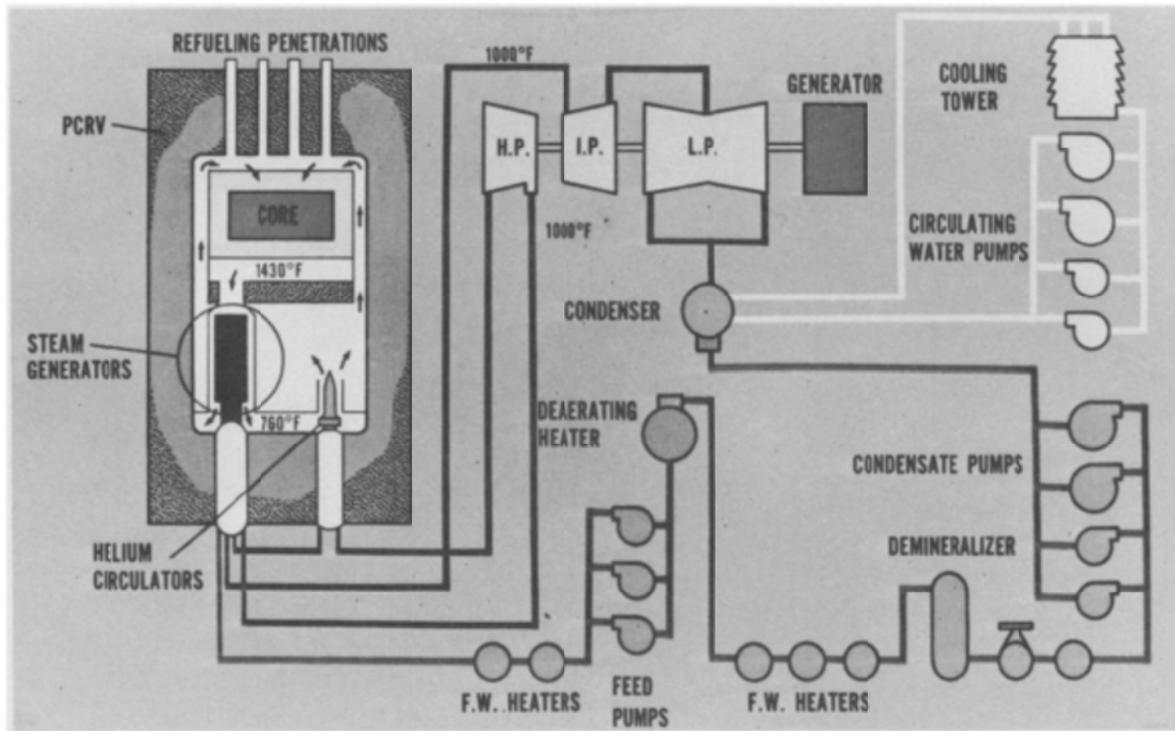


Fig. 50. Turbine generator configuration and balance of plant.

[*Fort St. Vrain Nuclear Generating Station Construction and Testing Experience*, A. L. Habush and R. F. Walker]

4.5.2 Decay heat removal systems

Unlike other GCRs described in this summary, Fort St. Vrain did not employ a separate, dedicated shutdown cooling system as described in Sect. 2.7.1 of this report or a passive reactor cavity cooling system described in Sect. 2.7.2 for decay heat removal. Instead, the Safe Shutdown Cooling System was a function or mode of operation of the same systems used for normal heat removal. The seismically and environmentally qualified Safe Shutdown Cooling System that was credited in the safety analysis for emergency core cooling consists of five major divisions of equipment shown in Fig. 50: (1) the helium circulators operated on water turbine drives, (2) the helium circulator auxiliaries, (3) the steam generator sections for both main and reheat steam, (4) the alternate flow paths to the helium circulator water turbines and steam generator sections, and (5) the safety water supply source. Other alternative, nonsafety sources of water for the cooling flow to the steam generators were available as were nonsafety steam supply and nonsafety pressurized water supply for the steam and water turbines to meet diversity and redundancy requirements.

In normal shutdown operation, the heat removal operated just as in power operation. Steam produced by the reactor drove the steam turbine to power the helium circulators which cool the core. The same steam

also powered the boiler feed pumps. When the power level and cooling rate of the core was insufficient to produce steam, the circulators were powered by pressurized water from either the boiler feed or the condensate pumps. The water turbine, called the Pelton wheel drive, was a safety component. Electrically powered and steam-powered boiler feed or condensate pumps gave diverse supplies of pressurized water for the steam generators and the Pelton drives. Diesel generators provided backup electrical power, and an auxiliary boiler and a backup auxiliary boiler could provide steam for the steam-driven boiler feedpumps. Auxiliary systems for circulator seals and bearings are safety-grade components. In normal shutdown cooling mode, excess steam from the steam generators is routed to the steam drain tank and then to the condenser or the service water heat exchangers in closed loop cooling. The safety-grade water source is the firewater system which is supplied by two seismically qualified storage ponds which are required to have 9 days' supply of cooling water available. Other nonsafety water sources were also available.

Unlike other GCR designs in this summary, Fort St. Vrain was a larger core and required forced helium circulation to be started within 60 minutes of depressurization from equilibrium full power. In the depressurization event, two loops must be able to operate. "Operate" means that one of two circulators in each loop must be operational, and the associated water turbine must be able to sustain a rotational speed of 8000 RPM. If depressurization event started from an equilibrium power of 82% and only one circulator could be started, analysis showed that less than 1% fuel damage is sustained.

The dependence on operational equipment during accident conditions led to a complex analysis of the safety of the cooling systems to determine that the regulations and general design criteria in 10 CFR 50 were met. In the technical evaluation³⁸ of the safety-related and important-to-safety cooling functions in Fort St. Vrain's Updated Final Safety Analysis Report, a method of identifying analogous systems and functions for shutdown cooling in the Westinghouse Standard Technical Specifications and the Fort St. Vrain plant was used to show that the plant met the intent of the 1967-proposed GDC 1 through 5, 19 through 26, and 40 through 43. Nevertheless, the system was complex and was the source of multiple water ingress events during operation.

4.5.3 Containment heat removal

The Fort St. Vrain system also required a cooling for the metallic liner and the structural concrete of the PCRV. The cooling system, called the PCRV liner cooling system (LCS), was in continuous operation for all normal and accident conditions. The system is divided into two redundant trains, either is sufficient for cooling the PCRV. The cooling tubes on the PCRV liner are alternately fed from the two trains so that all parts of the vessel are adequately cooled by a single train. In normal operation, the LCS rejects heat in a recirculating closed mode to the nonsafety Service Water heat exchangers or, in emergencies, is supplied with water by the safety class firewater in an open, nonrecirculating cooling mode.

4.5.4 Leak detection systems

The Steam Line Rupture Detection/Isolation System (SLRDIS) automatically detected and isolated High Energy Line Breaks (HELBs). The isolation maintained building environment to assure continued operation of the safety-related electrical equipment for safe shutdown and decay heat removal. Following actuation of the SLRDIS, safe shutdown cooling was restored within 90 minutes by providing boosted fire water to one helium circulator and fire water to one steam generator (last resort).

The Maximum Credible Accident resulted from multiple failures involving the helium purification system regeneration piping. The primary coolant leakage resulted from a postulated rupture of a 2-in. pipe from the PCRV top head to the helium purification regeneration system just below the refueling floor. About 2 minutes into the accident, the reactor would scram on low primary pressure. The peak building

³⁸D. L. Moses, *Technical Evaluation Report for the Review of Fort St. Vrain Technical Specification Upgrade Program*, Fort St. Vrain Nuclear Generating Station, Docket 50-267, July 1988.

temperature would be about 79.4°C (175°F) 40 minutes into the accident, not accounting for heat sinks or helium mixing in the building volume. Since the electrical equipment would remain operable in that environment, reactor cooldown was accomplished by continued forced circulation core cooling at a reduced helium density.

4.5.5 Current status

The Fort St. Vrain reactor initially loaded fuel in 1974 and reached power operation in 1976. The plant ended nuclear operations in 1989 due to higher-than-anticipated operations and maintenance costs. A review of operational experience is given NUREG/CR-6839.³⁹

4.5.6 Plant protection, control, and instrumentation systems³⁶

Plant protection system (PPS)

The PPS contained

1. reactor protective circuitry,
2. instrumentation and control for certain engineered safeguards, and
3. circuitry oriented toward protecting various plant components from major damage which is only indirectly concerned with the basic safety of the plant as it relates to the public.

The major automatic functions of the PPS were:

1. reactor scram,
2. loop shutdown and steam/water dump,
3. circulator trip, and
4. rod withdrawal prohibit.

The plant protection system consisted of the instrumentation and controls required to initiate automatic corrective actions upon onset of an unsafe condition. These actions were directed toward reducing plant power and shutting down reactor plant equipment and were designed to override the plant operator and the normal plant controls. The plant protection system was utilized upon occurrence of the following.

1. Equipment failures which require corrective action beyond the capability of the plant control system.
2. Failure of the plant control system causing an abnormal condition.
3. Incorrect operation which result in a potentially unsafe condition.

The protective functions required of the plant protection system were related to conditions which might lead to:

1. loss of core cooling,
2. power increase not matched by core cooling,
3. PCRV pressure rise, and
4. core or major equipment damage.

The plant protection system achieved reliability through redundancy and coincidence and was designed to perform its function in the presence of any single failure and consequential effects. The system also used channel independence to guard against the effects of plausible single events, such as shearing or blocking of process connections, environmental effects, seismic events, and module removal. Independence is achieved through:

³⁹NUREG/CR-6839 (ORNL/TM-2003/223), *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, Oak Ridge National Laboratory, 2003.

- channel combination (voting logic) as close to output as practical,
- physically separated channel connections from PPS to process,
- physically separated redundant sensors (separate wells),
- physically separated wiring races for channels,
- redundant power supplies,
- ground/short isolation,
- fail-safe circuits/components where practical, and
- instruments located to minimize chance for common mode accidental damage
 - protection and control measurement channels are physically and electrically separated, and
 - bypass or removal of scram-related channels initiates a trip.

Safe plant shutdown and normal core afterheat removal could be performed with one operational steam generator loop. Thus, complete automatic shutdown of the second loop is prohibited by the PPS except for the case of a steam pipeline rupture and which is automatically followed by a reactor scram.

Channel trips used 2 out of 3 general coincidence logic system for in the reactor scram circuitry. Three independent sensing circuits (A, B, C) are provided for each scram parameter. One sensor circuit for each input parameter was combined in an OR solid-state gating to trip A (similarly in B and C)—a trip of any one sensing circuit trips the channel.

Reactor scram logic

Automatic brakes in the control rod drive mechanisms are energized to hold the rods out of the core during normal plant operation. Upon scram signal, the brakes were de-energized, and the rods fall into the core by gravitational force.

Figure 51 shows the logic diagram for the reactor scram. The following plant states are used by the plant protection system to initiate the automatic reactor scram logic.

- Manual (two independent switches and actuation mechanisms are provided)
- Low main steam line pressure
- Low hot reheat steam pressure
- High wide range channel rate of neutron flux change
- High startup count rate (startup only)
- Rate of change of startup count rate (startup only)
- Neutron flux high
- High moisture in the primary coolant
- High reheat steam temperature
- Low helium pressure (only at power)
- High primary coolant pressure
- High hot reheat line pressure (only at power)
- Low superheat line pressure (only at power)
- Plant electrical system power loss
- Two-loop trouble (leak detected in more than one steam generator loop)
- Reactor building temperature
- Auxiliary scram actions

Several of the reactor scram events involved trip envelopes that were functions of two or more variables. The Fort St. Vrain operated with a fixed helium inventory and helium temperature varied with power. Consequently the pressure trip depended on both pressure and temperature. Figure 52 shows the envelope of allowable pressure between the high- and low-pressure trip functions.

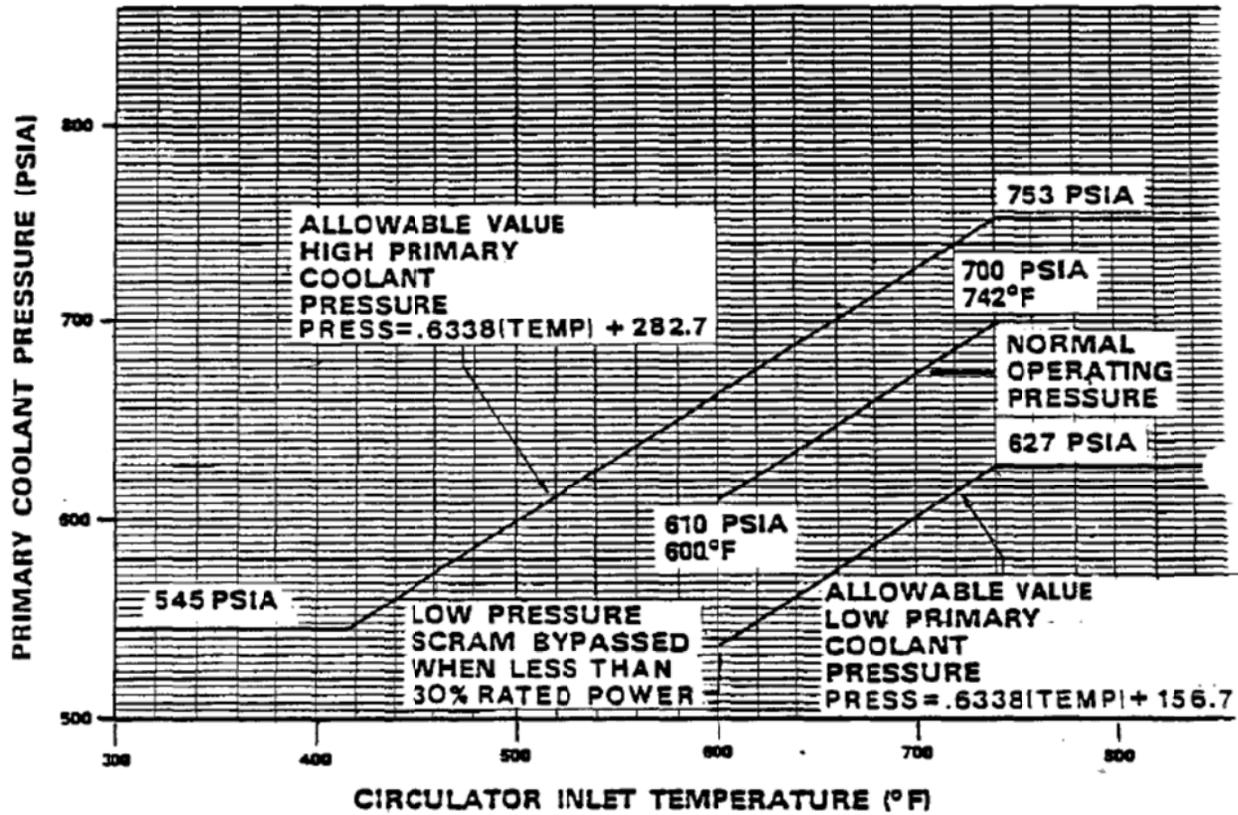
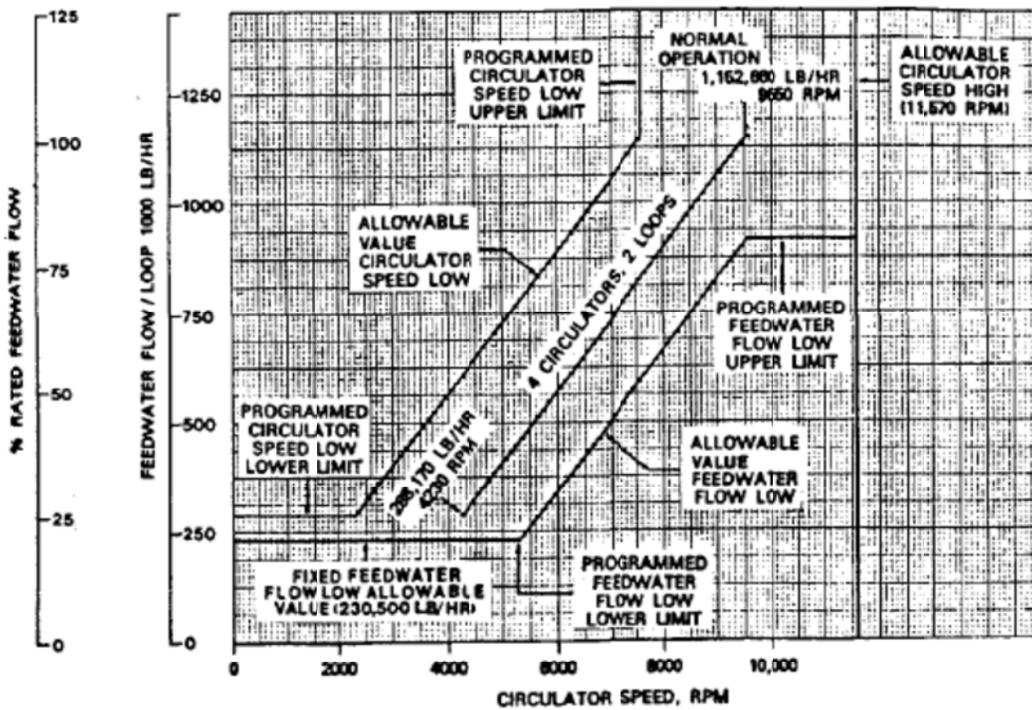


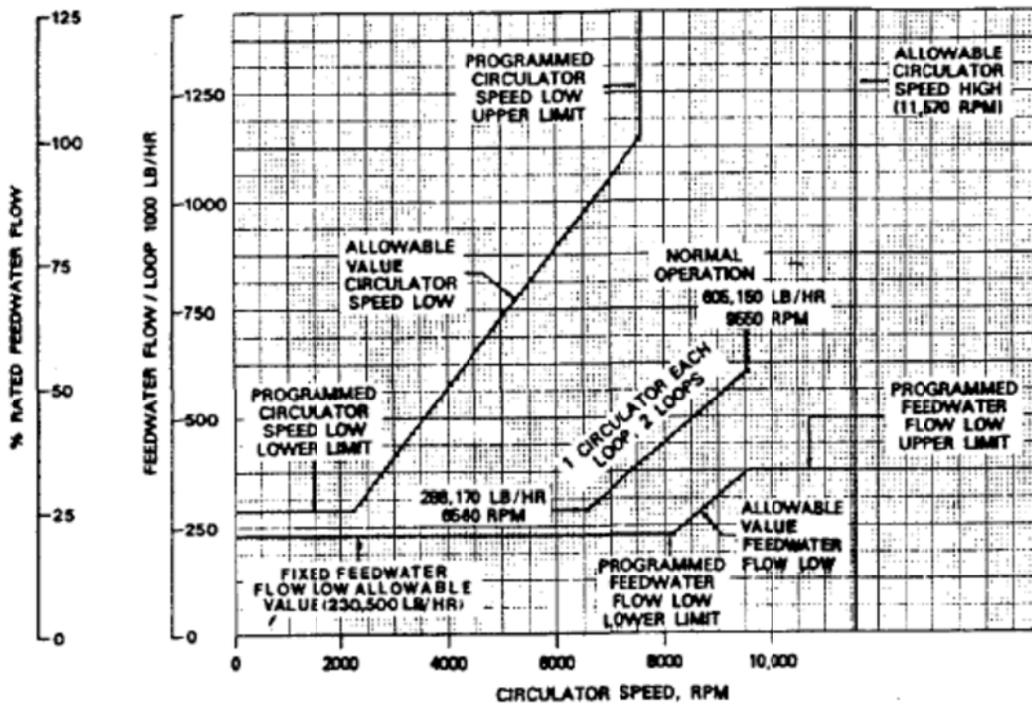
Fig. 52. Primary coolant pressure vs circulator inlet temperature.

[Fort St. Vrain FSAR, Revision 8, Chapter 7]

The feedwater flow vs circulator speed also depended on power level. The trip envelope for speed vs flow (shown in Fig. 53) enforced the variable limits and an overall high speed limit. In addition to circulator speed dependence, the limits depended on the number of circulators operating in a loop as shown in subplots (a) and (b). The programmed limits were implemented using analog hardware.



(a) TWO CIRCULATORS IN EACH LOOP OPERATING



(b) ONE CIRCULATOR IN EACH LOOP OPERATING

Fig. 53. Programmed trip limits for helium circulator speed vs feedwater flow.

Circulator trip logic

The circulator trip results in (1) closing the circulator steam turbine inlet and outlet valves, (2) reducing the load setting of the main turbine governor to 50% load, and (3) changing the feedforward and proportional gain in the steam temperature control.

In the event of a failure of a single helium circulator, the plant remained online at a reduced load. The turbine and reactor did not automatically trip. Power level was reduced to 50%, and normal plant controls acted to stabilize the feedwater and steam systems at the lower level. In the loop with only one circulator running, control gains were modified, but the action was otherwise normal control of circulator speed.

The circulator trip logic systems used redundant input channels in a 2-out-of-3 with specific (local) coincidence logic. The plant protection system used these parameters in circulator trip circuit and provided an input to the reactor protection through loop shutdown and two loop trouble.

- Manual
- Low circulator speed
- High circulator speed—steam turbine
- High circulator speed—water turbine
- Low feedwater flow
- Circulator bearing water loss
- Circulator seal malfunction (bearing water leakage to primary coolant, labyrinth helium flow high)
- Circulator penetration pressure high
- Loop shutdown
- Steam leak detection (turbine building pressure, rate of rise)
- Steam leak detection (reactor building pressure, rate of rise)
- Steam leak detection (turbine building pressure, fixed setpoint)
- Steam leak detection (reactor building pressure, fixed setpoint)

Rod withdrawal prohibition logic

The rod withdrawal logic used redundant A and B hindrance logic and was, otherwise, similar to the loop shutdown and circulator trip logic. The plant protection system used these parameters in rod withdrawal prohibition:

- low count rate,
- high startup range channel rate of neutron flux change,
- high wide range channel rate of neutron flux change,
- high flux level,
- flux level interlocks,
- rod control circuit load,
- power range downscale failure,
- rod group sequencing, and
- automatic loop shutdown logic,

The plant protection system used these parameters in automatic loop shutdown:

- high loop moisture (high-range instrument or low-ranger instrument),
- high reheat header activity,
- hot reheat header radioactivity high,
- steam generator penetration overpressure,
- low superheat header temperature (only at power),

- high differential temperature between loops,
- high primary coolant pressure, and
- trip of both circulators in a loop.

Reserve shutdown system and safety shutdown cooling system logic

The reserve shutdown system and safe shutdown cooling systems were manually actuated with no operating bypasses.

Steam/water dump

The steam dump system isolated and drained a steam generator to limit the amount water in the steam generator that could enter the primary in the event of a steam generator tube leak. The detection of moisture in the primary resulted in activation of emergency feedwater isolation valves. Steam from the other steam generators was prevented from entering the isolated steam generator by main steam stop/check valves. The dump was accomplished by the rapid opening of two parallel redundant valves relieving water and steam through the feedwater header to the dump tank. Either valve was sufficient to drain the steam generator. The dump was terminated manually by the operator by closing the dump valves when it was determined from the radiation monitors in the drain tank that helium was entering the drain.

The steam/water dump activation of one loop prevented initiation of the dump of the other loop. This interlock ensures that cooling was provided during shutdown. The system was triggered by

- detection of moisture in a helium loop,
- high primary coolant pressure, or
- high pressure in the steam generator penetration interspace.

Analysis showed that if the wrong steam generator was isolated (the intact steam generator), the operator would have sufficient time to detect the error from humidity readings in the primary or radiation readings in the reactor cavity and would be able to restart the intact steam generator and isolate the failed steam generator before significant damage to the fuel or radiation release occurred.

4.5.7 Plant control system

The Fort St. Vrain plant operated in fully automatic control mode from 25 to 100% of full power. The plant was designed for base load operation at a fixed power level but was also capable of following load changes with a maximum rate of change of about 5% per minute. The control system was designed regulate the production of high-pressure, high-temperature steam for the electrical power generation. The plant started up under manual control by the operator. From 0 to 30%, individual systems were switched into automatic control mode as the plant reached the normal power range.

The overall plant controls system design is shown in Fig. 54. The automatic control system regulated the system to the operating point and responded to load changes and gradual changes in the plant. The control system was also designed to respond automatically to larger disturbances such as loss of feedwater, turbine-generator trip, and reactor scram.

The control scheme for normal power operation was a boiler-follow-turbine strategy in which load changes were introduced by changing the position of the turbine admission valves. The feedwater valve position, circulator speed, and reactor rod position were operated in feedforward plus feedback control scheme to respond to the load change promptly and then regulated the plant to the operating point. This scheme gave rapid turbine response by drawing down stored energy from the steam generator and from the thermal mass in the core and reflector. The feedback response to errors in steam pressure, steam temperature, reheat temperature, and differential pressure across the feedwater control valves gradually restored these variables to their operating point.

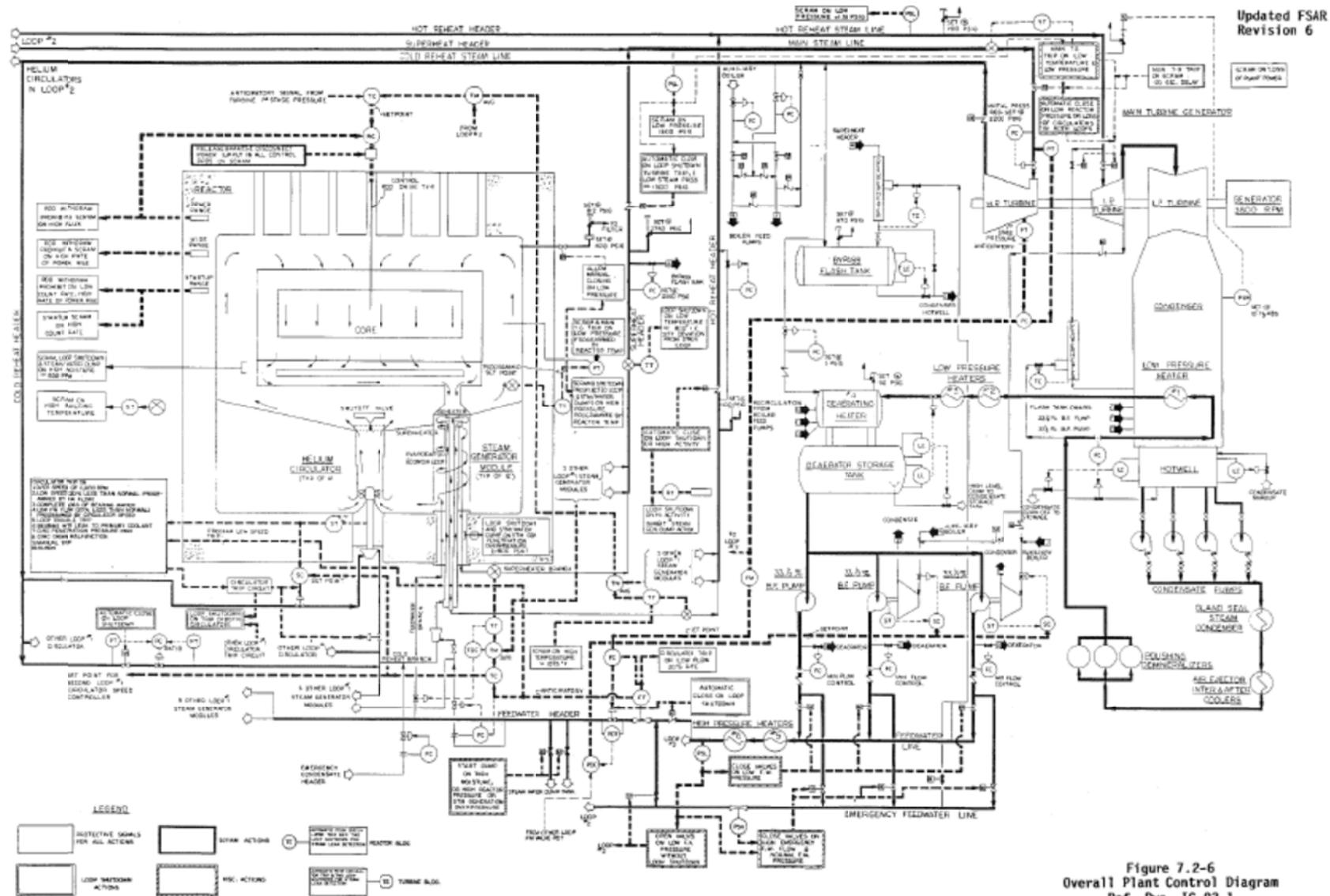


Fig. 54. Fort St. Vrain plant control system.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

Figure 7.2-6
Overall Plant Control Diagram
Ref. Dwg. IC-93-1

Alarms for abnormal values of plant parameters were provided. The system allowed operators to take manual control instead of automatic to avoid initiation of protective functions of the safety system. The safety system always provided the necessary safety response when design trip conditions are exceeded.

The following sections describe the individual control loops.

Feedwater flow control

The feedwater flow setpoint was adjusted to control steam pressure. The steam pressure setpoint was 16.5 MPa (2400 psig) throughout the normal load range. The feedwater flow setpoint was computed as a steam pressure error with proportional and integral action summed with the first stage pressure. The first stage pressure is very nearly proportional to turbine load. This part of the flow setpoint signal served as a feed forward of the load to the feedwater flow.

The feedwater flow setpoint cascaded to the flow controller. Each feedwater control valve received the same flow setpoint. The flow controller was a closed loop controller that adjusted the feedwater valve to match the measured feedwater flow to the flow setpoint received from the pressure controller.

The turbine speed control for the boiler feedpump was based on maintaining a constant differential pressure across the feedwater control valves. The measured differential pressure across the valve was used in a closed loop control for the turbine speed.

The feedwater flow controller also contained a fast runback mode that was initiated following most scrams. A feedwater flow runback rate of 0.5%/s was used for reactor scram and turbine trip. A runback rate of 0.25%/s was used for loop shutdown, circulator trip, trip of three circulators, and boiler feedpump trip. The rapid runback brought feedwater flow down to the required level very quickly and through the feedforward ties to circulator control and flux control was able to coordinate the reductions in power production and transport through the primary system.

Helium circulator control

The helium circulators were used in a closed loop control to maintain main steam temperature at the setpoint of 541°C (1005°F). The main steam temperature was controlled by individual loop temperature controllers, each of which determined a helium circulator speed setpoint for its associated loop. The circulator speed setpoint contained steam temperature error with proportional and integral action and an anticipatory feedwater flow signal. The feedwater flow is a feedforward signal to ensure rapid response to load changes. The feedback errors react more slowly and stably to bring the temperature to the setpoint.

Reactor power control

Reheat steam temperature was controlled by creating a change in the neutron flux controller setpoint, which changed neutron power which, in turn, restored reheat steam temperature to its setpoint. The flux setpoint contained the reheat temperature error with proportional and integral action and a signal proportional to steam flow which was used as a feedforward to anticipate load changes. The flux setpoint cascaded to the flux controller.

Reactor power was controlled via flux controllers. The flux controller operated one control rod drive for automatic power regulation. The automatic rod drive was connected to a pair of control rods near the center of the core. The flux measurement signal for the flux controller was averaged from six detectors. The flux controller was a three-zone, on-off controller with an adjustable deadband acting on the flux error. The rod position controller effectively integrated the flux error to achieve zero offset between measured flux and the flux setpoint that cascaded from the steam temperature control.

Only one pair of control rods was automatically controlled. Since one rod pair is insufficient for the 25 to 100% normal load swing, manual shimming of three symmetrically located rod drives was required occasionally.

Helium temperature was not directly controlled but was determined by the helium flow rate and the reactor power level for the hot helium and by the feedwater temperature entering the economizer for the cold helium. The control scheme described thus far has five manipulated variables—turbine admission valve position, rod position, feedwater valve position, helium circulator speed, and boiler feedpump speed. The system has five measured variables that are controlled to setpoints—load, steam pressure, steam temperature, reheat steam, and feedwater valve differential pressure. Hence, the degrees of freedom match the constraints, and it is not possible to control helium temperature also. Nevertheless, the average helium temperature is uniquely determined (though not fixed to a setpoint) by the other constrained variables and remains in the safe operating range. A consequence of not controlling the average helium temperature was that the helium pressure varies over the power range. This expected variation is included in variable helium pressure trip setpoints in the reactor protection system.

Shim rod control

The core contains 37 pairs of control rods. Normally, only one pair was dedicated to automatic control. Six pairs were used as shim rods which were manually controlled to adjust core reactivity in response to burnup and large load swings. The shim rods also had an automatic runback mode in which the group of six rod pairs was used simultaneously by the flux controller for fast power reductions. The remaining 30 pairs are used for safe shutdown of the reactor.

Because of the potential for uncontrolled reactivity insertion, the shim rod control system was designed with simple, reliable switch controls for positioning the rods, rod position indications, indications for in-limit, out-limit, and slack cable, and inhibits to prevent multiple rod pairs to be inserted or withdrawn simultaneously. Alarms were provided for group misalignments. Nevertheless, accidents involving the simultaneous withdrawal of all 37 rod pairs at 25 and 100% were considered in the design basis accidents. Analysis showed that negative temperature feedback is sufficient to protect the core from damage starting from any initial power level in the event all rods are run out simultaneously.

Orifice control system

The orifice control system in Fort St. Vrain positioned variable orifices in inlet coolant passages within the reactor to control the distribution of flow of helium coolant through each region of the core to compensate for variable power generation in each region. The purpose was to reduce the variation in core outlet temperatures across fuel and reflector. No GCR design since Fort St. Vrain has used the orifice flow control mechanism.

The orifice valves were manually controlled from the control room. Only one orifice at a time may be repositioned. Limit switches were provided at the 98.5 and 1.5% of open positions, to prevent running orifice valves into their mechanical stops. Orifice position indication was required in the control room. The control and position indication system was integrated with the region outlet temperature display and other pertinent information displayed on the primary coolant control board.

The orificing valve was positioned by a stepping motor. The total time to drive the valve from the fully open position to the fully closed position was approximately 30 minutes. Transfer of the orifice selector switches during orifice motion was prohibited by solenoid interlocks on the selector switches. The motor control indexer required that the AC power not be turned on during the selection of a drive. A “Normal-Select” pushbutton switch was also provided and electrically interlocked to the selector switches and indexer. This pushbutton was depressed to allow the orifice selector switches to be repositioned and it simultaneously disconnected AC power to the motor control indexer. Indicator lights were provided to

monitor the condition of the orifice control circuitry. One light indicated the availability of power; the other indicates when a motor is in a drive cycle.

Three digital orifice position indicators were provided which obtain position information from potentiometers in the mechanism. The selection of an orifice for positioning (by the orifice selector switches) simultaneously selected its position for display on the appropriate digital indicator. An indicating light directed the operator's attention to the position indicator corresponding to the valve being operated.

The outlet gas and fuel temperatures that resulted from accidental closure of an orifice were analyzed and shown to be within acceptable limits.

4.5.8 Plant control system transient events

The plant control system was studied extensively in dynamic simulations prior to operation to investigate the adequacy of the design under a wide range of operational events. This section illustrates three basic events with normal control system response. The events are a normal load change, turbine trip without scram, and reactor scram. The events depicted show that the normal operational control is smooth and stable and that conditions that might damage the fuel or affect the design life of fuel or core structural materials are not reached by a considerable margin.

Normal load change (Fig. 55) is an example of the capability of the plant control system to respond at the maximum design rate of load change, 5%/m. The transient ramps from 100 to 25% and back. The reactor power leads turbine power in the decrease. The reactor power must lead the turbine power on the decreasing ramp to reduce the temperature of the fuel and reflector. Similarly, the reactor power leads the turbine load on the increasing ramp to heat the core and reflector back to the temperature corresponding to full power.

The steam pressure error remains close to setpoint throughout the transient. The maximum deviation is 9.1 psi (62.7 kPa) over the setpoint. The main steam and reheat steam temperature have very little deviation from setpoint in the transient. The maximum positive deviation from setpoint is 15°F (8.3°C) and maximum negative deviation is 6°F (3.3°C).

Turbine trip without scram

Figure 56 shows turbine trip from a full load without a scram. This event is a reduction in the heat removal capability of the secondary. The control strategy is to run the reactor back to the heat removal capacity of the steam bypass system without tripping the reactor. This strategy minimizes thermal stresses on the core and potentially reduces the time for return to power thereby improving plant availability.

After tripping the turbine, steam pressure goes to the bypass system backpressure control setpoint 17.58 MPa (2550 psig) with the steam pressure regulated by the bypass system. The reactor power decreases to steady-state of approximately 25% after approximately 20 minutes. Rapid runback controls for feedwater valves bring the feedwater flow back to a low flow limit that is within the reduced load capacity of the bypass system. In back pressure control mode, feedwater flow is no longer responsible for controlling steam pressure.

Circulator speed and flux controls operate to regulate steam temperature and reactor power and, because of the feedforward terms, are coordinated with the feedwater flow. Over the same 20-minute period, the reheat steam temperature and main steam temperature are restored to their setpoints. The turbine trip without scram transient illustrates the capability for rapid runback through feedforward actions plus gradual feedback to restore the plant to operating point following a major disturbance.

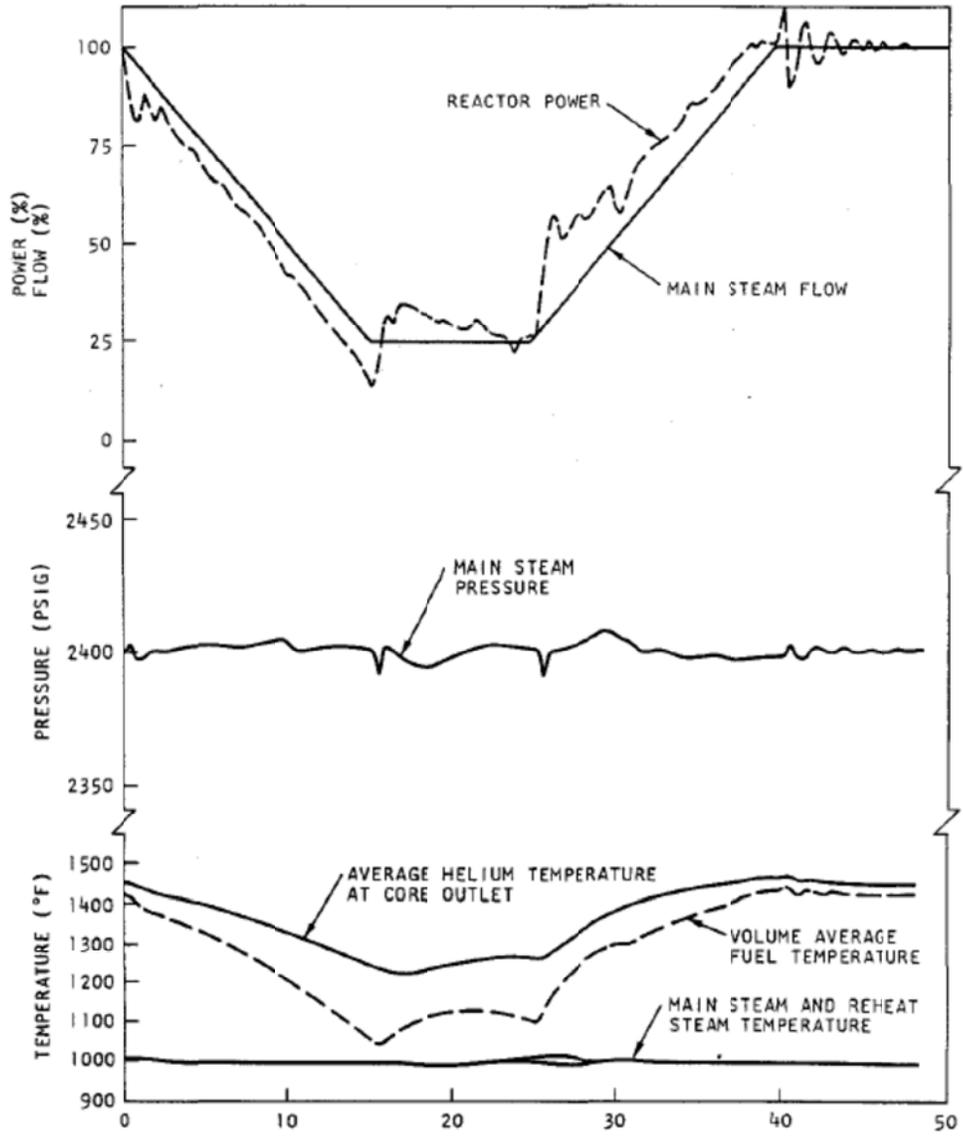


Fig. 55. Normal load change at maximum design rate.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

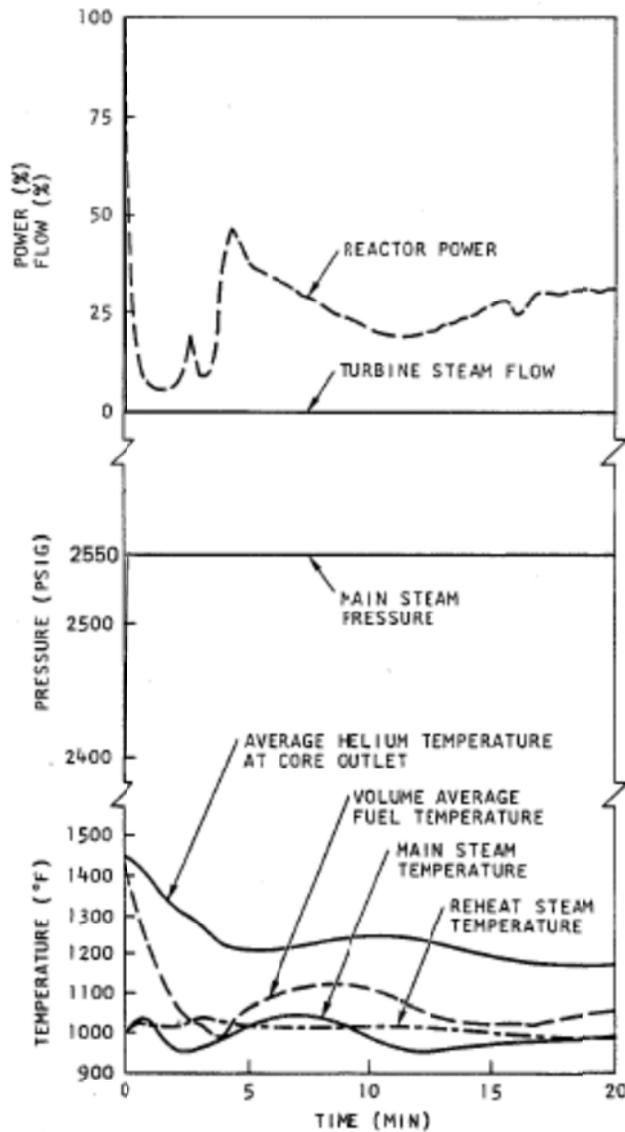


Figure 7.2-2
Turbine Trip from Full Load

Fig. 56. Turbine trip from full load.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

Manual reactor scram

In normal operation, the plant control system responds to the post-scrum conditions to bring the plant to an equilibrium condition. Figure Fig. 57 shows a reactor scram from full power. The response of the control system following a reactor scram is a programmed reduction in feedwater flow to 28 at 0.5%/s and a turbine runback to 10 at 0.75 %/s. After 2 minutes, the turbine is tripped to slow the cooling rate of the core. Reheat and main steam temperatures remain close to the 1000°F (538°C) for 5 minutes then begin to fall as decay heat drops off. The average helium temperature, main steam temperature, and reheat steam temperature decay to approximately 500°F (260°C) after approximately 20 minutes. If continued, the transient would show a gradual approach to the saturation temperature for 2550 psig (17.58 MPa).

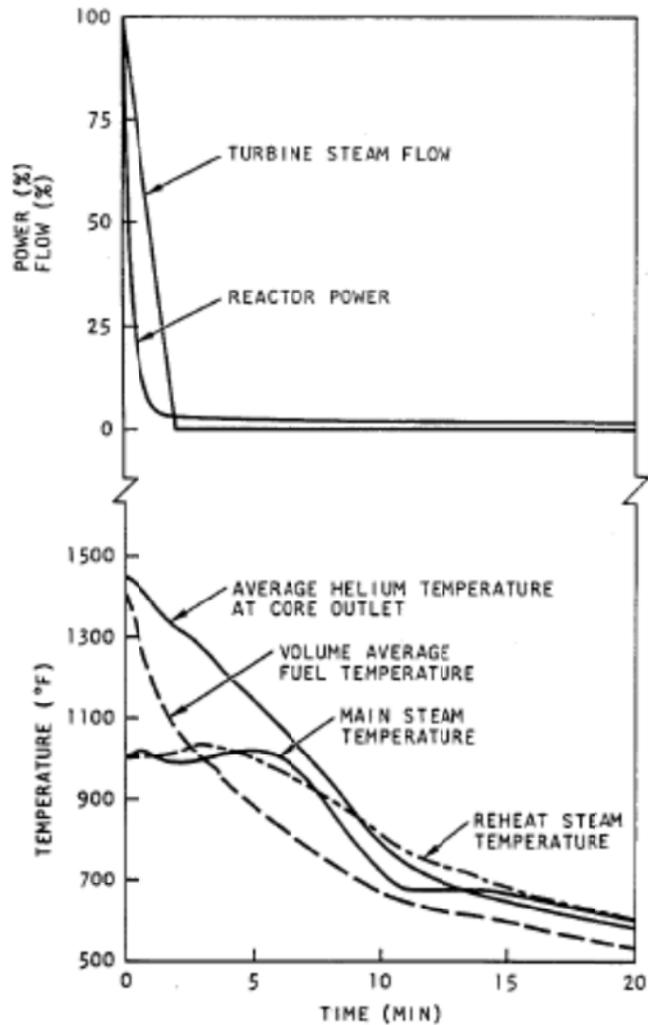


Fig. 57. Reactor scram from full power.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

4.5.9 Plant instrumentation

Nuclear instrumentation

The nuclear instrumentation (Fig. 58) monitored the neutron flux in the reactor from shutdown to well above full-power operation. The nuclear instrumentation used multiple detectors to cover the flux range for all operation—two source range, three dual range (wide range logarithmic and power range), three power range, and a control channel. The ranges overlap.

The dual range channels shared a single detector. The control channel consisted of six separate ion chambers and a linear amplifier; the control signal is an average of the six chambers. None of the channels required range switching. All circuitry was solid state.

Neutron flux and rate of flux change were indicated, alarmed, and recorded in the control room during startup and power operation of the reactor. Outputs connected into the plant protection system.

The 14 neutron detectors are located as shown in Fig. 59 in eight wells in the PCRV; none penetrates the liner. Six wells extend vertically downward from the operations floor above the reactor vessel to a position opposite the core midplane. Two vertical wells each contain two detectors (one for control, one for protection). Two startup source-range detector wells extend horizontally inward to a position over the core. Figure 59 also shows the location of the startup neutron sources.

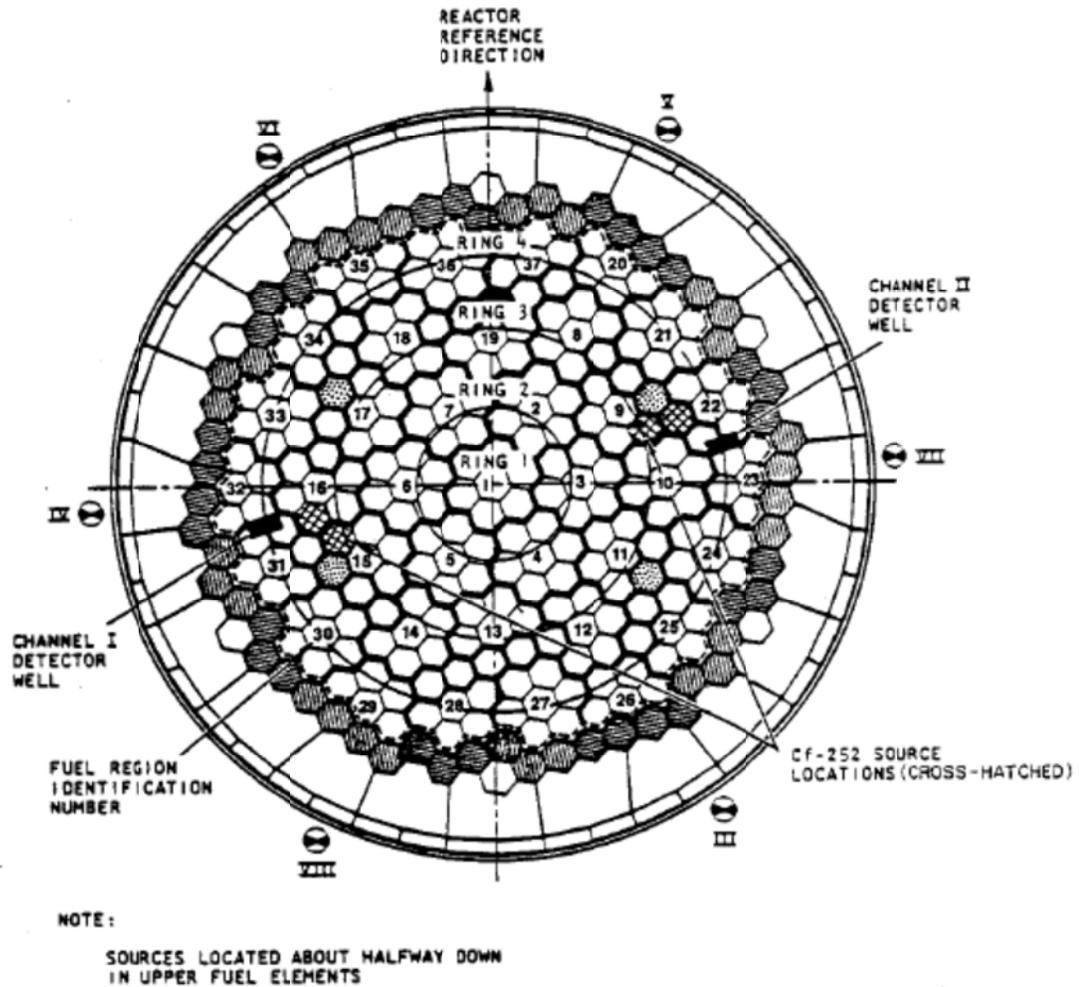


Fig. 59. Core locations for startup sources (and detectors).

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

The high-sensitivity startup detectors were B-10 lined proportional counters with a sensitivity of ~18 cps/nv in a 200 R/h gamma field. The remaining 12 detectors were dual-range fission chambers having the following sensitivities:

As a counter:

Thermal neutron sensitivity..... 0.7 cps per n/cm²-s
 Thermal neutron flux range..... ~2E+05 n/cm²-s

As an ionization chamber:

Thermal neutron sensitivity..... 1.5E-13 amp per n/cm²-s
 Gamma sensitivity..... 2E-11 amp per R/h
 Thermal neutron flux range..... ~1E+05 to 1E+10 n/cm²-s

Moisture monitoring

Fort St. Vrain had two moisture monitoring systems. One was an analytical system capable of continuously drawing coolant at any system pressure either by use of system pressure or a sample pump at low pressure. This system provided alarm and tracking capability but was not part of the plant protection system. The other system was the Dewpoint Moisture Monitoring (DPMM) system, part of the plant protection system and provided automatic corrective action in the event of water ingress. In the DPMM, three moisture detectors sampled the primary coolant continuously in each loop as shown in Fig. 60. Two of the three detectors operated in trip mode only; the third was a combination trip and indicating instrument.

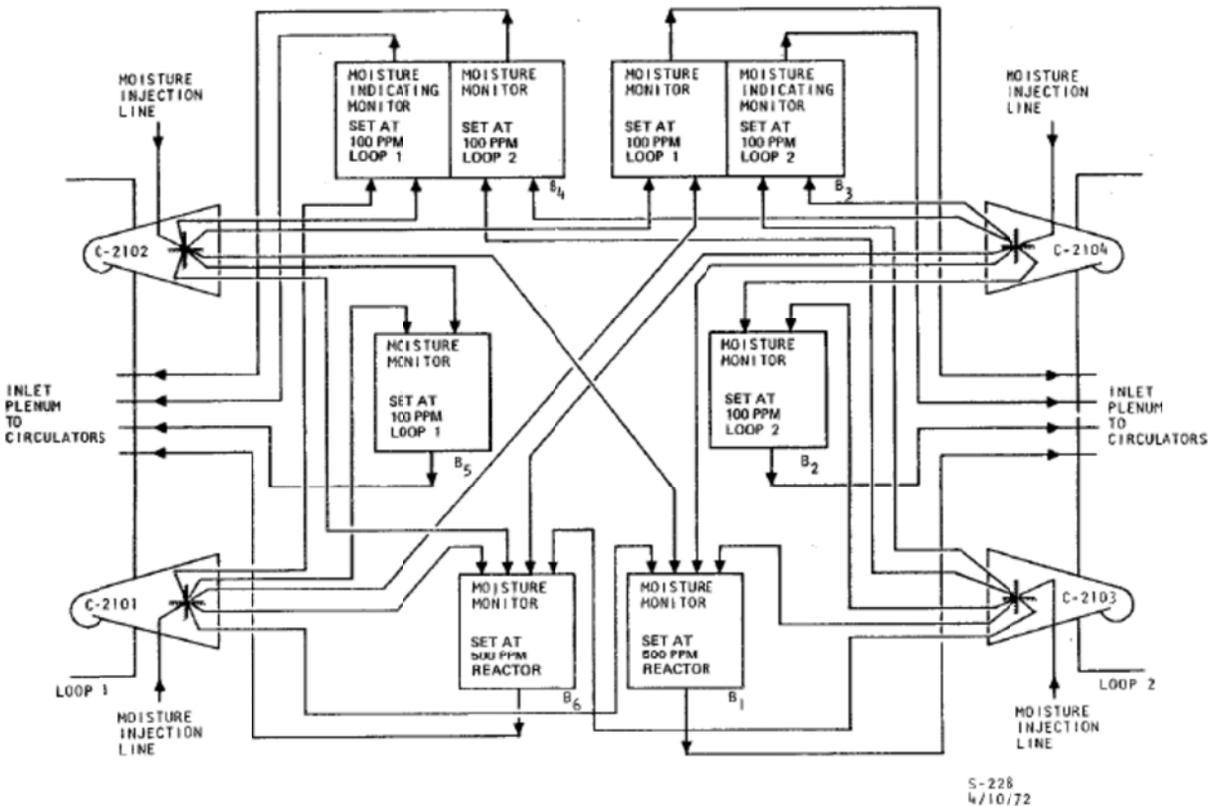


Fig. 60. Moisture sampling system.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

The trip mode operated at a fixed temperature setpoint corresponding to the dewpoint temperature of the limiting concentration for moisture in the coolant. A decrease in light reflected by the mirror indicated fogging and that moisture content was higher than the limit. The measurement gives a discrete state change at the trip point but does not give a continuous measurement of the moisture content. By contrast, the indicating mode of the DPPM increases and decreases the mirror temperature to locate the dewpoint temperature in a continuous cycle. The location of the servo amplifier indicates the instrument operation. In trip mode (Fig. 61), the servo amplifier which located near the bottom of the diagram is controlled by the temperature. The amplifier turns on the heater when the mirror temperature is below the setpoint and turns it off when the temperature is above. This mode of operation maintains the mirror at the setpoint temperature. In the indicating mode (Fig. 62), the servo amplifier, which is located near the center of the page, is controlled by the optical reflection signal. If the light is reflected, the servo amplifier turns off the heater which cools the mirror. If the light is not reflected, the amplifier turns on which heats the mirror. In this control mode, the mirror temperature tracks the dewpoint temperature. The trip limit is detected in the indicating mode of operation by detecting when the measured dewpoint temperature is less than the temperature corresponding to the limiting moisture content. The DPMM also has circuits to indicate malfunctions such as failure of the temperature controller, low flow to the cooling circuit, or failure of the servo amplifier.

All six detectors are set to trip at a moisture concentration of 100 ppmv of 4.83 MPa (700 psia) pressure [ppmv is *parts per million by volume*]. Two additional trip instruments sample a mixture of primary coolant gas from both loops and are set to trip at a moisture concentration of 500 ppmv at 4.83 MPa (700 psia) pressure. The three-detector system identifies the leaking loop; the two-detector system detects high moisture for reactor scram.

Temperature, pressure, and flow

Outlet coolant thermocouples measured the temperature of the coolant gas at the outlet of each of the 37 fuel regions and were used for high temperature alarm. The outlet coolant temperatures were used in conjunction with the hot reheat steam temperature to adjust the core orifices and to estimate fuel temperatures.

Reactor pressure was required to be measured by three independent pressure sensors for the reactor protection system. Each measurement was fully redundant from transducer to the protection system including electronics and power supply. A total of six pressure sensors were installed (three operational and three spares), each in a separate penetration. The pressure transducers had the capability for online testing. A line at the inlet to the PCRV pressure transducer was utilized for operational checks and calibration of the transducers. The instrument was checked by connecting a helium cylinder to the line and pressurizing the line to above the pressure of the PCRV. A restrictor in the sampling line to the transducer allowed helium from the cylinder to flow into the PCRV; the differential pressure across the restrictor and sensing line, plus the PCRV pressure, was then measured by the instrument. This test allows a quick operability check of the transducer to demonstrate that it responded to a pressure increase. The same test facility was used for calibration but required access to the penetration interspace to close the isolation valves in the sensing lines.

In addition to the main reactor pressure instrumentation, the low-range primary coolant pressure was monitored during the late phase of depressurization, shutdown, and early part of repressurization. A differential pressure transducer was provided to monitor the core pressure drop.

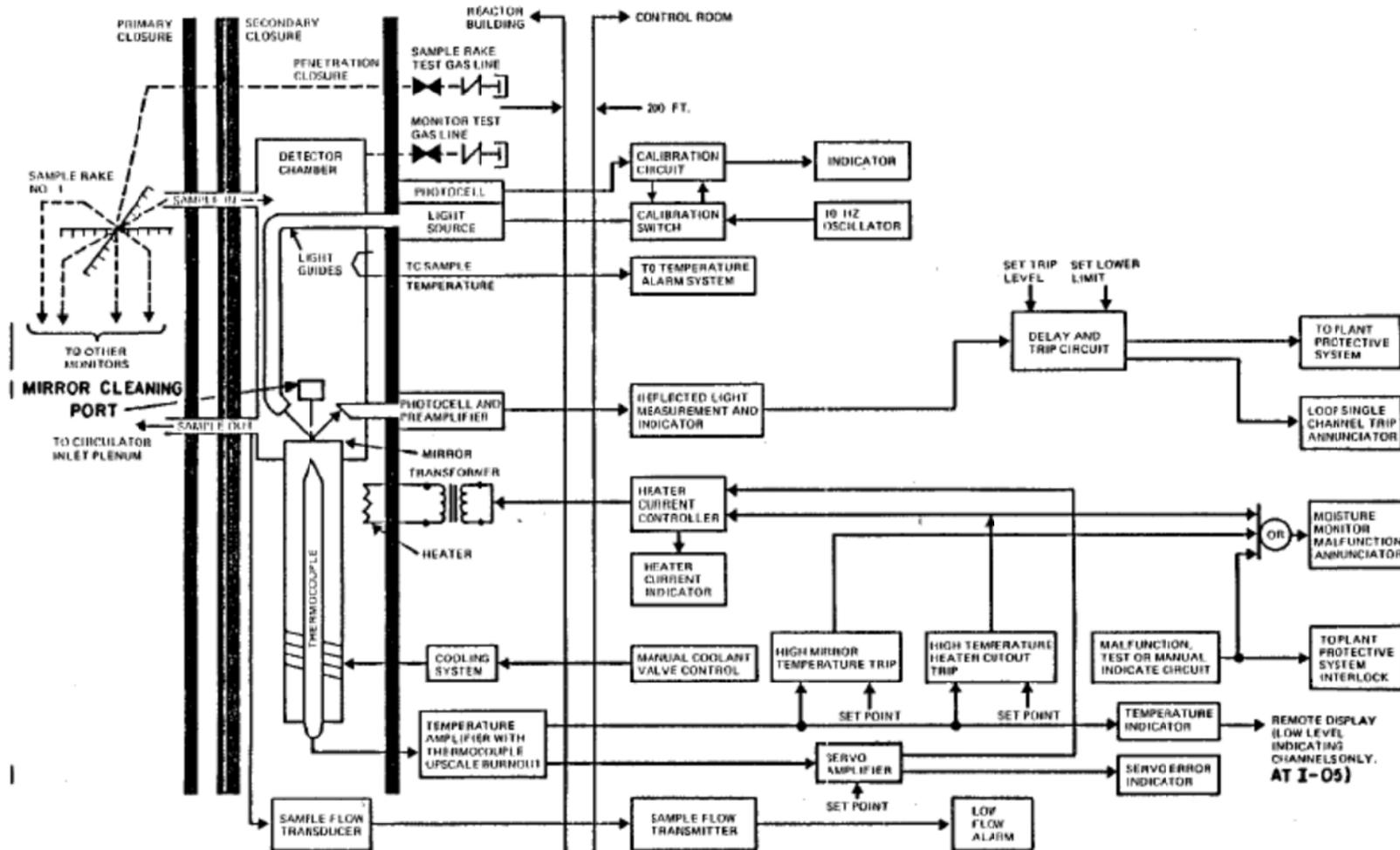


Fig. 61. Moisture detector—operating in trip mode.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

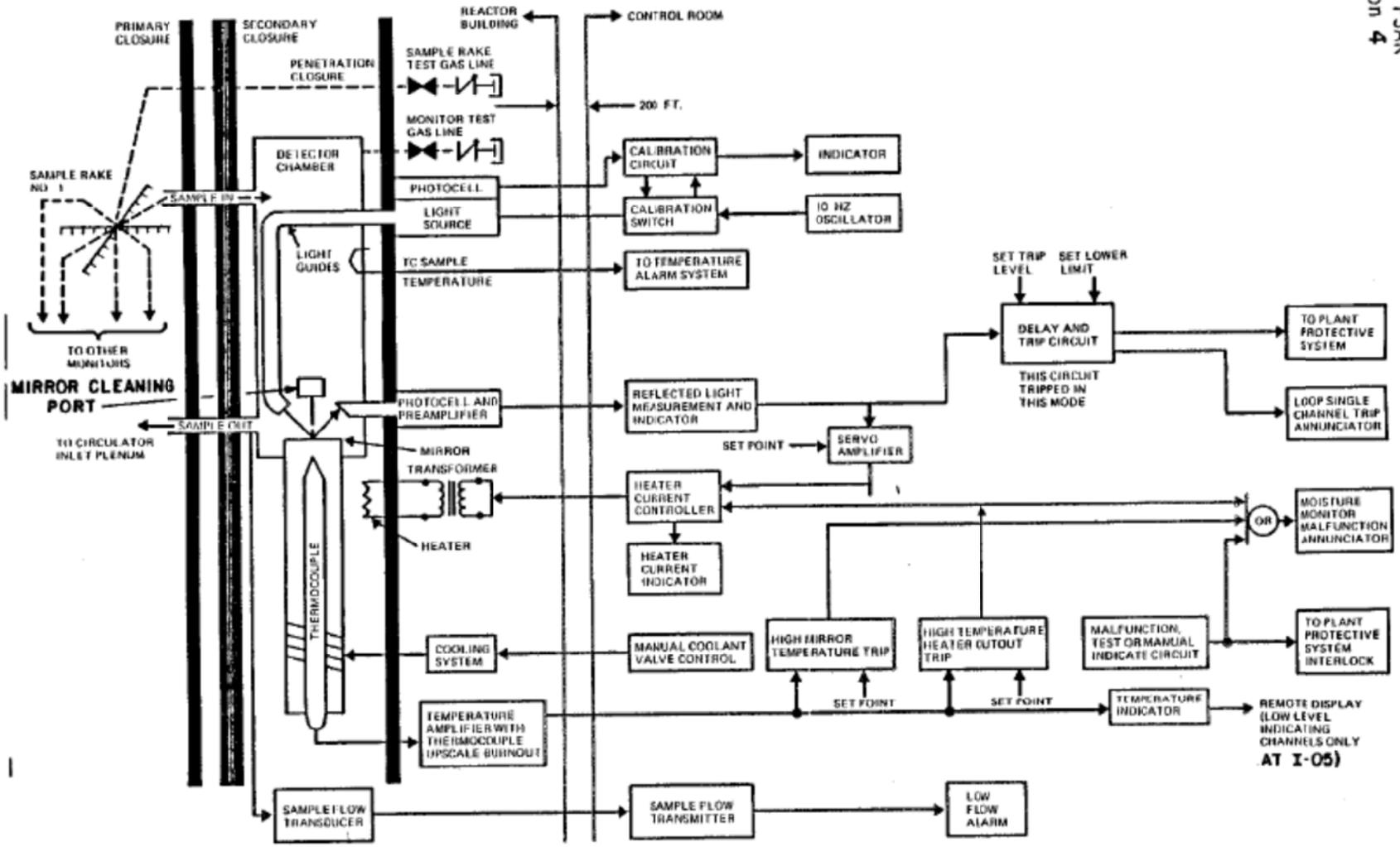


Fig. 62. Moisture detector—operating in indication mode.

[Fort St. Vrain FSAR, Revision 7, Chapter 7]

Mass flow in each circulator was computed from differential pressure across the circulator inlet nozzle. The flow was compensated for helium density using the circulator inlet temperature measurement and a common pressure measurement at the inlet plenum. Power-to-flow measurement was accomplished by totaling the coolant mass flow from the circulators and taking the ratio of total flow to reactor power. The power-to-flow ratio measurement system was not safety-related (not PPS, Class 1 nor required for safe shutdown), and did not initiate any automatic protective system or control system actions as in some GCRs. (It is comparable to LWR post-accident monitoring instrumentation such as LWR reactor coolant system subcooling margin monitor, etc.)

Radiation monitoring

The hot reheat steam lines and the outlet of the main condenser air ejector were monitored for possible leakage of radioactive contaminants from the primary. Two sets of three redundant detectors were located adjacent to each of the two hot reheat loop headers and were shielded from background by 1.5 in. of lead. The two sets of monitors were part of the protective system. Each set was connected in 2/3 coincidence.

Other radiation detectors monitor the loop header condensate, the exhaust line of the air ejector, and the reactor building ventilation exhaust.

4.5.10 Safety evaluation

Upgraded final safety analysis report

Chapter 14 of the Fort St. Vrain Upgraded Final Safety Analysis Report (UFSAR) provides a complete review of the safety events and their evaluations that are considered in the Fort St. Vrain safety analysis. The availability of the FSAR gives a more complete evaluation of this plant than is possible with the other reactors considered in this summary. Only a summary of the analysis is given in this section. Considerably more information is contained in the UFSAR.

The UFSAR divides the events considered into categories:

1. Environmental events
 - Events including seismic, wind, flood, fire, landslides, snow and ice, and explosions from nearby natural gas wells
2. Reactivity accidents and transients
 - Upsets from various reactivity sources and from rod withdrawal incidents
3. Incidents
 - Miscellaneous structural events
 - Primary coolant events including malfunctions of helium circulators and their auxiliary system
 - Malfunctions of the instrument and control systems
 - Malfunctions of the electrical system
 - Malfunctions of the helium purification system
 - Malfunctions of the helium storage system
 - Malfunctions of the nitrogen system
 - Malfunctions from handling heavy loads

4. Loss of normal shutdown cooling
 - Cooling on one steam driven circulator
 - Cooling with one water driven circulator
 - Partial loss of circulators (at least one circulator operational) and depressurization events
 - Heat removal events (e.g., flooded reheater, loss-of-coolant flow for less than 30 minutes)
5. Secondary coolant system events
 - Steam leaks inside and outside the PCRV
 - Steam/water leaks into primary
6. Auxiliary system leakage
 - Failures of the helium purification failure
 - Accidents involving the gas waste system
7. Primary coolant leakage

The design basis events are events that are the worst case events conceivable. Two events were originally considered credible. Design Basis Accident No. 1 was the permanent loss of forced circulation. Design Basis Accident No. 2 was a rapid depressurization event.

The permanent loss-of-forced circulation would require the extended failure of all four helium circulators, their steam and water drives or their multiple sources of motive power, or failure of both the main steam and reheat steam sections of both steam generators. Two hours following loss of forced circulation at full power the plant operator would begin depressurization of the primary coolant system. The PCRV was depressurized through the helium purification system and the reactor building vent stack filters to atmosphere. When the operator realized that the loss of circulation was permanent, about 5 hours following the loss of forced circulation, the reserve shutdown system would be operated to assure adequate shutdown margin. The PCRV cooling water system would continue. Two separate identical closed loops supplied cooling water to the separate zones of the PCRV—top head penetration, core support floor, PCRV liner on side wall and top head, and PCRV bottom head and bottom penetrations. The assumed case had only one loop operating. This accident involved core damage and fission product release causing offsite doses. The peak core temperature reached 2982°C (5400°F); approximately 95% of fuel particles suffered failed coatings, releasing 28% of the core fission product inventory (less than 5% gas borne in the PCRV). The 6-month doses at the low-population zone boundary were 0.37 mrem whole body gamma, 36 mrem thyroid, and 1 mrem bone. [FSAR Chap. 14 Rev. 5]

The Design Basis Accident No.2, (DBA-2) “Rapid Depressurization/Slowdown,” was a rapid depressurization/blowdown from a hypothetical sudden failure of both closures in the bottom head access penetration. This accident was not considered credible [FSAR Chap 14 Rev. 8] because it required failure of two safety valves in the reactor penetration closure to fail. The UFSAR has retained the analysis of the event for historical purposes.

In DBA-2, blowdown of the PCRV to atmospheric pressure is completed in about 2 minutes. A reactor scram would occur on low primary coolant pressure with forced circulation cooling being continued by auto-start of the Pelton wheels using feedwater. In the analysis performed in UFSAR Section 14.11.2.2, forced circulation cooling was assumed to be interrupted until the auto-start of the helium circulator Pelton wheels occurring 5 minutes into the accident. The analysis indicates a peak fuel temperature of 1427°C (2600°F), which is below the conservative FSAR temperature limit of 1593°C (2900°F), a temperature well below that at which rapid fuel deterioration is expected to occur. Ambient reactor building temperatures would quickly peak at 131°C (267°F) with an elevated high temperature and a rate-of-rise sufficient to trip SLRDIS. This would result in isolation of all secondary coolant flow not permitting forced circulation cooling to be quickly re-established as assumed in the current FSAR accident analysis.

Delay times of 30 and 60 minutes for manual restart of forced circulation were considered in the analysis. For a 60 minute delay in restart of forced circulation, the maximum fuel temperature is 1543°C (2810°F). This maximum fuel temperature satisfies the conservative FSAR temperature limit of 1593°C (2900°F), a temperature well below that at which rapid fuel deterioration is expected to occur. Average core outlet gas temperature is less than 1093°C (2000°F) and, therefore, is acceptable regarding Class B thermal barrier insulation. The total amount of graphite oxidation due to air ingress for the 60-minute interruption in forced circulation is 10.5 kg (23 lb). This amount of oxidation is not significant.

The UFSAR concluded that while rapid depressurization would result in an interruption of forced circulation due to actuation of SLRDIS, sufficient time existed for the operators to restart forced circulation cooling with no change in the accident consequences. The need for forced circulation and the reliance in some scenarios on non-safety equipment for pressurized water supply for the steam generator cooling and for motive power for the helium circulators is one of the weaknesses in the safety case that is addressed in other designs by sufficiently low-power density that passive reactor cavity cooling systems can maintain safe fuel temperatures in a depressurized loss of forced circulation.

4.5.11 Evaluation of operating experience

In 2003, a study was conducted by Oak Ridge National Laboratory to assess the operational experience of Fort St. Vrain using the monthly operating experience reports produced by ORNL during the years 1981 through 1989.⁴⁰ The report was produced under contract to the NRC to capture lessons learned from the Fort St. Vrain experience for future GCRs that might be built.

The monthly reports which were the source material for the analysis were generated by ORNL from Licensee Event Reports. ORNL filed 96 monthly reports with the AEOD between 1981 and 1989. These monthly reports were reviewed again in the ORNL study. The 279 events reported in the set of monthly reports were catalogued into one of seven categories: (1) 29 water incursion events and failures of moisture detection systems; (2) two air or other unwanted gas incursion events and failures of gas detection systems; (3) three fuel failures or anomalies; (4) two failures or cracks in graphite, pipes, and other reactor structural components; (5) no failures of nuclear instrumentation systems; (6) 47 human factors and operator performance issues; and (7) 196 other events or conditions that may be relevant to current GCR designs. The assessment of the categories given in the report is as follows:

1. *Moisture Intrusion*

The moisture intrusion events had the greatest safety significance. The 29 events were placed into one of four subcategories as follows: (1) 18 were classified as thermal-hydraulic moisture outgassing events, (2) four were determined to be tube leaks, (3) five involved moisture detection instrumentation failures, and (4) two were a plugging of or an obstruction of process lines.

2. *Gas Intrusion*

The two instances of helium leaks did not present a safety hazard at Fort St. Vrain.

3. *Fuel Failures*

A dropped Lucy Lock (a Lucy lock is a mechanical device to maintain uniform spacing of prismatic fuel elements) to the top of the core during a refueling outage did not damage the fuel. Another event caused only slightly skewed radial and axial power profiles; however, there was no adverse power peaking. A third event was a failed surveillance on one hopper.

⁴⁰D. A. Copinger and D. L. Moses, *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, NUREG/CR-6839 (ORNL TM-2003/223), September 2003.

However, the system would still have been able to perform its design safety function. Based on these assessments, the three incidents did not present a safety hazard at Fort St. Vrain.

4. *Structural or Graphite Failures*

Routine inspections discovered superficially cracked fuel element webs that were not considered a safety issue at Fort St. Vrain. Corroded prestressed concrete reactor vessel tendon wires also did not present any undue safety hazards to Fort St. Vrain.

5. *Human Factors*

There were no extraordinary human factors issues uncovered as part of this analysis, and they did not present a safety hazard at Fort St. Vrain.

6. *Instrumentation and controls*

No failures of nuclear instrumentation systems were recorded.

7. *Other*

The potential safety consequences from the 196 other events were collectively representative of routine operational events at Fort St. Vrain. A more detailed analysis of the 196 events may reveal a hidden component or cause that was not apparent from the study.

4.5.12 Significant issues

The safety consequences from moisture intrusion events at Fort St. Vrain are arguably the single most important issue identified in the operation of the plant. The events directly affected the plant's safety and accident analyses. While the final safety analysis report accident analysis accounted for large moisture incursions over the short term, the long-term effects from a small incursion (i.e., low volumetric or inleakage rates) were not clearly understood or appreciated, and ultimately these had a much greater effect on plant operations. Small amounts of moisture degraded both the control rod drive and reserve shutdown systems. Moreover, six control rod pairs failed to scram during an event on June 23, 1984. This failure to guarantee a plant shutdown when required represented a significant safety hazard for plant operations. Low levels of moisture were a common cause effect leading to the failure of the both the primary and backup scram mechanisms.

The Fort St. Vrain plant required forced circulation from two loops for a trip with maximum decay heat. Providing a primary and backup safety related means for power to the helium circulators required an extensive list of plant equipment. The analysis of that system was difficult to analyze and to license. Later generations of GCRs were designed and sized for passive decay heat removal at temperature levels below the point at which fuel particle failure would occur. Other revisions based on the Fort St. Vrain circulator problems were the use of a separate shutdown cooling system rather than the main helium circulators for normal plant post-shutdown cooling and the use of electric drives for the helium circulators rather than steam and water turbines.

4.6 10 MW High Temperature Gas-Cooled Test Reactor (HTR-10)

4.6.1 Reactor system design

The HTR-10 design, as described by Wu,⁴¹ is a Chinese pebble bed reactor core with online refueling based on the German HTR-Module design. The objective of the HTR-10 for the emerging Chinese nuclear power plant industry is to verify and demonstrate the technical and safety features of the modular HTGR

⁴¹Z. Wu, D. Lin, and D. Zhong, "The Design Features of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 25–32 (2002).

and to establish an experimental base for developing nuclear process heat applications and the gas turbine cycle for electricity production. The specific goals of the HTR-10 have been defined as follows:

- acquiring expertise in the design, construction, and operation of HTGRs;
- establishing an irradiation and experimental facility for fuel elements;
- demonstrating the inherent safety features of the modular HTGR;
- testing electricity/heat co-generation and gas turbine technology; and
- carrying out R&D on high temperature process heat application.

The HTR-10 is the first step of development of modular high temperature gas-cooled reactors in China. The HTR-10, in its initial configuration, provides co-generation of electricity using a once through steam generator and conventional steam turbine and district heating with its rated 10 MW thermal power. A planned future upgrade of the test facility will increase the helium operating temperature to allow operation of a gas turbine topping cycle. The modified system will incorporate an intermediate heat exchanger (IHX) in series in the steam generator. The secondary side of the IHX will use nitrogen gas as the working fluid and will be connected to a gas turbine for energy conversion. The steam turbine and gas turbine will operate together as a combined cycle plant.

The pebble bed core of HTR-10 contains about 27,000 spherical fuel elements of 6-cm diameter. The fuel elements contain TRISO coated fuel particles in much the same design as the AVR fuel. The core region is 180 cm in diameter and 197 cm in average height. The mean power density of the core is 2 MW m^3 . The small physical size of the core and low power density contribute to the ability to use inherent heat removal for decay heat removal. The HTR-10 is refueled online.

The upper, side, and bottom graphite reflectors surround the reactor core. Each layer of the side reflector consists of 20 segmented graphite bricks with drilled channels for ten control rod channels, seven absorber ball channels, and three experimental channels. In addition, 20 cold helium channels are located in each layer of the side reflector to reduce the graphite temperature under operating conditions and to aid in cooling the core under accident condition due to the large heat capacity of the graphite structure. The bottom structure of the core is a conical section with a 30° angle to allow free movement of the fuel elements into the refueling system by gravity. The heated helium gas flows through the channels in the bottom reflector graphite bricks and into the hot gas chamber, and then out of the reactor vessel through the hot gas duct which connects the reactor vessel with steam generator. The inner surface of the side reflector has dish-like indentations to prevent pebbles from forming a rigid bridge structure that would prevent free movement of fuel pebbles down the internal wall surface of the reflector.

Boronated carbon bricks surround the graphite reflector. The carbon and boronated carbon bricks serve as thermal insulation to reduce heat loss from the core and as neutron shielding to protect the core barrel and the reactor pressure vessel from neutron irradiation damage. The graphite and carbon bricks are connected vertically with a dowel and socket system, and horizontally with the key and keyway system to insure the mechanical stability of the core structure and to prevent the formation of gaps which would allow excess bypass flow. The dowels and keys are made from graphite material. The ceramic internals are supported on a metallic lower support plate and are connected with the core vessel by metallic keys. The bottom of the metallic internal structure is supported on the inside flanges of the reactor pressure vessel wall by ten roller bearings. The movable structure allows differential thermal expansion between the metallic internal structure and the reactor pressure vessel. A cross section of the reactor structure of the HTR-10 is shown in Fig. 63.

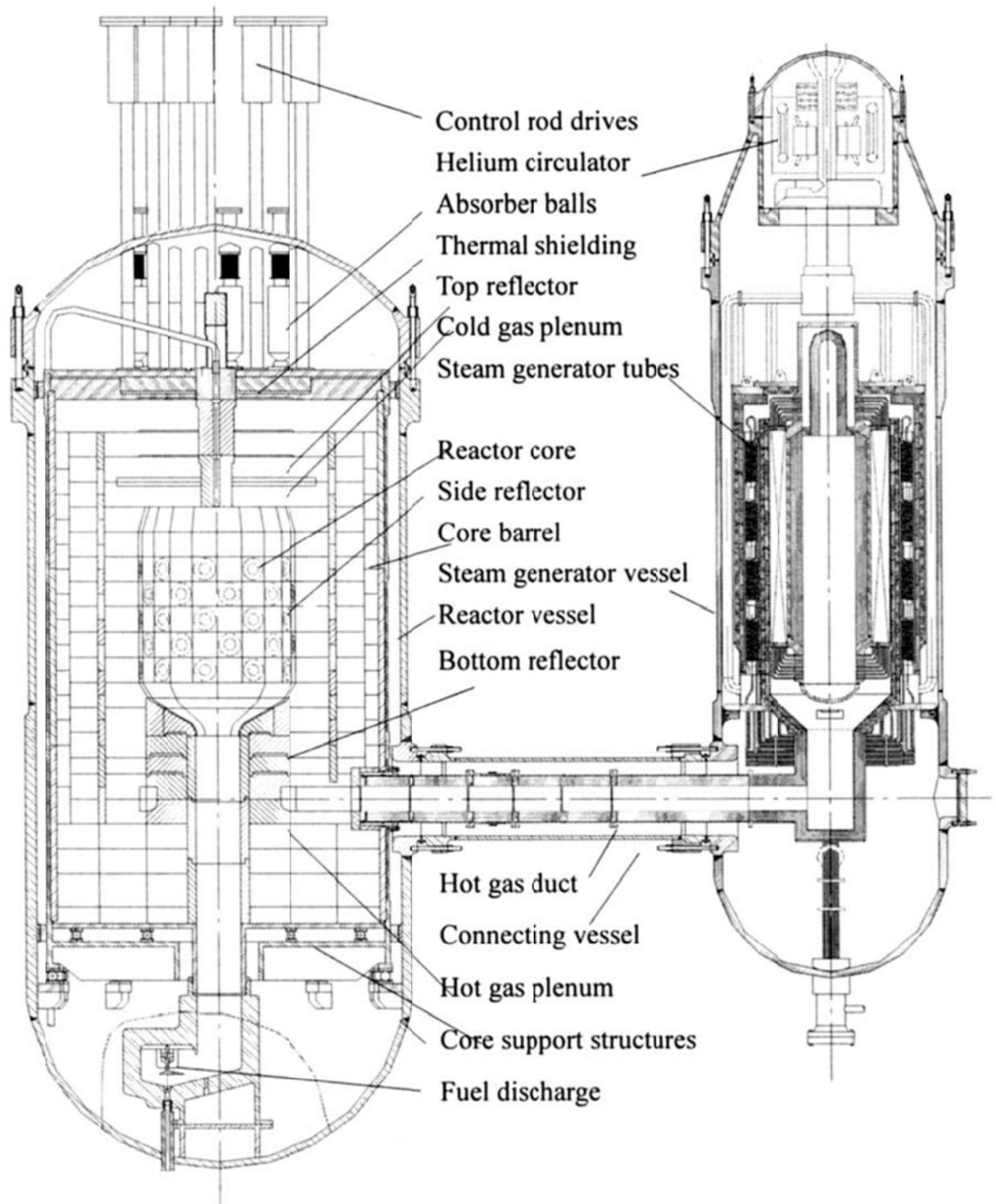


Fig. 63. The HTR-10 reactor and steam generator arrangement in the primary cavity.

[Z. Wu, D. Lin, and D. Zhong, "The Design Features of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 25–32 (2002).]

The HTR-10 uses chemically inert helium gas as coolant. The cold helium enters the core at an inlet temperature of 250°C. The coolant flows up through the reflector and then flows downward through the pebble bed core exiting the core with an average temperature of 700°C. Under normal operating condition, the peak fuel temperature occurs near the core outlet. One of the benefits of the concurrent flow design in which both fuel and coolant flow downward in the core is that the higher burnup fuel and the higher coolant temperature both occur near the outlet. Both burnup and Doppler feedback tend to reduce the flux peaks in the lower region of the core. The co-current flow has the beneficial effect of reducing the peak fuel temperature in comparison to counter current flow of fuel pebbles and coolant as in the AVR.

The main design parameters of the HTR-10 are summarized in Table 21. The main features of the reactor are shown in Fig. 64.

4.6.2 Heat transport loop

The reactor vessel and the once-through steam generator shell are steel pressure vessels arranged side by side as shown in Fig. 63. The two vessels are connected by the annular hot gas duct. The flow path is designed so that the pressure vessel walls of the reactor, steam generator, and hot gas duct are in contact with the cold helium (about 250°C) as it leaves the circulator. The hot gas flows in the interior of each vessel. This arrangement protects the metallic surfaces from the hot gas temperature. The helium circulator is located on top of the steam generator vessel. The helium enters the main circulator from the annular tube bundle. The pressurized helium flows down the outside of the steam generator to the outer coaxial pipe of the hot gas duct. It enters the channels in the side reflector, and then flows through these channels from bottom to top. The cold gas turns downward in the upper plenum and enters the reactor core region passing through the pebble bed from top to bottom where it is heated to a temperature of about 700°C. The hot helium exits the hot gas chamber in the bottom reflector and flows through the hot gas duct to the steam generator. The heat from the helium is transferred to water in the secondary circuit to produce steam. The temperature of the helium at the exit of the steam generator is 250°C.

The advantages of the side-by-side arrangement of the reactor and steam generator are the ease of maintenance and the reduced probability of a steam generator tube rupture resulting in water entering the reactor core. Both maintenance and water intrusion were problematic for the AVR design with the steam generator above the reactor in a single vessel. The once through steam generator has 30 helical tube bundle modules. A small helical tube bundle with a diameter of 112 mm is contained within each module. The heat transfer tubes are constructed with 2-1/4 Cr-1 Mo and can withstand temperatures up to 500°C. Figure Fig. 63 shows the HTR-10 reactor and steam generator arrangement in the primary cavity.

4.6.3 Online refueling

The reactor has an online refueling system similar to the AVR reactor described in Sect. 4.3. The HTR-10 refueling apparatus is shown schematically in Fig. 64.⁴² Loss of reactivity in the core over time can be compensated by adding fresh fuel pebbles from the top of the core. The fuel pebbles are circulated through the core region an average of five times before their burnup limit is reached. The mixture of fresh and burned fuel in the ‘multi-pass’ scheme reduces the power peaking factor of the HTR-10 in comparison to a single pass.

⁴²Y. Yang, Z. Luo, X. Jing, and Z. Wu, “Fuel Management of the HTR-10 Including the Equilibrium State and the Running-In Phase,” *Nuclear Engineering and Design*, **218**, pp. 33–41 (2002).

Table 21. Major design parameters of the HTR-10 test reactor⁴³

Item	Unit	Value
Core		
– Thermal power	MW	10
– Reactor core diameter	cm	180
– Average core height	cm	197
– Primary helium pressure	MPa	3.0
– Average helium temperature at reactor inlet/outlet		
– Helium mass flow rate at full power	°C	250/700
– Average core power density	kg s ⁻¹	4.3
– Power peaking factor		
– Number of control rods in side reflector	MW m ⁻³	2
– Number of absorber ball units in side reflector		1.54
		10
		7
Fuel		
– Nuclear fuel		UO ₂
– Heavy metal loading per fuel element	g	5
– Enrichment of fresh fuel element	%	17
– Number of fuel elements in core	Multipass	27,000
– Fuel management		
– Average residence time of one fuel element in core	ERPD	1080
– Max. power rating of fuel element	kW	0.57
– Max. fuel temperature (normal operation)	°C	919
– Max. burn-up	MWd tHM ⁻¹	87,072
– Average burn-up	MWd tHM ⁻¹	80,000
– Max. thermal flux in core (E>1.86 eV)	n cm ⁻² s ⁻¹	3.43 × 10 ¹³
– Max. fast flux in core (E>1 MeV)	n cm ⁻² s ⁻¹	2.77 × 10 ¹³

⁴³Wu, *op. cit.*

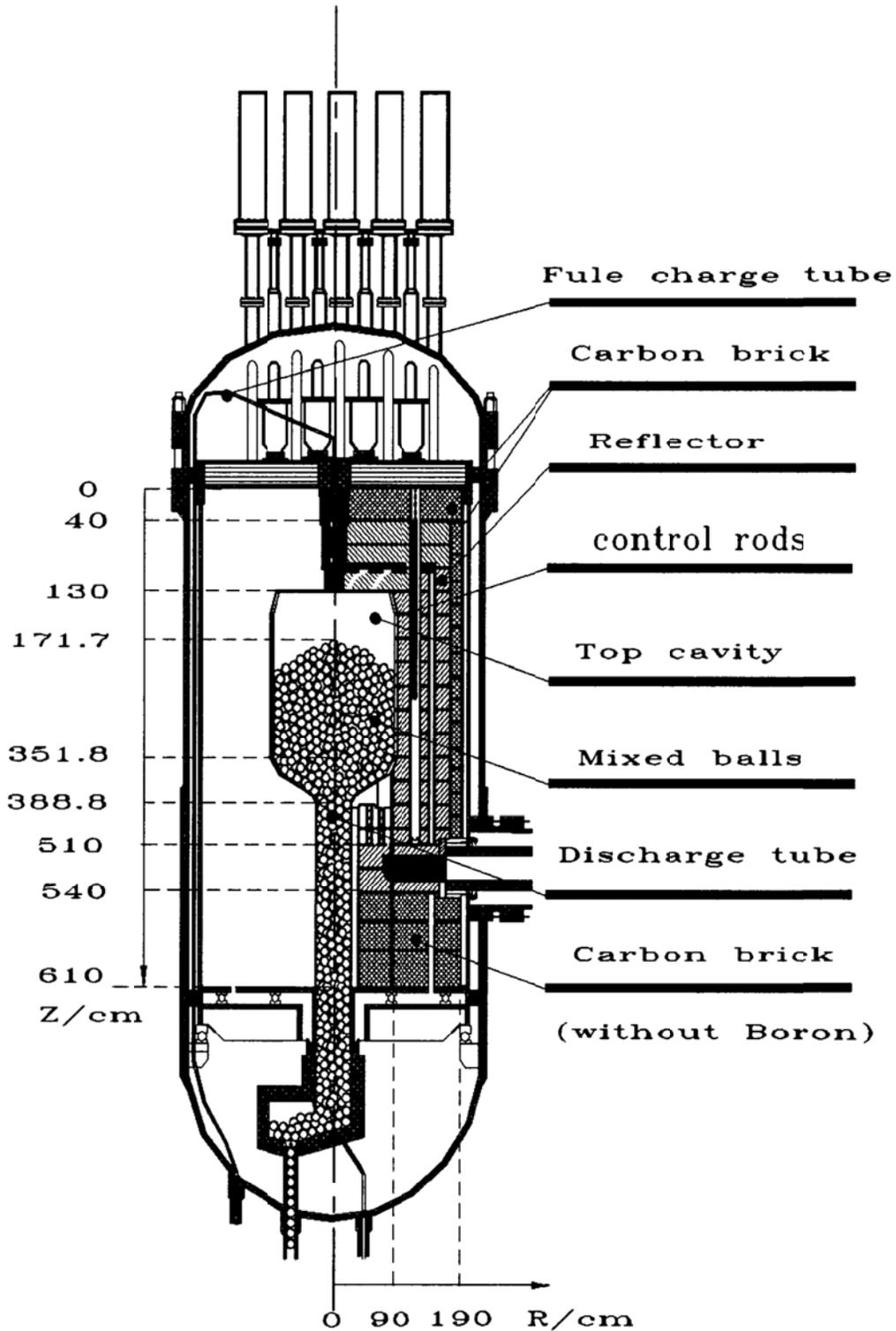


Fig. 64. Online refueling system; cross-section of the HTR-10.

[Y. Yang et al., "Fuel Management of the HTR-10 Including the Equilibrium State and Running-In Phase," Association of German Engineers (VDI), *Nuclear Engineering and Design*, **218**, pp. 33–41 (2002)].

The fuel elements drop into the reactor core from the central fuel charging tube. An estimated space of 40 cm height between the top of the pebble bed and the bottom of upper graphite reflect provides a margin for accommodating the criticality calculation uncertainty and burnup. The fuel elements move downward through the reactor core and discharge through a tube of 50 cm inside diameter at the core bottom. A singularizer lines up fuel elements and separates individual spheres for testing one by one.

The defective fuel elements and the scrap fragments are detected by the refueling system and diverted into a scrap container. The burnup for each fuel pebble is measured in the refueling apparatus. Elements which have not reached the burn-up target are re-circulated into the reactor core. The spent fuel elements exceeding the burnup target are discharged and transported into the spent fuel storage tank. New fuel elements to compensate for burnup are loaded into the core via a special pressurized charging facility to prevent air from entering into the primary system or coolant being released into the environment. Fuel elements are conveyed through the fuel handling system by pneumatic force and gravity.

4.6.4 Confinement

The HTR-10 adopts the confinement rather than containment strategy. As described by Wu,⁴⁴The concrete compartment around the pressure vessel is not a sealed containment designed to retain released gases throughout any accident as in a conventional PWR. This confinement design is permissible because the safety analysis of the plant shows that radioactive release in all safety events is below allowable limits for the following reasons.

1. No possible accident can cause the fuel elements to exceed their temperature limit and lead to widespread release of fission products from the fuel particles.
2. The uranium content of the fuel elements is low.
3. The graphite retains a significant fraction of the radioactive contamination released by any failed fuel particles.
4. Activated corrosion products in the primary coolant are negligible.

The HTR-10 relies on confinement of the reactor atmosphere to allow retention of contaminants from the reactor and filtering before release when needed. Concrete compartments which house the reactor vessel, the steam generator vessel as well as other parts of primary pressure boundary are designed to be leak-tight and serve as the confinement. While the concrete structure does not have sufficient pressure capacity to withstand a total core depressurization event, the confinement, together with the accident ventilation system, serves as a barrier against the release of radioactivity into the environment.

During normal operation conditions the exhaust system maintains the cavity of the concrete compartments at negative pressure to prevent the dissipation of radioactivity inside the cavity into the reactor building. The air from the confinement building is filtered before exhaust via the chimney to minimize the impact on the environment according to the ALARA (as low as reasonably achievable) principle.

In depressurization accidents, when the pressure inside the cavity exceeds 0.1 bars above atmospheric pressure, a rupture disk in the exhaust pipe automatically opens. The air exiting the cavity initially is not filtered but is released directly into the atmosphere via the chimney. The design of the confinement is based on a concept of lowest risk release. In a severe depressurization accident, the release of radioactivity can be divided into two parts, the prompt release and delayed release. Gaseous fission products in the helium coolant and solid fission products deposited on the graphite dust are transported to the break by the flow of the helium coolant. However, the initial part of the release contains relatively low contamination because of normal operating controls and purification of the coolant. The main danger of the initial release is the high volume and energy of the initial release that could potentially damage the filters. The delayed release of the depressurization has the potential for higher contamination because, as

⁴⁴Wu, *op. cit.*

the accident progresses, fuel elements may be damaged by the higher, post-accident temperatures or by the introduction of air or water into the core. This delayed release could last for several tens of hours. Therefore, the prompt release without filtering of the initial depressurization protects the filters from use and damage by the initial high energy and volume prompt release and conserves the filters for the delayed stages of the transient with lower volume but potentially higher contamination.

4.6.5 Shutdown cooling system

During normal shutdown operation, core decay heat is removed by the main heat transport loop. The main heat transfer system is composed of the primary helium circulator, steam generator and feed pump, and circulating water system. The primary helium circulator cools the core and transfers to the start up and shut down system through the steam generator. Heat is removed from the secondary side of the steam generator by the circulating water system. In a depressurization event, the main heat transfer system is ineffective due to the reduced density of the coolant. However, analysis shows that no forced circulation core cooling is needed at all. Decay heat can be dissipated via the core structure by means of heat conduction and radiation to the outside of the reactor pressure vessel, where a reactor cavity cooler is installed on the wall of the concrete housing cavity. The reactor cavity cooling system is connected to the air coolers on the top of the reactor building. The RCCS is a passive, natural circulation heat transport loop that conveys the decay heat to the atmosphere via the air coolers.

The HTR-10 has two independent of RCCS trains for passive decay heat removal system. Each train has the capacity to remove 100% of decay heat. The core diameter of HTR-10 is small and the average power density is low, therefore, the maximum fuel temperature in a depressurization event with the passive RCCS is more or less equal to normal operating conditions with forced flow and 100% power. Even in the extreme condition of the failure of both trains of the RCCS, the core could dissipate its decay heat through the wall of reactor concrete to the surrounding earth. The maximum temperature of fuel elements in this beyond design basis event would be below the temperature limit of 1600°C.

Analysis also shows that the cooling system for the concrete reactor housing cavity, which is designed to provide for cooling for the vessel and its support in normal operation, will keep the fuel temperature in the allowable range if neither the main heat transport loop nor the RCCS is available. The instrumentation of and surveillance for cavity cooler are maintained to ensure the operability and control of the cavity cooling as necessary for emergency conditions.

4.6.6 Helium purification plant

The helium purification system⁴⁵ of the HTR-10 purifies a bypass stream from the primary coolant system to remove chemical impurities, such as hydrogen, carbon monoxide, carbon dioxide, water vapor, oxygen, nitrogen, methane, and gaseous radionuclide fission products such as krypton, xenon etc. in the primary coolant helium. The system also removes particulate solids produced by abrasive action of the pebble flow. The normal sources of contaminants are low level quantities of air or moisture that are desorbed from reactor components, residual air, air in-leakage, fission products that migrate from the fuel, moisture from steam generator leakage, and contaminants from new helium supply. The helium purification system is not a safety grade system and is not credited in the safety analysis of the reactor. However, moisture removal purification is important for the post-accident operation in water ingress events. Consequently, a postaccident purification train, consisting of a cooler and a moisture separator, is provided.

The helium purification system, shown in Fig. 65 of is composed of a cartridge filter, a copper oxide bed, a molecular sieve adsorber, a low-temperature adsorber, and two diaphragm compressors. The cartridge filter at the beginning of train removes particulate impurities. For particles of 5 µm or larger, a retention

⁴⁵ M. Yao, R. P. Wang, Z. Liu, X. He, and J. Li, "The Helium Purification System of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 163–167 (2002).

efficiency of almost 99% can be attained. The first stage of the gas purification train is a high temperature copper oxide bed with a temperature of 250°C for oxidation of hydrogen and carbon monoxide. Molecular oxygen is also simultaneously removed by adsorption onto the high-temperature copper in the unit. The second stage is a room temperature molecular sieve adsorber which adsorbs the reaction products of water vapor and carbon dioxide from the first stage. The third stage is a low temperature (~160°C) activated carbon adsorber, which retains the remaining impurities. The purification system components are designed for a service life of more than 2000 h at normal operation and are used for both the circulating helium and for newly delivered helium.

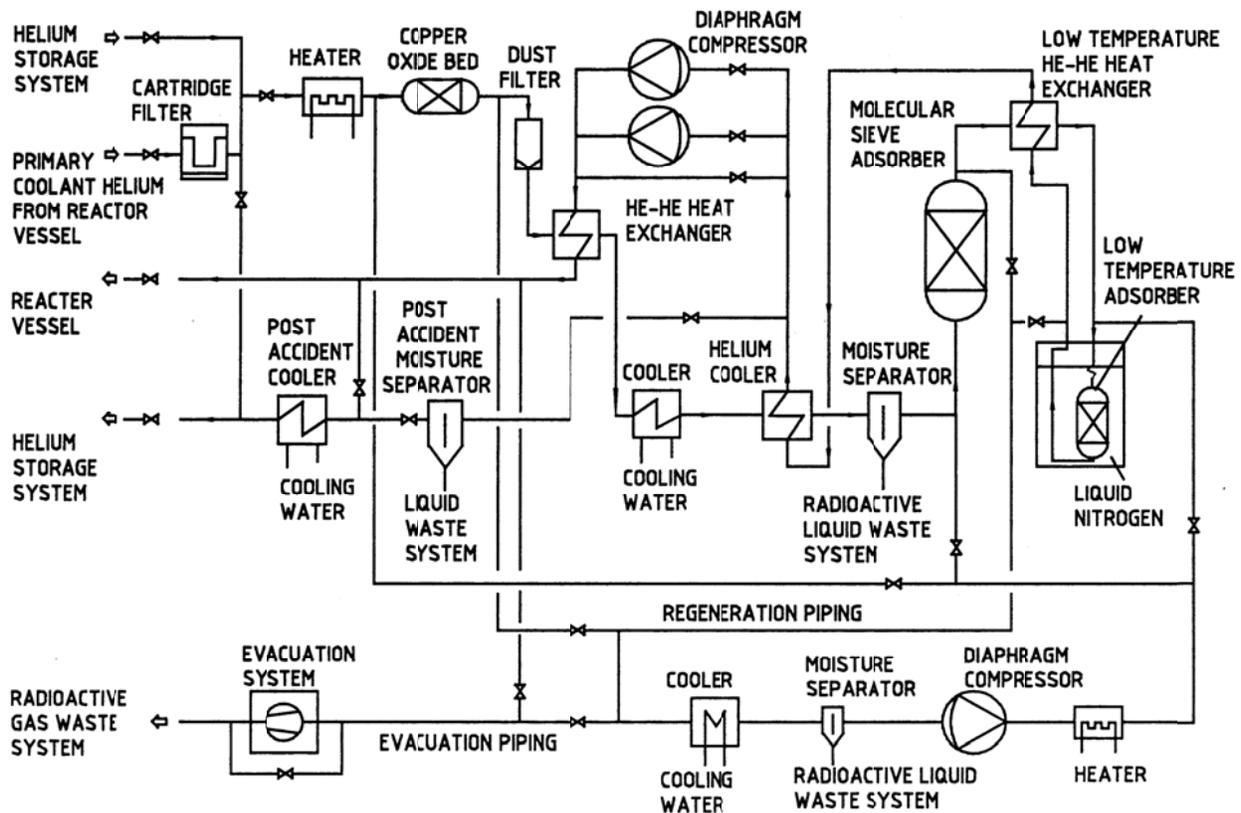


Fig. 65. Schematic of the HTR-10 helium purification system.

[M. Yao, R. P. Wang, Z. Liu, X. He, and J. Li, "The Helium Purification System of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 163–167 (2002).]

During normal operation the primary coolant helium at 250°C and 3.0 MPa from the outlet of the primary helium circulator enters the purification system with a flow rate of 10.5 kg h⁻¹ driven by the pressure head of the primary helium circulator. After being purified, the helium exits the purification system at approximately 185°C passes through two regenerative He/He heat exchanger and is returned to the primary system at the inlet of the primary helium circulator in the steam generator pressure vessel. The pressure loss of the primary circuit due to leakage is controlled by introducing fresh helium from the helium storage tanks into the purification system. A diaphragm compressor (with another as stand by) with a volume flow rate of 2.2 m³ h⁻¹ provides the necessary pressure head to drive the helium stream to regulate the pressure of the primary circuit when the primary helium circulator is shutdown. When a depressurization of the primary circuit is required, the purified hot helium from the He/He heat exchanger is routed to the postaccident cooler, where it is cooled to about 40°C and then pumped to the helium

storage system. The purification system also purifies helium transferred from the primary circuit to the storage during depressurization for maintenance.

Reactor protection system

The HTR-10 reactor protection system is a fully digital protection system. In the event of an accident, the reactor protection system detects changes in the process variables that are indicative of the accident and initiates the protective functions. These protective actions include:

- drop of the reflector rods by gravity,
- shutdown of the primary circuit blower,
- isolation of the secondary system,
- isolation and draining of the steam generator,
- isolation of the primary system,
- dropping of the small absorbed balls by gravity,
- startup of the helium purification system, etc.

The reactor protection system performs different protective measures depending on the measured conditions. For example, when the protection system detects that the primary circuit humidity exceeds the limit value, the isolation of the secondary system will be implemented. The reactor protection system trip parameters and protective actions are given in Table 22.

Table 22. Reactor protection system trip parameters of the HTR-10

Protection variables	Warning level	Trip setpoint	Applicable power range	Action
Nuclear power (source range)	150% rated power	1 MW	Power <1 MW	A
Nuclear power (power range)	110% rated power	120% rated power	Power >1 MW	A
Rate of power increase	2.3%/s	3.5%/s	Power <500 W	A
Core outlet temperature	720°C	740°C		A
Core inlet temperature	270°C	290°C		A
Increase rate of helium pressure	0.01 MPa/min	0.03 MPa/min	Power >3 MW	A
Decrease rate of helium pressure	0.01 MPa/min	0.03 MPa/min	Power >1 MW	A,C,D
Ratio of helium to water flow	1.2	1.3	Power >1 MW	A
Ratio of water to helium flow	1.17	1.33	Power >1 MW	A
Helium humidity	50 ppmv	800 ppmv	Power >1 MW	A,B
Decrease rate steam pressure	0.6 MPa/min	1.0 MPa/min	Power >1 MW	A
Deviation of helium flow from rated	20% of rated flow	20% of rated flow	Power >1 MW	A

A – Reactor trip and helium circulator shutdown.

B – Isolate and drain steam generator.

C – Isolate refueling system.

D – Isolate the thermal measurement system from the primary.

4.6.7 Plant instrumentation and control systems

Normal operating instrumentation and control system

The HTR-10’s instrumentation and controls for the heat transport systems are described by Shuoping⁴⁶. The main functions are:

⁴⁶Z. Shuoping, H. Shouying, Z. Meisheng, and L. Shengquiang, “Thermal Hydraulic Instrumentation System of the HTR-10,” *Nuclear Engineering and Design*, **218**, pp. 199–208 (2002).

- providing the thermal parameters to monitor and control the operation of the HTR-10 in the main control room or locally in the plant where needed,
- providing safety-related thermal parameters to trigger protective actions for the protection system of the HTR-10, and
- providing safety-related thermal parameters for the accidents monitoring system during and after accidents. Those data can be used to monitor the reactor status, to determine the initiating event for an accident, or to evaluate the accident results.

Operating controls

The operating controls are implemented in a digital control system illustrated in Fig. 66. The details of the control algorithm are not given in any reference found to date.

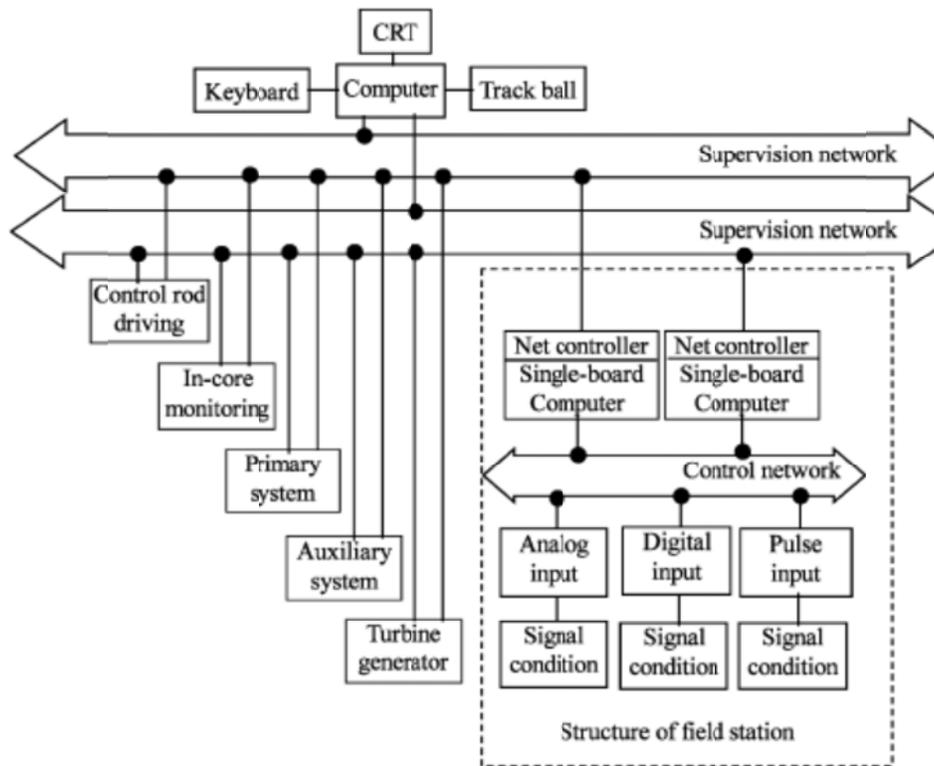


Fig. 66. HTR-10 data acquisition and control system.

[Z. Shuoping, H. Shouying, Z. Meisheng, and L. Shengquiang, "Thermal Hydraulic Instrumentation System of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 199–208 (2002).]

4.6.7.1 Startup/shutdown

Normal startup

To monitor the approach to criticality in the HTR-10, a neutron source is inserted to track subcritical multiplication. This neutron source (a 20-Curie Am-Be source) along with three ^3He neutron counting detectors are placed in three experiment channels. The neutron source emits 4.4×10^7 neutrons per second. In the approach to criticality, the fuel is loaded by the elevator of the fuel loading and discharging

system. The balls are loaded at a rate not faster than three balls per minute and at a rate of reactivity increase not faster than 7×10^{-5} ($\Delta k/k$)/min. The initial start-up found that the critical configuration was 9,627 fuel balls and 7,263 graphite balls.⁴⁷

Normal shutdown

The normal and backup shutdown systems for the HTR-10, described by Wu et al.,¹ are similar to the systems of other HTR reactors. The normal system consists of 10 control rods which are inserted into drilled holes in the reflector blocks. The backup system consists of boronated absorber balls which also are inserted into channels in the reflector. Both shutdown systems are able to bring the reactor to cold shutdown conditions with the allowable subcriticality margin. The control rod drive mechanism is composed of a step motor, a gearbox, a chain wheel, a speed restrictor, and a rod position indicator. Each control rod consists of five individual sections held together by articulated joints. Each section of rod is an annulus formed by 1-Cr 18-Ni 9-Ti coaxial cladding tubes. The absorber material in the form of annular rings of sintered B₄C fills the space between the two coaxial tubes. The total length of the control rod is 2750 mm including the absorber length of 2435 mm. On normal drive demand, the control rods are driven by the step motor and chain wheel. On trip demand, the stepper motor is de-energized which releases the electromagnetic holding force of the motor and the rods drop into channels of the side reflector by means of gravity.

The small absorber ball system is the second reactor shutdown system, also called the standby shutdown system. When flux and/or rod position measurements indicate that rods did not drop on demand, the small absorber ball system can be manually triggered to bring the reactor to subcritical conditions at cold shutdown. The small absorber balls are composed of sintered graphite mixed with 25% B₄C. The balls are 5 mm in diameter of. Seven ball storage tanks are installed on the upper support plate above the upper reflector. The tanks are connected to seven slotted channels of 160×60 mm² cross-section to the side reflector. On demand, a motor pulls a plug covering a hole on the bottom for each storage tank and the balls in the seven storage tanks drop through the holes into the reflector channels by gravity. A pneumatic suction system is used to return the absorber balls from the reflector channels to the storage tanks one by one before the reactor can be restarted.

In an event in which rods fail to scram, the reactor first shuts down by automatic trip of the helium circulator. As the reactor temperature rises with decreased cooling, the strong negative temperature reactivity coefficient then provides sufficient negative reactivity to stop the chain reaction. The absorber balls are manually triggered to maintain subcriticality as decay heat diminishes and the reactor approaches cold shutdown.

Normal operation

HTR-10 is an experimental reactor for the evaluation of operations and equipment for HTGRs. TECDOC-1198⁴⁸ describes two operational test phases for the HTR-10. The first phase has a core outlet temperature of 700°C and a core inlet temperature of 250°C. The second phase core outlet temperature is 900°C and its core inlet temperature is 300°C. The first phase has a steam turbine cycle for electricity generation, and maintains a capability for district heating. The second phase has a combined cycle gas turbine and steam turbine for electricity generation. In the first phase, steam is produced in the steam generator at 400°C and a pressure of 4.0 MPa and sent to the turbine-generator unit. In the second operational phase, a helium-to-nitrogen IHX with is added to the primary circuit. The secondary side of the IHX produces nitrogen gas at

⁴⁷X. Jing, X. Xu, Y. Yang, and R. Qu, "Prediction Calculations and Experiments for the First Criticality of the 10 MW High Temperature Gas-Cooled Reactor Test Module," *Nuclear Engineering and Design*, **218**, pp. 199–208 (2002).

⁴⁸IAEA-TECDOC-1198, *Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology*, February 2001.

850°C for the gas-turbine cycle. The steam generator produces steam at 435°C for the steam-turbine cycle.

Operation of online refueling

The HTR-10’s spherical fuel handling system (FHS) loads new fuel, recirculates partially burned fuel, and discharges fully burned fuel elements during reactor operation.⁴⁹ Table 23 summarizes the principal parameters of the FHS.

Table 23. Principal parameters of the fuel handling system⁹

No.	Designation	Parameter
1	– Fast circulation rate	Approximately 350 balls per hour
2	– Conventional circulation rate	Approximately 50 balls per hour
3	– The number of fuel elements fed per equivalent full-power day (EFPD)	Approximately 125 balls
4	– New fuel elements fed per EFPD	Approximately 25 balls
5	– Average time per fuel element for measuring burn-up	Approximately 60 s
6	– Operating pressure	Approximately 3.0 MPa
7	– Operating pressure after the first charging isolation valve	Approximately 0.2 MPa
8	– Operating pressure ahead of the third discharging isolation valve	Approximately 0.2 MPa
9	– Operating temperature	150–180°C
10	– Fuel element capacity of failed fuel cask	Approximately 1000 balls
11	– Fuel element capacity of buffer line	Approximately 30 balls
12	– Spent fuel element capacity of shipping cask	Approximately 2000 balls

4.6.8 Safety evaluation

The main safety functions of a nuclear power plant are to control reactivity, control heat removal, and limit release of radionuclides to less than licensed limits. An evaluation of design basis accidents of the HTR-10 by Zuying⁵⁰ found that no accident caused the maximum fuel temperature to exceed the fuel temperature limit or caused the reactor core pressure to exceed the limit for the safety valve. Therefore, the fuel element and the primary pressure boundary are not expected fail under any circumstances. Because the reactor has a negative temperature coefficient of reactivity, even if an ATWS accident occurs the reactor will shut itself down. The reactor cavity cooler and decay heat removal system then transfer the decay heat out of the system safely. The analysis also studied hypothetical beyond basis accidents (BDBA) and found that the maximum fuel temperature in no BDBA exceeds 1230°C and graphite corrosion never exceeds 320 kg. The fuel particles will retain their fission products, and the released radioactivity is kept to a low level. No hypothetical design basis or beyond design basis accident poses any safety danger to the environment or public.

⁴⁹J. Liu, H. Xiao, and C. Li, “Design and Full Scale Test of the Fuel Handling System,” *Nuclear Engineering and Design*, **218**, pp. 169–178 (2002).

⁵⁰G. Zuying and S. Li, “Thermal Hydraulic Transient Analysis of the HTR-10,” *Nuclear Engineering and Design*, **218**, pp. 65–80 (2002).

Reactivity insertion events

The study by Zuying looked for the most severe reactivity insertion initiating event which was found to be a design basis earthquake. The earthquake is a Class IV accident with a very low probability. The reactivity insertion combines two hypothesized worst case reactivity effects. First, the earthquake is assumed to cause a failure of rod controls or rod drive system resulting in the uncontrolled withdrawal of a control rod with reactivity worth of $\Delta k/k = 0.01207$. Second, the pebble bed density is assumed to increase due to packing and settling of the fuel pebbles resulting in a reactivity addition of $\Delta k/k = 0.00207$. In a worst case scenario, the primary trip (which would be on high neutron flux) is assumed to fail. Therefore, flux rises until the back-up trip, high outlet temperature setpoint, is reached. The analysis estimates the trip occurs at 69.1 s. The maximum temperature that the fuel is estimated to reach is 1209.9°C, less than the accident limit of 1230°C. Therefore, the accident does not result in an unsafe fuel temperature increase, and therefore the fuel is expected to retain its fission products with no radiation release or safety consequences. The following safety analyses describe the mechanisms that protect the plant in various design basis events.

Core heat removal events⁹

The disturbance of the heat transfer is caused by a chain of events initiated by the loss of external power. This loss of power causes the helium circulator and the feedwater pump to stop working. Then, the reactor core temperature begins to increase. Even if several protective actions fail, the reactor will still shut itself down because of its negative temperature coefficient of reactivity. The decay heat removal system then removes the residual heat. This transient can produce a maximum temperature of 1033°C, and a maximum pressure of 3.18 MPa, which is below the safety values of temperature and pressure. Therefore, the release of fission products is prevented because the integrity of the fuel is not compromised.

Water and air ingress events

Three different water and air ingress events have been looked at in the Zuying study. The first event is a rupture accident of the fuel loading tube. To be conservative, the decay heat is assumed to be 20% higher than calculated. The location of the fuel loading tube rupture is assumed to be at the top of the pressure vessel. Following the rupture, coolant leaks until the pressure increases to the point that the reflector rods are dropped to shut down the reactor. Then, the reactor temperature increases. Finally, the oxidation reaction process between the graphite and the oxygen begins. Since the natural convection is very weak after depressurization, only a very low flow rate of air reaches the hot fuel and thus graphite corrosion is very low. The fuel particles maintain their integrity. The maximum fuel temperature does not exceed 1230°C, and the fuel elements prevent the release of radioactive contamination. Corrosion slows as the temperature of the core drops following shutdown

The second event that was studied was a hot-gas duct rupture. In this event, the internal and external tubes of the hot-gas duct rupture at the same time resulting in rapid depressurization followed by an air ingress accident.

When the reactor cavity pressure is greater than 0.11 MPa, the rupture disc in the reactor cavity will break and the gas will rapidly discharge into the environment from the reactor cavity without filtration. After pressure equilibrium is reached between the reactor pressure vessel and the reactor cavity and the negative sliding rate of reactor cavity pressure reaches 1000 Pa s^{-1} , the negative pressure ventilation system is closed and 5 min later, the isolation valve on the pressure relief line is closed. Then the negative pressure ventilation system is started up again. The air in reactor cavity is discharged after filtration and the ventilating flow is 100% per day in the first 3 days. Counter measures (e.g., foam) are assumed to be implemented after 3 days that cut off the air source in to the reactor pressure vessel to any further prevent air ingress into the reactor, then the cavity is sealed. Natural convection is established via gas diffusion

and convection. For this hypothetical accident, the total graphite corrosion is 319.2 kg. The estimated fuel temperature remains below 906.5°C, and no significant fission product release occurs.

The third event and most severe hypothetical ingress accident that was studied is two steam generator tube rupture and the secondary relief system failing to work, simultaneously. Following the rupture, water and steam enter the primary system, eventually reaching the core region. Various protection systems activate. The analysis estimates that 129.9 kg of water enters the core region, resulting in a slightly positive reactivity. However, the maximum fuel temperature is 1036.2°C, well below the limit of 1230°C to produce fuel particle failures. At this temperature the steam-carbon reaction is slow and despite the large amount of water, total amount of graphite corrosion is estimated to be less than 4.88 kg. Therefore, no significant fission product release is expected to occur, even for the most severe hypothetical accident.

5. NEXT GENERATION NUCLEAR PLANT—NGNP

5.1 Reactor System Design

This section provides a summary of the instrumentation and control features of the Next Generation Nuclear Plant (NGNP). The NGNP project was established by the U.S. Department of Energy (DOE) to integrate high-temperature reactor technology with the production of electricity, process heat, and hydrogen. The scope of the NGNP project includes design, construction, licensing, and operation of a full-scale prototype high temperature gas-cooled reactor (HTGR) plant.

5.2 Current Status

Over the last several years, DOE has funded the preconceptual development of three plant designs: a pebble bed reactor developed by a Westinghouse-led team and prismatic core reactors developed by General Atomics and AREVA, respectively. Preconceptual design work on these three designs was completed in 2007.

The NGNP project, the three contractors, and an industry alliance performed a comprehensive review of industry needs and project objectives. The NGNP 2009 Status Report⁵¹ summarized the results of this review. Important conclusions from the review were that the technology be supplied by the early 2020s, a commercial rather than a demonstration plant be constructed, a reduction in outlet temperature requirements, and desirability of a modular-type plant. Consequently, each contractor team developed a simplified preconceptual design that used a steam generator in the primary loop. Instead of preparing conceptual designs for all three options, DOE developed a Funding Opportunity Announcement to share development cost in the development of up to two conceptual designs. A decision to fund conceptual designs for the PBMR and the General Atomics was announced in March 2010.⁵² Also, a decision by the South African government to eliminate funding for the Pebble Bed Modular Reactor Company⁵³ may affect the development of that NGNP concept. In light of this uncertainty, all three pre-conceptual designs of the NGNP will be summarized. As more details of the simplified designs become known, information in this section may need to be updated. The instrumentation and control features of the designs have not yet been established; however, possible implementations will be discussed.

⁵¹*Next Generation Nuclear Plant Project 2009 Status Report*, INL/EXT-09-17505, May 2010.

⁵²*Teams Compete for NGNP Design*, World Nuclear News, March 9, 2010, http://www.world-nuclear-news.org/NN_Teams_compete_for_NGNP_design_0903101.html.

⁵³*Government Pulls Plug on PBMR*, Johannesburg Times Live, July 18, 2010, <http://www.timeslive.co.za/business/article555632.ece/Government-pulls-plug-on-PBMR>.

5.3 Fuel

The common aspect of the NGNP design is that each of the three designs is an HTGR with a helium-cooled, graphite moderated nuclear reactor that is capable of operating at reactor outlet temperatures from 700–950°C. The higher end of the range is necessary for the direct production of hydrogen or to provide high-temperature process heat for other industrial applications. Electrical energy conversion efficiency improves with increasing temperature but even the low-end range produces higher efficiency than current light-water reactor technology. The higher the temperature is set for the reactor outlet, the greater the potential challenges, especially regarding fuel performance and structural characteristics of metallic components.

The NGNP reactor is a direct successor of other HTGR designs reported in Chapter 4. The NGNP uses ceramic coated spherical fuel particles—TRISO particles—that contain the fuel and retain fission products within layers of carbon and silicon carbide. The center of a fuel particle consists of a kernel of uranium oxide or uranium oxycarbide with a diameter of 350–500 microns, depending on the reactor design. The term, TRISO, refers to the three shells that encase the fuel particle and act as a containment. The fuel kernel is surrounded first by a layer of low-density carbon material that retains fission products and accommodates fuel kernel swelling. The three protective layers of the TRISO coating are (1) high-density gas-tight pyrocarbon barrier to fission product diffusion, (2) high-density, silicon carbide that provides a pressure retaining barrier and second fission product diffusion barrier, and (3) high-density gas-tight pyrocarbon that serves as a third and final fission product barrier and protective layer. The final diameter of a fuel particle is roughly 800–900 microns. Thousands of these particles are formed into a carbon matrix sphere or cylinder depending on the reactor design as shown in Fig. 67.

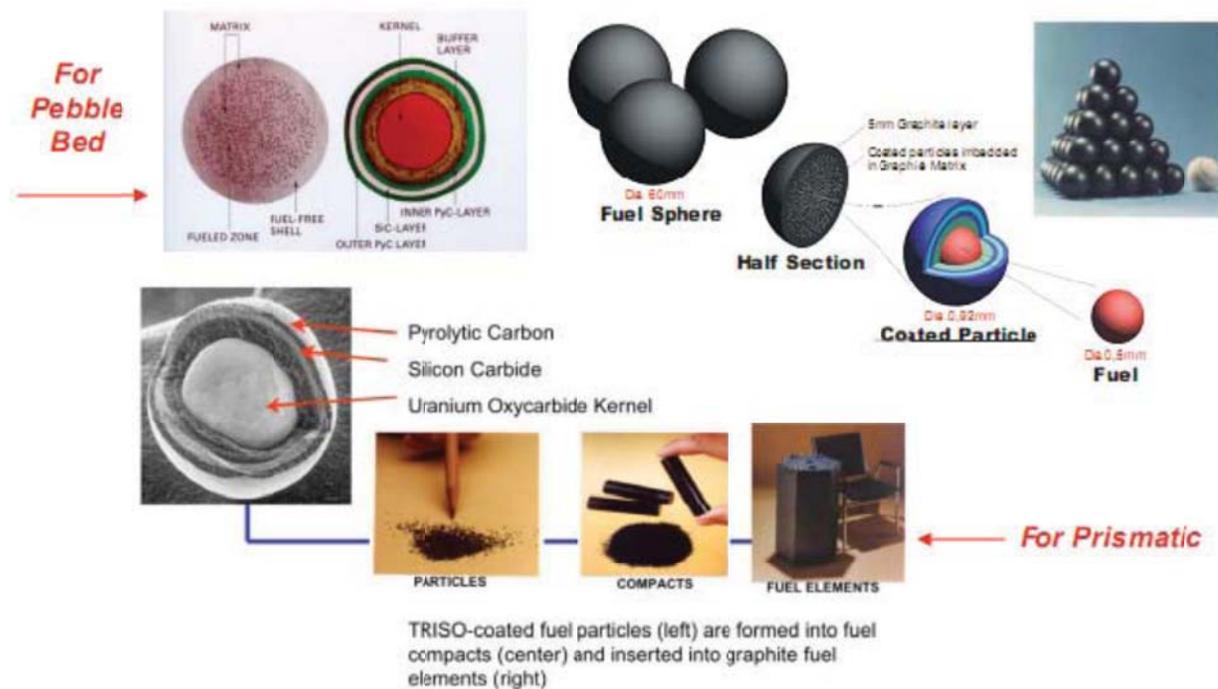


Fig. 67. TRISO fuel.

[Next Generation Nuclear Plant Project 2009 Status Report, INL/EXT-09-17505]

As discussed in the context of the existing HTGRs in Chapter 4, the inherent safety attributes of the HTGR are based on the properties of the fuel. The fuel particles retain their integrity (and fission products) even at the highest temperatures seen in normal operation and accident conditions. The helium coolant is chemically inert and nonreactive. The graphite core retains its strength at high temperatures and is effective in slowing down neutrons for efficient fission reactions. HTGR reactor cores have a high-thermal mass which limits heat up and cool down rates and greatly reduces the need for fast acting control systems to manage transient conditions in accidents.

Two types of core configurations are being considered for the NGNP—prismatic and pebble. The prismatic fuel is based on the MHTGR and Fort St. Vrain designs presented in Sects. 4.1 and 4.4, respectively. The core prismatic block reactor consists of hexagonal blocks of graphite that are stacked inside a cylindrical pressure vessel. Vertical holes in the blocks are provided to contain fuel cylinders filled with cylindrical fuel pellets, allow coolant flow, and provide space for control rods or other means for reactor shutdown. Graphite blocks stacked around the outside of the core area (and sometimes the inside of the core area as well, leaving an annular fuel region) reflect neutrons back into the core. New fuel is added every 1.5 to 2 years.

The second alternative is the pebble bed design. This design follows after the fuel design pioneered in the German AVR reactor presented in Sect. 4.3. The pebble bed is also used in the South African PBMR design and the Chinese HTR-10 described in Sect. 4.5. The pebble bed reactor uses fuel formed into billiard ball size spheres (pebbles) instead of long cylinders. The pebbles fill a cylindrical reactor core volume. Graphite reflectors surrounding the pebble region return neutrons to the core. Some designs also use an inner reflector to displace fuel from the center of the core to reduce fuel temperatures at the central area of the core. Pebbles are continuously withdrawn from the bottom of the core, monitored, and inserted back into the core. New pebbles replace those which have reached their prescribed burnup levels or are identified as defective; thus, pebble bed reactors operate continuously and do not have planned shutdowns for refueling. Preconceptual design parameters for the NGNP reactor are shown in Table 24. The parameters vary depending on the design.

Table 24. Generic NGNP reactor parameters

Reactor type	Prismatic block or pebble bed
Reactor power	500–600 MW(t) (in early design variations—less in newer design variations)
Primary coolant	Helium
Inlet temperature	350–500°C
Outlet temperature	700–950°C
Coolant pressure	7–9 MPa
Active core height	8–11 m
Inner core/reflector diameter	2–3 m
Outer core diameter	4–5 m
Side reflector diameter	5–6 m
Reactor pressure vessel outer diameter	7–8 m
Reactor pressure vessel height	25–31 m

Teams headed by Westinghouse, AREVA, and General Atomics prepared pre-conceptual designs for consideration by DOE. Descriptions of their designs will be summarized in the following sections. These designs were prepared prior to a decision by a NGNP project, contractor, and industry alliance partnership to reduce the reactor coolant outlet temperatures to 700–800°C, which might have an effect on subsequent designs, especially on material requirements for metallic components.

5.4 Westinghouse PBMR Design

A summary of the Westinghouse proposal for the NGNP is provided in the NGNP Pre-Conceptual Design Report.⁵⁴

5.4.1 Reactor

Figure 68 shows the reactor components of the PBMR. The PBMR uses approximately 450,000 spherical fuel elements. Other reactor internals include graphite reflectors, control rods, and the core barrel.

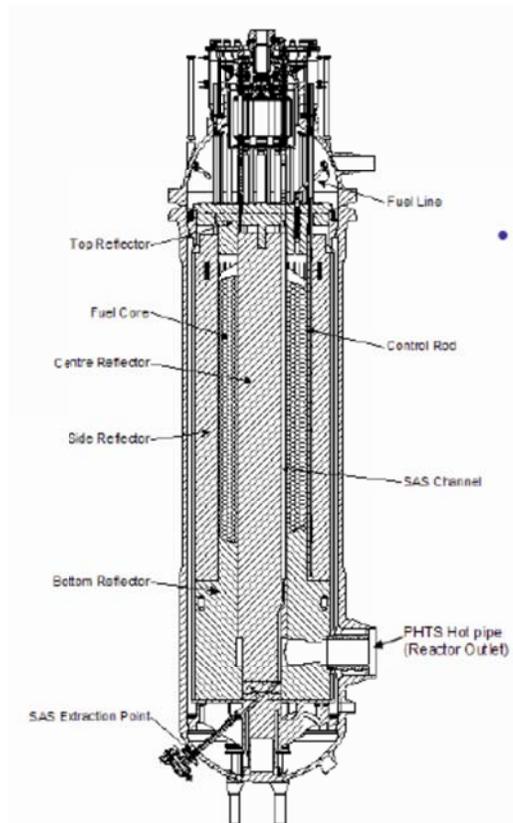


Fig. 68. PBMR.

[*NGNP Pre-Conceptual Design Report, INL-EXT-7-12967*]

The graphite reflector moderates neutrons and acts as a slow-changing thermal mass and heat conduction medium to conduct heat from the fuel to the core barrel in accident conditions. Three zones of reflectors consist of a central reflector (in an early design variation) and inner and outer side reflectors. The central (if used) and inner side reflectors are replaceable because of the irradiation damage. The outer side reflector is permanent. There are also top and bottom graphite core support structures.

Twenty-four control rods are located in the side graphite reflector blocks. Twelve are used for control and 12 are used for shutdown. The shutdown rods are the length of the reflector blocks. The shorter control

⁵⁴*Next Generation Nuclear Plant Pre-Conceptual Design Report, INL/EXT-07-12967, Revision 1, November 2007.*

rods run in the upper half of the reflector block. A secondary shutdown system above the central reflector drops small B₄C spheres into channels in the central reflector if rods fail to operate.

A stainless steel core barrel sits between the wall of the reactor pressure vessel (RPV) and the outer reflector to support the graphite blocks and maintain core geometry.

The RPV is a cylindrical vessel with hemispherical bolted upper head and welded lower head. The upper head has an opening to provide access to the core for reflector replacement. The lower head has openings to discharge of fuel pebbles and secondary shutdown pellets. The RPV has a diameter of about 6.8 m and is about 30 m high.

Intermediate heat exchanger vessels contain the intermediate heat exchangers and connect the primary system to the secondary system.

5.4.2 Shutdown cooling

The core conditioning system is used for decay heat removal during normal shutdowns or if the main circulator trips. It can also be used to remove decay heat during postulated accident conditions to supplement passive heat removal features of the reactor design.

5.4.3 Reactor cavity cooling

Figure 69 shows the reactor cavity cooling system (RCCS). The RCCS is a constant flow, water-based cooling system that cools the concrete walls of the reactor cavity during normal shutdown and accident conditions. The RCCS operates by pumping water through standpipes that line the inside of the cavity. It can also operate in a passive mode by boiling the water in the standpipes, possibly for up to 72 hours. The time requirement has not yet been fixed.

5.4.4 Fuel handling

The fuel handling system moves fuel pebbles to and from the reactor core. Fuel is discharged from the bottom of the reactor and passed through the fuel monitoring system to determine its integrity and fuel burnup. If the fuel has burnup remaining and is in good condition, it is returned to the top of the reactor where it is dropped into inner or outer core positions, depending on the desired neutron flux effect. Over time, the pebbles move from the top of the core to the bottom as pebbles are continuously cycled. New fuel is inserted and used fuel is stored as needed. Fuel insertion and removal rates and can be varied to suit longer-term reactivity requirements. The fuel sphere transfers are made in a pressurized helium environment.

5.4.5 Helium services

Helium services systems and subsystems are used to clean the helium coolant and maintain coolant inventory and pressure.

5.4.6 Instrumentation and control systems

The preconceptual design of the PBMR NGNP plant does not describe I&C requirements or control philosophy. However, the plant will have many similarities with the PBMR demonstration power plant originally planned for Koeberg, South Africa. Conceptual design information based on that plant has been provided to the NRC for a design certification preapplication review for the PBMR.

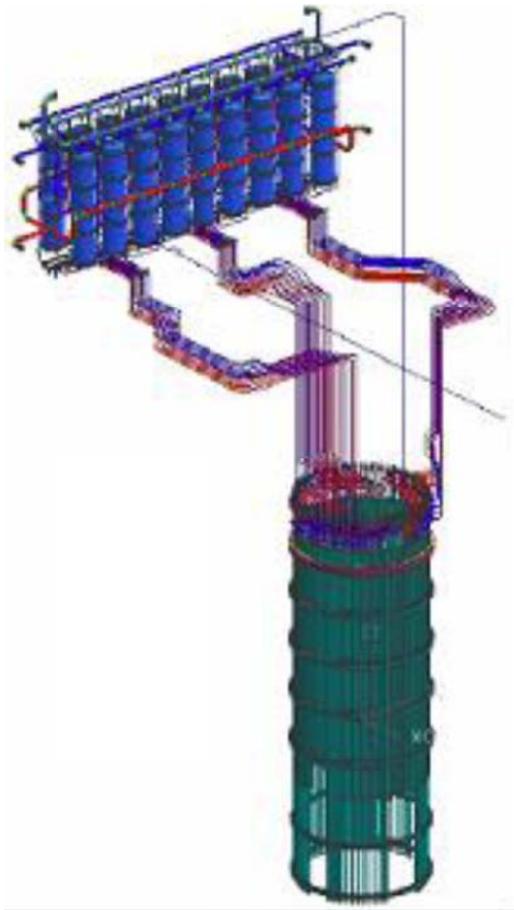


Fig. 69. Reactor cavity cooling system.

[NGNP Pre-Conceptual Design Report, INL-EXT-07-12967]

The PBMR automation system (AS) will perform power plant monitoring, control, and protection functions. An ORNL report⁵⁵ provides an overview of the implementation. A presentation of the PBMR demonstration plant⁵⁶ also describes the AS and its functions. The NGNP PBMR is expected to be similar.

The AS system provides redundancy in all safety-related functions and in many nonsafety-related functions. For example, the reactor shutdown function is accomplished by two automatic systems on diverse hardware and software platforms and by a manual shutdown system. Redundant equipment also protects high-value plant systems and equipment.

The AS is a digital I&C system with both safety and nonsafety functions. The hardware design uses integrated commercial off-the-shelf, digital programmable systems. The AS consists of several systems:

- *Human system interfaces*—Enables plant operators to interact with the plant through the automation system in the main control room and the post-event monitoring and recovery room (if needed).

⁵⁵*Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, Oak Ridge National Laboratory, NUREG/CR-6842 (ORNL/TM-2004-74), 2004.

⁵⁶Charles L. Kling, *PBMR Automation System*, February 2006 (NRC accession number ML060680144).

- *Reactor protection system*—Ensures that reactor heat production safety limits are maintained by automatically shutting down the reactor under design basis conditions.
- *Post-event instrumentation*—Provides information displays to operators in normal, accident, and post-accident conditions to allow them to monitor the condition of the plant.
- *Equipment protection system*—Provides investment protection capability.
- *Operational control system*—Performs nonsafety plant protection, control monitoring, and data recording, including automatic runback of control rods.
- *Reactor manual shutdown system*—Provides manual control of control rod insertion and secondary shutdown system small absorber sphere insertion.
- Activity measurement system.
- Burnup measurement system.
- Core instrumentation.

5.4.6.1 Human system interface

Two control areas are provided from which the operator can interact with the automation system. The main control room is the primary area. The post-event monitoring and recovery room is an alternative area. The control areas will provide a habitable environment with workstations with multifunctional displays to provide a consistent, ergonomic interface for operator activities for all plant operating conditions.

5.4.6.2 Reactor protection system

The RPS will be a Class 1E digital system with 2 out of 3 coincident logic and will be compliant with IEEE Std 603 and IEEE Std 7-4.3.2. It will be capable of bringing the reactor to a subcritical condition and maintaining that condition under all design basis accidents. It will be powered by an uninterruptible power supply. The RPS will sense and monitor process conditions and initiate protection actions appropriate for the sensed conditions. Actions include a control rod scram in which 12 control rods drop by gravity into the side reflector channels, a reactor scram in which the 12 control rods and 12 shutdown rods all drop into their side reflector channels, and the initiation of the small absorber sphere insertion into the central reflector channels. Several reactor conditions are monitored by the RPS system, including the following.

- *Reactor overpower*—A control rod scram is initiated if reactor power based on ex-core neutron detectors reaches 105%. A reactor scram is initiated if reactor power reaches 110%. A control rod scram is also initiated if reactor power remains at 103% for 8 consecutive hours.
- *Primary coolant over-temperature*—For the PBMR demonstration power plant, a control rod scram is initiated based on average high reactor coolant outlet temperature (925°C) as measured by thermocouples located in the reactor outlet pipe upstream of the high-pressure turbine. A reactor scram is initiated if the temperature is 935°C. The temperature setpoints have not yet been stated for the revised PBMR NGNP design, whose planned core outlet temperature is 700–800°C, instead of ~900°C for the PBMR demonstration power plant design.
- *Excessive reactor power increase rate*—A control rod scram is initiated if the reactor period as calculated from the ex-core neutron detectors is too short.
- *Loss of forced cooling*—A control rod scram is initiated after a predetermined time delay on loss of coolant flow through the reactor as measured by differential pressure instrumentation. The time delay is long enough to minimize operational interference but short enough to prevent the reactor from becoming critical again after it has gone subcritical due to its negative temperature coefficient.

- *Loss of primary coolant*—Two RPS actuations may occur following the loss of core coolant pressure. A reactor scram could be initiated (per Kling, *PBMR Automation System*) or the secondary shutdown system insertion of the small B₄C spheres into the core could be initiated⁵⁷. The initiation of either could occur after a time delay following the initiation signal of loss of core coolant pressure. The time delay is long enough to minimize operational interference but short enough to prevent the reactor from becoming critical again after it has gone subcritical due to its negative temperature coefficient.
- *Seismic event*—A reactor scram and secondary shutdown system actuation are initiated following detection of a safe shutdown earthquake.

5.4.6.3 Post-event instrumentation

The post-event instrumentation system (PEI) provides information monitoring, recording, and display of plant parameters to operators during normal operation and during and following design basis accidents to ensure that they can assess the safety status of the plant. The information is provided in the main control room and in the post-event monitoring and recovery room. The system is powered by an uninterruptible power supply for 24 hours. It would be designed to meet the guidance of NRC Regulatory Guide 1.97.

The PEI provides indication of the RPS, safety-related equipment, plant status during and after design basis accidents and system bypassed information, including:

- RPS, including its execute functions,
- other auxiliary or supporting system that could render safety functions of the RPS inoperative,
- RCCS water level status,
- pressure relief shaft damper status,
- reactor shutdown status parameters,
- residual heat removal system status and performance parameters,
- primary coolant pressure boundary status parameters,
- containment integrity parameters,
- reactor cavity parameters, and
- radiological release monitoring parameters.

5.4.6.4 Equipment protection system

The equipment protection system (EPS) provides investment protection capability for significant, high value, plant systems and equipment (e.g., turbogenerator). It is intended to be a highly reliable nonsafety system that monitors plant parameters and initiates protective action to prevent potential equipment damage. For the PBMR demonstration power plant, example protection functions are provided below. The NGNP PBMR functions for the pre-conceptual design (also a Brayton cycle gas turbine) are expected to be similar. Functions for the revised PBMR design with a lower core outlet coolant temperature and steam turbine system have not yet been stated.

- Turbogenerator overspeed
- Turbogenerator vibration
- Turbogenerator axial displacement
- Turbogenerator bearing status
- Turbogenerator bearing oil supply failure
- Turbogenerator turbine high-inlet temperature
- Turbogenerator turbine high-exhaust temperature

⁵⁷*Technical Description of the PBMR Demonstration Power Plant*, PBMR Document Number 016956, February 2006 (NRC ADAMS accession number ML061420576) (Proprietary).

- Turbogenerator blade path temperature spread
- Turbogenerator dry gas seal
- Turbogenerator electrical system trip
- Turbogenerator slow acceleration during run-up
- High-pressure compressor high-inlet temperature or surge
- Low-pressure compressor high-inlet temperature or surge
- Recuperator high-inlet temperature
- Reactor high-inlet temperature
- Reactor high reactor temperature differential
- Failure of the operational control system main power system controllers

5.4.6.5 Operational controls system

The operational control system (OCS) is expected to be a commercially quality distributed control system consisting of distributed input/output modules and intelligent field devices that provide closed-loop control of plant variables; nonsafety plant protection, control monitoring, and data recording; diverse reactor shutdown capability; and monitoring and storage of plant variables and data for operators for plant supervision and control.^{5,6} Redundant networks and controllers protect against consequences of single equipment failures. The system is to be planned to permit hardware and software upgrades over time. It will be implemented on a type of platform that is diverse from the RPS.

Automatic functions to regulate the operating conditions within set limits for the PBMR demonstration plant systems and components are shown below. Automatic functions for the NGNP PBMR pre-conceptual design (with the Brayton cycle gas turbine) are expected to be similar. Functions for the revised PBMR design with a lower core outlet coolant temperature and steam turbine system have not yet been stated.

- Reactor outlet temperature
- Reactor inlet temperature
- Recuperator inlet temperature
- Helium inventory
- Reactor core power
- High-pressure compressor pressure
- Compressor surge margin
- Turbogenerator speed
- Core conditioning system decay heat removal

Additional process controls or capabilities include

- reactivity shutdown margin monitoring,
- reactor core neutron flux distribution alarms,
- reactor approach-to-criticality and startup operations support,
- primary pressure boundary leakage alarms, and
- fuel handling operations.

5.4.6.6 Reactor manual shutdown

The reactor manual shutdown system is operator initiated to shut down the reactor through control rod insertion or through insertion of the small B₄C absorber spheres. This system, with independent, hardwired controls, provides a diverse shutdown capability from the automatic reactor shutdowns from

the reactor protection system or operational control system. Manual shutdown capabilities are provided in the main control room and in the post-event information monitoring and recovery room.

5.4.6.7 Activity measurement system

The activity measurement system uses a wide-range gamma sensitive ionization chamber to measure the gamma radiation emitted by fuel spheres to determine whether the spheres contain fuel or graphite moderator.

5.4.6.8 Burnup measurement system

The burnup measurement system measures the degree of fuel utilization of PBMR fuel spheres. The system measures the fuel burnup using a cryogenic, high-purity Germanium detector, digital signal processor, and photon collimator to evaluate burn up of the fuel based on its inventory of ^{137}Cs . The PBMR Automation System presentation reference notes that a test program will be developed to validate the proposed fuel management program.

5.4.6.9 Core instrumentation

Ex-core neutron detection is provided to measure neutron flux and correlate the measurement to reactor power.

In-core instrumentation for the PBMR is used for source range flux measurement for approach to criticality and initial startup, to map core flux distribution, measurement of graphite core structure and core barrel temperature distribution, and measure displacement of the core barrel top plate and core barrel support structure. Flux measurements are made with self-powered neutron detectors. Temperature measurements are provided by thermocouples. Displacement measurements are provided by strain gauges.

5.5 AREVA Prismatic Core Design

As noted in Sect. 4.1.2, a decision was made in March 2010 to fund conceptual designs for the PBMR and General Atomics. However, much work was performed to prepare a pre-conceptual design study of the AREVA prismatic core gas-cooled reactor and elements of that design could be of interest from the regulatory perspective. Therefore, a summary of the AREVA recommendations for the reactor design presented in the 2007 *NGNP Pre-Conceptual Design Report* (INL/EXT-07-12967) will be provided.

5.5.1 Reactor

AREVA recommended a prismatic core for the NGNP HTGR in part because a reactor with a prismatic core (Fort St. Vrain) had already been licensed and operated; thus, there was a degree of familiarity with the design. The AREVA prismatic reactor is shown in Fig. 70. The prismatic fuel blocks have 360-mm flat-to-flat spacing. Fuel blocks with and without holes for control rods are shown in Fig. 71.

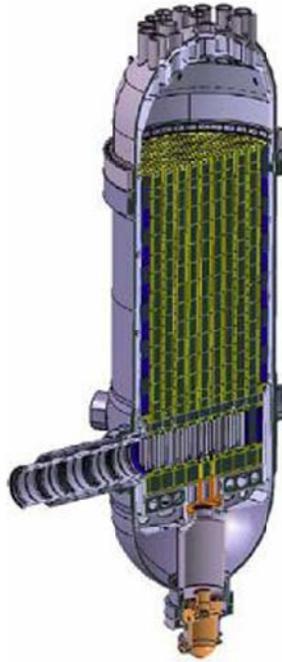


Fig. 70. Prismatic reactor.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

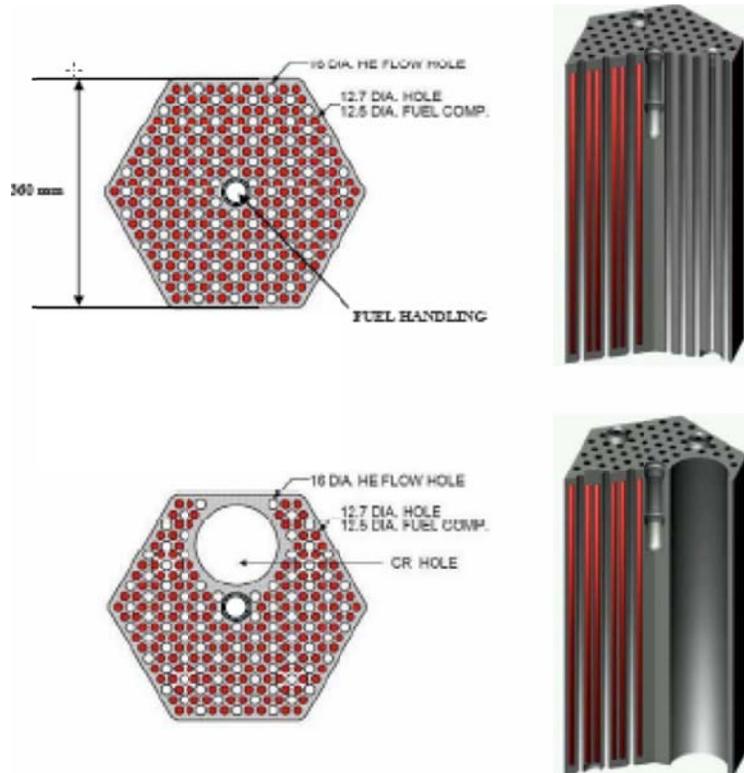


Fig. 71. Prismatic fuel blocks.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

The reactor internals of the AREVA prismatic core pre-conceptual design included three zones of graphite reflector blocks that moderate neutrons and serve as a large, core thermal mass. Central and inner side reflector blocks are replaceable. An outer side reflector is permanent. Graphite structures also support the top and bottom of the core.

There are 36 control rods in the inner ring of the outer reflector and 12 startup control rods in the inner ring of fuel columns that are withdrawn while the reactor is in operation. Neutron absorbing material (B_4C and other materials to be considered) in the control rods is encased in carbon composite sleeves. A secondary shutdown system is provided in which spherical absorber pellets are dropped into channels in selected fuel blocks. The carbon composite sleeves were noted as requiring significant research activities to qualify their use.

A core barrel that consists of a double-wall structure of Incoloy 800H material between the reactor pressure vessel and the outer side reflector is provided to support the graphite reflector blocks and maintain core geometry.

The reactor pressure vessel is shown in Fig. 72. The RPV is about 25 m high, 7.5 m in diameter, and 150 mm thick at the core belt line. It is expected to be made of 9 Cr-1 Mo, a material being developed for this usage. Penetrations for the control rods and the fuel handling system are provided in the upper vessel head. The shutdown cooling system blower connects at an opening in the bottom vessel head. Nozzle penetrations are provided around the lower vessel for multiple loops.

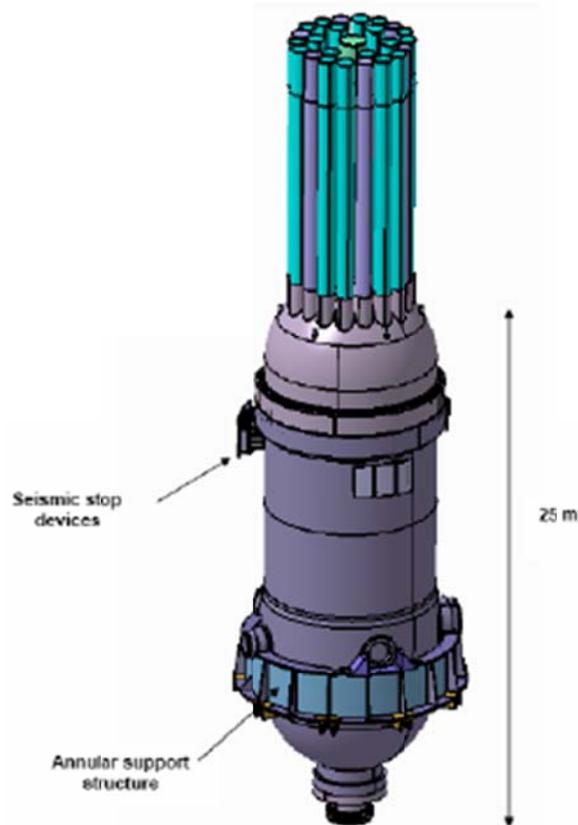


Fig. 72. RPV.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

Cross vessels consisting of concentric ducts (cooler gas in the outer duct, hot-core outlet gas in the inner) connect the reactor pressure vessel with the intermediate heat exchanger (IHX) vessel. (For the simplified design, the cross vessel would connect the reactor vessel with the steam generator vessel.)

5.5.2 Shutdown cooling

A shutdown cooling system is used to provide for decay heat removal if the main circulator trips during accident conditions to supplement passive safety features of the reactor or during refueling periods.

An additional heat removal path in a secondary loop is envisioned for use as a startup and decay heat removal system in the pre-conceptual design that has a secondary gas loop. Whether a similar additional heat removal path would be provided in the simplified design having a steam secondary loop is not clear.

5.5.3 Reactor cavity cooling

Figure 73 shows the RCCS. This system consists of water-filled panels connected to water tanks and ring the reactor cavity. Heat is removed from the cavity to the water storage tanks by natural circulation. A nonsafety water circulation loop with forced flow rejects heat from the water storage tank to the outside environs. If forced cooling is not available, water in RCCS panels boils and steam is vented to the atmosphere.

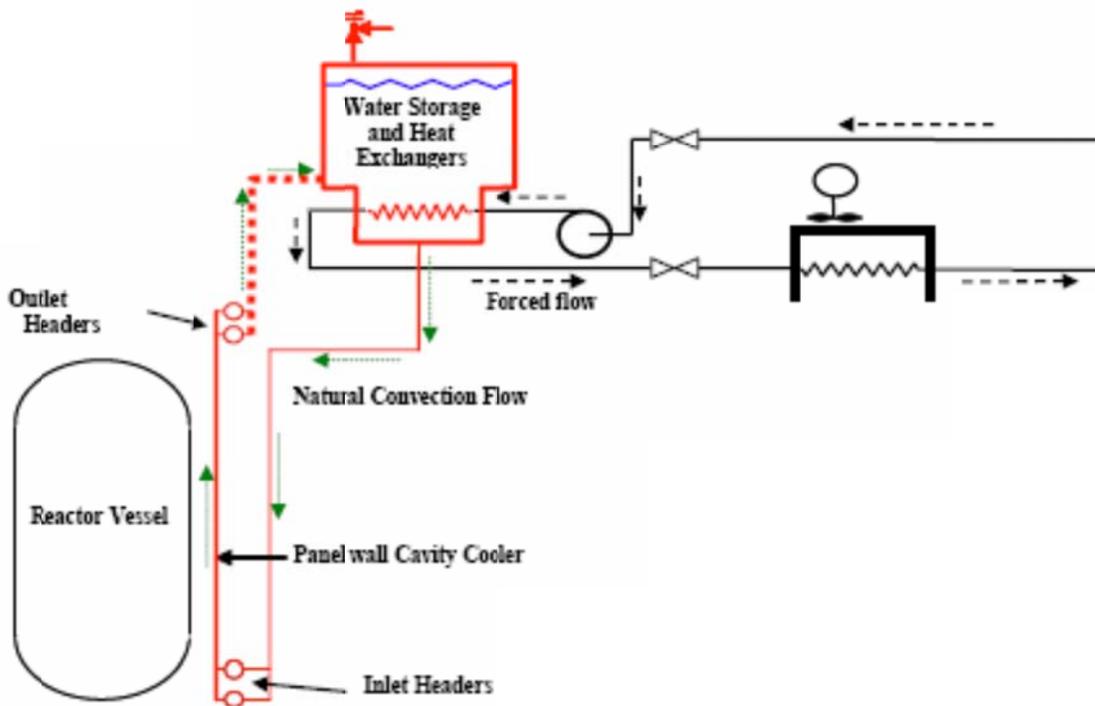


Fig. 73. RCCS.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

5.5.4 Fuel handling

The fuel handling system consists of a fuelling adaptor, fuel elevator, and a fuel handling machine robotic manipulator as shown in Fig. 74. The adaptor is placed on top of the reactor vessel. The fuel elevator is inserted through the adaptor through which the manipulator is placed. A grapple hooks to a connector in the top of the fuel or reflector blocks, which are moved one at a time.

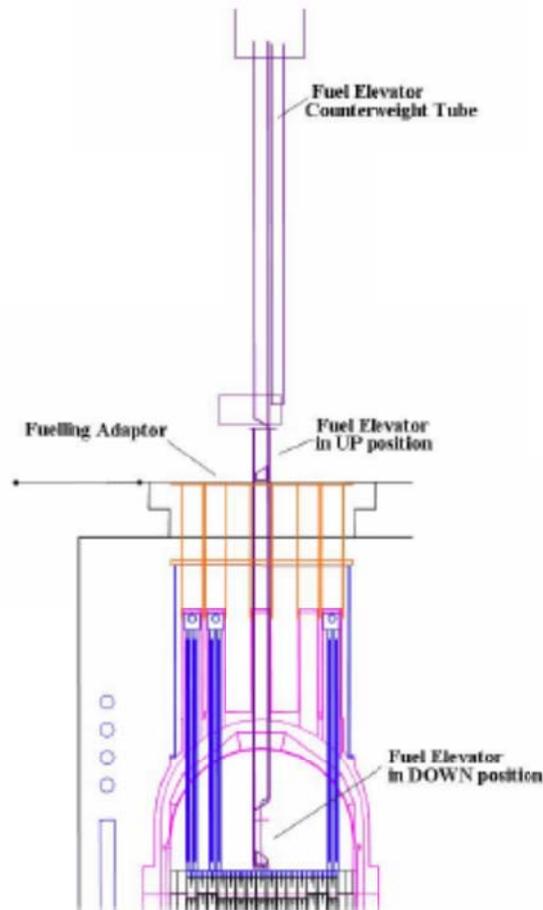


Fig. 74. Fuel handling system.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

5.5.5 Helium services

Helium services systems and subsystems purify the primary helium coolant and maintain helium pressure and inventory during reactor operation and shutdown periods.

5.6 General Atomics Prismatic Core Design

As did AREVA, General Atomics preconceptual design of the NGNP plant was a prismatic core design.

5.6.1 Reactor

The General Atomics pre-conceptual NGNP design prismatic core has 360-mm flat-to-flat spacing. Fuel blocks have holes for fuel compacts, coolant channels, and holes for burnable poison. Sample fuel assemblies are shown in Fig. 75. Three reflector zones are specified. Central and inner side reflectors are replaceable. An outer side reflector is permanent. Graphite structures also support the top and bottom of the core.



Fig. 75. Fuel block assembly.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

There are 36 control rods in the inner ring of the outer reflector and 12 startup control rods in the inner ring of fuel columns that are withdrawn while the reactor is in operation. Annular compacts formed from B_4C granules in a graphite matrix serve as neutron absorbers in the control rods. The compacts are retained in Incoloy 800H canisters for support. A secondary shutdown system consists of 18 channels in which boronated pellets are inserted if needed.

The reactor pressure vessel is about 31 m high and about 8.2 m in diameter. It may be made of 2-1/4 Cr-1 Mo, 2-1/4 Cr-1 Mo-V, or SA508/SA533 steel, depending on expected operating temperatures and/or the provision for vessel cooling. Cross vessels consisting of concentric ducts (cooler gas in the outer duct, hot core outlet gas in the inner) connect the reactor pressure vessel with the power conversion system vessel and intermediate heat exchanger vessel. (For the simplified design, the cross vessel would connect the reactor vessel with the steam generator vessel.)

5.6.2 Shutdown cooling

A shutdown cooling system is used to provide for decay heat removal if the power conversion system is not available or for normal heat removal under accident conditions.

5.6.3 Reactor cavity cooling

Figure 76 shows the RCCS. This is a passive system that removes heat from the reactor cavity during accident conditions when the power conversion system and the shutdown cooling system are not available. Panels that connect to rising concentric ducts in which hot gasses rise in the inner duct and vent to the environs and cooler outside air returns through the outer duct. As this is a passive system, there are no active components. The system operates continuously in natural circulation.

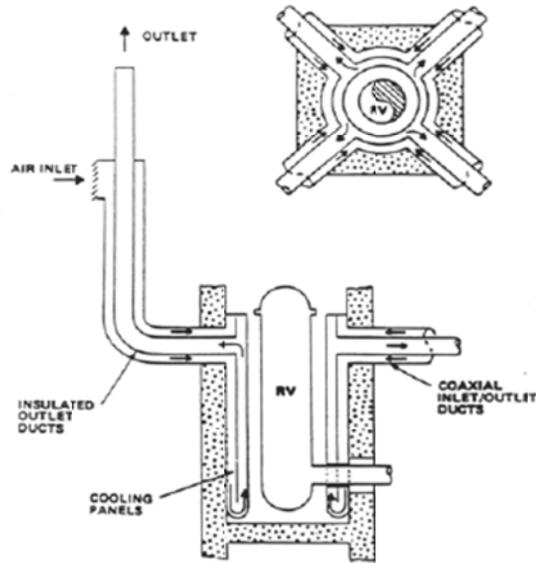


Fig. 76. RCCS.

[NGNP Pre-Conceptual Design Report, INL/EXT-07-12967]

5.6.4 Fuel handling

The fuel handling system consists of a fuel handling machine, two fuel transfer casks, an auxiliary transfer cask, positioned, support structure, and spent fuel storage and handling facilities as shown in Fig. 77. Fuel and reflector blocks are moved column by column rather than layer by layer.

5.6.5 Helium services

Helium services systems and subsystems purify the primary helium coolant and maintain helium pressure and inventory during reactor operation and shutdown periods.

5.7 Power Conversion and Hydrogen Production

The three 2007 preconceptual designs from Westinghouse, AREVA, and General Atomics teams deliver core outlet temperatures of 900–950°C and the capability of providing high-temperature process heat to support potential end user needs as described below.

Westinghouse proposed using two IHXs in series to remove heat from the primary loop and supply energy to a secondary helium loop. The high-temperature heat exchanger is potentially silicon carbide to tolerate the high end of the range for reactor outlet temperature. The secondary loop contains a high-temperature top cycle for hydrogen production and a bottom system for steam production. The tentative design shows hot gas to a hybrid thermochemical plus electrolysis process for hydrogen production. The bottom cycle takes the hot exhaust from the chemical plant through a steam generator that supplies steam to a steam turbine generator as shown in Fig. 78.

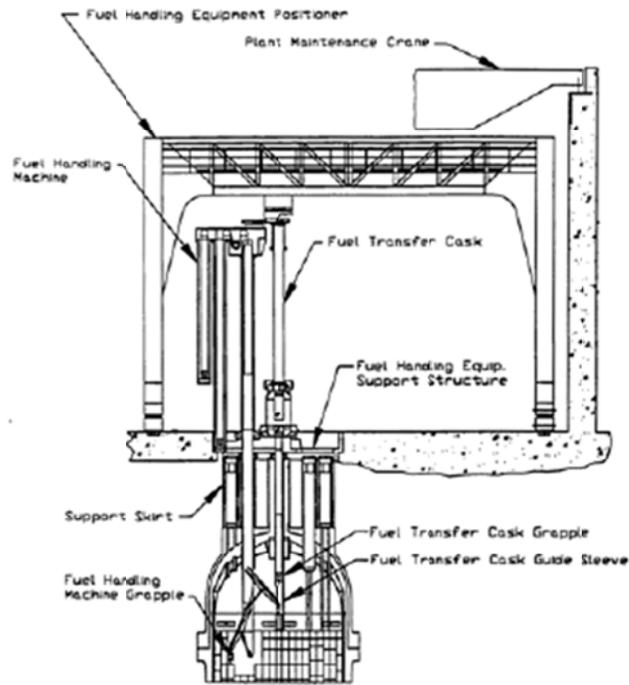


Fig. 77. Fuel handling system.

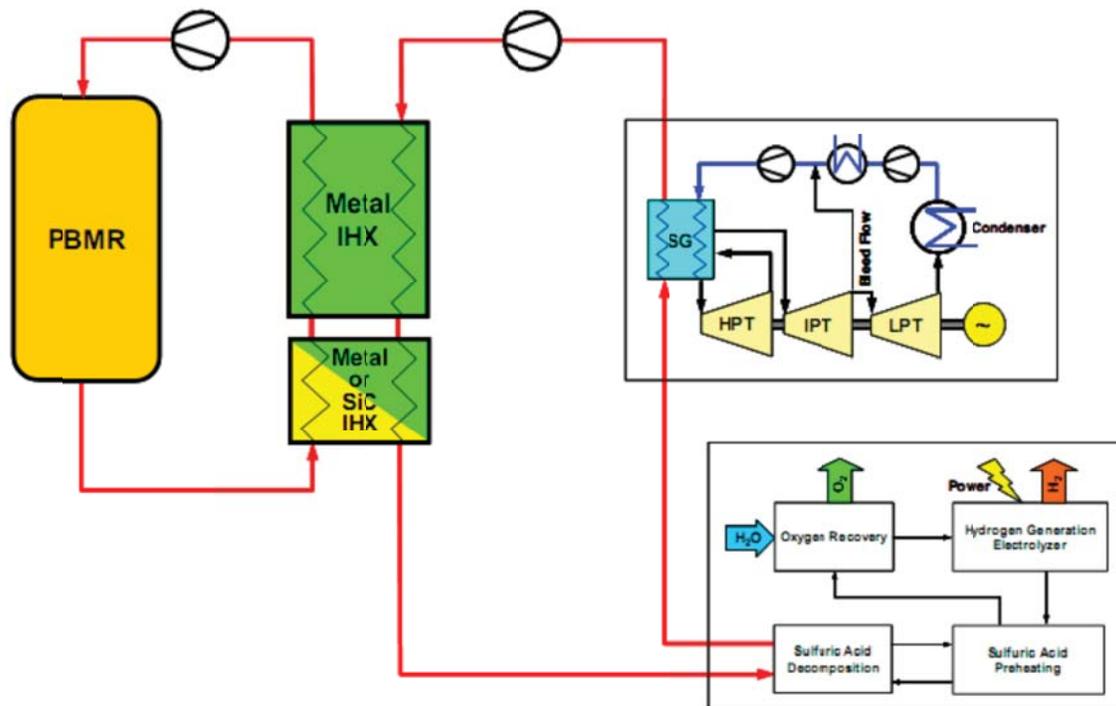


Fig. 78. Westinghouse original NGNP configuration.

[NGNP Project 2009 Status Report, INL/EXT-09-17505]

AREVA's design is based on the ANTARES plant, which was designed to produce electricity and provide high-temperature process heat as shown in Fig. 79. Intermediate loops feed a combined cycle turbine configuration used for electricity production using a gas turbine with a steam bottoming cycle and the processes requiring high-temperature heat.

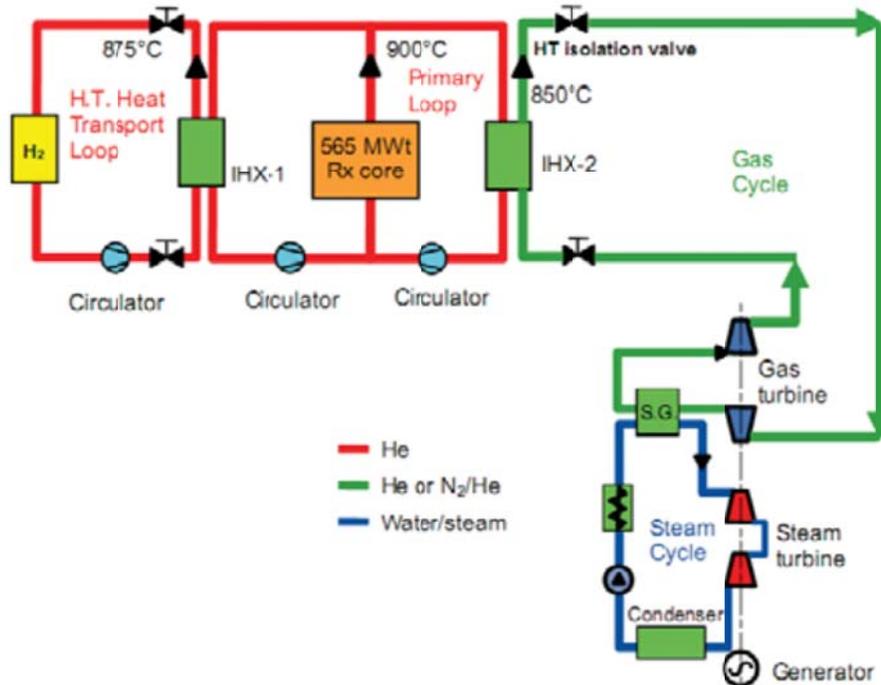


Fig. 79. AREVA original NGNP configuration.

[NGNP Project 2009 Status Report, INL/EXT-09-17505]

General Atomics original design was based on the GT-MHR plant and used a direct Brayton cycle gas turbine and an intermediate loop to deliver high-temperature process heat as shown in Fig. 80. A vertical axis turbine configuration was planned as shown on the left in the figure. A compact heat exchanger to provide high-temperature heat is shown on the right.

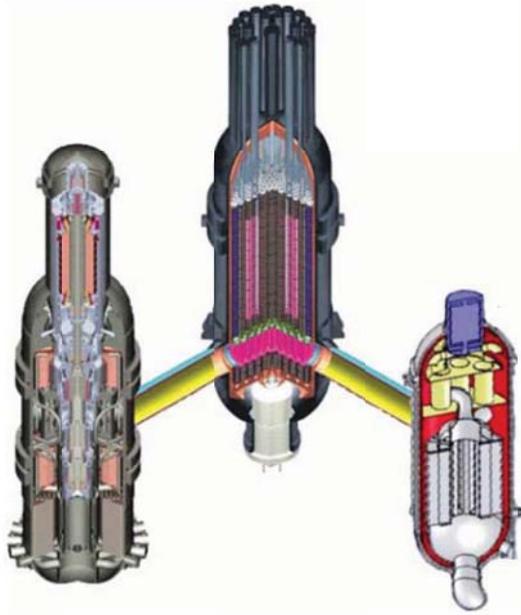


Fig. 80. General Atomics original NGNP configuration.

[*NGNP Project 2009 Status Report, INL/EXT-09-17505*]

5.8 Vendor Design Comparisons

The *NGNP Pre-Conceptual Design Report* (INL-EXT-07-12967) includes comments from contractor teams supportive of their particular designs. Westinghouse noted that

- the PBMR fuel and fueling system has been demonstrated and qualified based on AVR experience,
- PBMR development costs and risks are lower because of ESKOM's work on the PBMR demonstration power plant;
- a vendor/supplier infrastructure has been established;
- higher capacity factors inherent in the design (due to online refueling);
- lower fuel temperatures during normal operation result in lower maximum radionuclide releases under accident conditions; and
- lower fuel temperatures during normal operation allow use of LWR reactor vessel steels, resulting in reduced vessel high-temperature steel development effort and cost.

AREVA noted (without elaboration in some cases) that their design had advantages over the PBMR design, including

- greater economic potential,
- higher power level and passive safety,
- design flexibility,
- U.S. license history (referring back to the Fort St. Vrain reactor), and
- predictable core performance and scheduled outages reduce the chance of forced outages.

General Atomics also noted benefits of its design over the PBMR design, including

- inherently higher reactor power levels resulting in better economics;
- less uncertainty associated with dust in the primary coolant loop, core thermal/hydraulic performance, ease of replacement of graphite reflectors, and fuel accountability; and
- more flexible fuel cycle options (e.g., MOX fuel, transuranics from LWR fuel).

The purported benefits of the various pre-conceptual designs may vary, however, following an assessment of the needs of potential end users [described in the NGNP Project 2009 Status Report (INL/EXT-09-17505)], since all the prospective design teams revised their designs and plant configurations to help bring the concepts to market faster and with lower risk from the technology development perspective. In the revised designs, the reactor outlet temperature is lower, lower reactor power options are considered, and the principal product is steam that could be used to power a steam turbine generator or be used for on-site processes requiring steam. End users in the petrochemical and fertilizer industries still voiced their desire for economic hydrogen production. Thus, the NGNP project continues to support development of hydrogen production capability. The Status Report noted “high temperature steam electrolysis as the leading candidate for integration with NGNP in 2021.” The design teams recommended that a prototype of a hydrogen production process be demonstrated separately from the NGNP plant configuration.

5.9 Pending Issues

The NGNP Project 2009 Status Report describes the considerable effort that has been expended to develop the preconceptual designs and realize accomplishments associated with research and development, engineering, and licensing areas (e.g., high-quality fuel manufacturing and initial testing, graphite testing, high-temperature metals testing, modeling methods, end user requirements, high-priority licensing issues, etc.). Additional issues to be addressed were also noted.

- *Reference configuration*—At this point (prior to the NGNP conceptual design) the full definition of project needs has not been established. The need for steam to power a turbine and supply an industrial process was established. A module for supplying high-temperature process gas may also be specified. The selection of a pebble core or prismatic core must be decided. Outlet temperature and power level specification will be determined. Design-specific analysis models are needed for use in finalizing reactor type, design configuration details, and to support pre-application licensing activities.
- *Completion of research and development qualification programs*—Four formal R&D programs are underway to validate that fuel, graphite, high-temperature materials, and analytic methods are adequate to ensure that design requirements are met. Two areas of special importance from the technical and licensing perspective are the confirmation of attenuation factors in barriers to fission product transfer to the environment in support of source term and dose calculations and determining the effects of air and water ingress to the core-on-core integrity and source term. Low-dose rates under all conditions are critical to being able to locate an HTGR onsite with the user of process heat.
- Analysis codes for gas-cooled reactors need to be updated to reflect the results of experimental and development work since they were originally developed.
- Development of a commercial supply of reactor fuel and reactor-grade graphite.
- *ASME code case development*—Code cases and specifications are needed for graphite core components. Code cases may need to be updated for some materials to cover the operating temperatures expected, even given the reduced core outlet temperature specification.
- *Equipment and materials infrastructure development*—A capable and reliable supply of equipment and materials is needed for large vessels, helium circulators, ceramics, high-temperature heat exchangers, I&C components (for measurement of neutron flux, temperature, and flows in high-temperature conditions and for coordination and control of

processes across primary, intermediate, and other heat transfer loops), and valves used in high-temperature gas-coolant loops and to evacuate (dump) water quickly from steam generators.

- Facility or facilities for large-scale tests of critical components to ensure they achieve the technical readiness level for use in a first of a kind HTGR plant.
- Development and demonstration of hydrogen production processes.
- Improving cost and schedule estimate confidence levels.
- *Control of contamination affecting co-located users and products*—The process by which products produced co-located industrial processes could be contaminated by radioactive materials and the consequences to the plant energy users need to be understood and communicated.
- Design, licensing, and operational impacts of plants with multiple reactor modules and potentially shared control areas and staff.
- *Integration with end user industrial processes*—The process of integration of nuclear codes and standards with complex requirements of various industrial uses requires further development.

6. KEY ISSUES IN I&C FOR NGNP

6.1 Issues in Licensing

One of the strategies of HTGR designers has been to use the inherent safety properties of the HTGR design to gain an economic advantage by the reducing the number and scope of safety systems required in comparison to conventional LWR designs. Two of the proposed changes are (1) not to have a sealed containment but to rely on the ceramic fuel particle coating for protection against release of radioactive fission products and (2) to lower the safety designation of some equipment which has traditionally been designated by the NRC as safety-related to a new designation which is called “investment protection.” This strategy may have an indirect effect on I&C systems which are discussed in this section.

6.1.1 Safety system vs investment protection system

In the preliminary licensing proposal on the MHTGR presented by General Atomics to the NRC,⁵⁸ a licensing strategy was proposed that may foretell a trend in NGNP protection systems. The strategy was to take advantage of the inherent safety of the design to reduce the number of systems considered to perform safety-related functions. Certain functions which protect equipment but are not necessary for meeting dose limits in accident analysis are put into a new category of equipment which General Atomics called “investment protection systems” rather than “safety-related systems.” Systems that are investment protection in the MHTGR include many support functions that would be safety-related systems for conventional LWRs. The distinction between the safety and investment protection label is not in the systems themselves. The applicant is certainly motivated to protect his investment in the plant. The objective of the “investment protection” designation is to reduce regulatory oversight and leave the determination of acceptability of the investment protection systems to the licensee. The purpose of the designation is presumably to make the HTGR economically more competitive by reducing licensing and oversight costs associated with safety-related equipment.

The inherent safety function provides only limited protection of equipment other than the fuel itself. While the fuel is generally protected and radiation release is predicted to be within 10CFR100 limits

⁵⁸*Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, December 1995.

when relying solely on passive response of the reactor system, other equipment important to investment and operation may be vulnerable at the temperatures that may exist in the reactor and confinement cavity when only the inherent passive cooling is available. Active components such as pumps, valves, motors, control rod drives, and instrumentation may in fact be damaged by the high temperatures reached when the plant is involved in a worst case event unless active cooling systems are operational. The class of support function which would cool the active components is called “investment protection.” The concept of “investment protection” as an intermediate class between safety-related and nonsafety-related is a licensing approach that has not been accepted by the NRC. When the MHTGR preconceptual design was reviewed by the NRC, one of the unresolved issues was the concept of “investment protection” rather than “safety-related” designation for equipment analogous to LWR systems which are safety grade.

The regulatory basis for making auxiliary cooling equipment safety-related may come down to the need for maintaining diversity. The inherent reactivity control and passive core cooling method of protecting the public from radiologic release is a single type of protective function. The reliability of the inherent protection depends on the engineering of that design to have foreseen the most limiting conditions and designed the system adequately to shutdown the reactor and remove decay heat so that the limiting conditions for the fuel damage are not exceeded. If this analysis proves to be in error, there is not backup system to cool the plant. The high temperature could cause failure of most of the active cooling and reactivity control systems rendering any other cooling option but the inherent properties unavailable. Applying the diversity principle, it would seem that a different safety system (in this case an active system and any supporting equipment cooling functions) must back up the inherent features, thus requiring the component cooling water and shutdown cooling systems to be safety-related. In any case, it seems a weak safety argument to rely solely on the inherent properties. If component cooling systems fail and all instruments, pumps, and valves consequently fail, the operator has very few options to take corrective action to bring the plant to a safe configuration under any unforeseen circumstances. Making systems safety-related means that the NRC has the responsibility for determining that the supporting cooling systems are adequate.

6.1.2 Confinement vs containment

The confinement rather than containment strategy is touted as both an economic savings and safety enhancement. The reduced maximum pressure requirement of the confinement translates directly into significant construction cost savings. The advance in reactor safety is a more complex argument but hinges on releasing high energy coolant (high temperature and pressure helium) but low contaminated helium gas initially. The inventory of helium released from the reactor to containment is argued to be a higher risk for severe consequence if retained than if released. Helium release later may become more contaminated because of the progress of the event and higher fuel temperature. Retaining the high energy gas in a containment creates a mechanism for distributing the contamination more widely if the containment cannot be maintained in the long term.

The instrumentation and controls issue is that the new confinement strategy relies on radiation monitors and active control of relief valves and filtering systems to maintain safety whereas traditional containment buildings are primarily passive structures. In this case, it appears that the HTGR designs have swapped the LWR’s passive safety system (i.e., sealed containment) for an active controls system (confinement with direct release and filters and controls). It is not clear what licensing issues may emerge from the confinement strategy. But, the use of active controls and filtering processes for protection of the public against a radiation release in a loss of coolant accident is a new idea that must undergo careful scrutiny and requires development of appropriate regulatory guidance and acceptance criteria.

6.2 Issues in Protection System

6.2.1 High-temperature effects

Since the introduction of inherent safety as a design and operating principle of the AVR, all HTGRs have been designed to use the negative Doppler coefficient to shutdown the reactor in conjunction with a continuous passive heat removal process that is capable of removing the worst-case decay heat from the core without an active cooling system. The inherent safety approach makes the HTGRs safe from fuel damage and radionuclide release in excess of licensing limit even under some of the most severe accident conditions conceivable. However, the high temperatures that exist under passive cooling are potentially damaging to many systems in the plant. The consequences and vulnerabilities of systems to the resulting high temperatures needs to be fully understood. Operability of most of the active components, such as motors, valves, even control rods themselves, could be compromised. Peak temperatures in the upper head during passive cooling are difficult to calculate and measure. The main concern of LWRs is the fuel which is very susceptible to damage in loss of coolant and other undercooling events. In HTGRs, the fuel is much more robust to the consequences of accidents. However, other systems may be vulnerable. The issue is, what is the essential function of the safety system? Does an NRC-approved safety system have to preserve options for the operator to initiate an active system despite engineering predictions that they are not needed for protection of the fuel?

6.2.2 New types of protection systems

The inherent safety properties of HTGRs eliminate or significantly reduce the risk of some of the most severe accidents that LWRs deal with. However, some new types of active safety systems may require formulation of new requirements and guidance. The most severe accidents for HTGRs involve air and water ingress. Air ingress may rely on measures to reduce or restrict available air in the vicinity of a leak. Mitigation measures, such as foam to stop or slow air ingress, may be required to protect the fuel from erosion by oxygen. Water ingress may require an operable helium purification system to remove moisture in water ingress events. Confinement systems with active controls on either filtered or released helium leaked from the primary system in a depressurization event are also a new type of protection system. An inadvertent restart of a helium circulator following any emergency shutdown when the core is at peak temperature can produce helium temperatures that would damage heat exchangers. An inhibit function to prevent the start of the circulator when the core temperature is high may be needed. Acceptance criteria for these new types systems are not suggested by the existing general design criteria.

6.3 Issues in Control Systems

6.3.1 Automation and operational awareness

The advanced plant may have a much higher level of automation than existing plants. It may employ trip avoidance strategies to reduce the demands on the protection system. The heat load of a chemical plant for hydrogen production is very likely to be a more complex system than a conventional electrical power plant. A combined cycle plant with electrical and heat plant loads requires the control system to manage the load distribution and to respond to all operating events and failures of all loads. The controls for combined plant is thus considerably more complex than a plant with a single load. Traditionally, the review of I&C systems has focused primarily on the protection system with only limited review or regulation concerning the operating control system. However, as the complexity of operation and the degree of automation increase, the safety implications of control also increase and may become a safety issue.

6.3.2 Protection of heat exchangers from hot helium in loss of process heat plant

Very high temperature reactors for hydrogen production may operate with reactor outlet temperatures exceeding 900°C. Such reactors may have considerably greater reliance on active control systems to ensure emergency cooling of metallic components such as a steam generator or gas-to-gas intermediate heat exchangers from excessively high temperature during or following common operational occurrences. At temperatures proposed for hydrogen production, the heat exchanger materials could be subject to thermal shock or overheating. Active systems to isolate both sides of the heat exchanger or to provide emergency cooling from the secondary side may be required.

6.3.3 Support system controls

The discussion in this report focuses on the instrumentation and controls for the reactor and major heat transport systems. Other controls may also need to be examined in some detail in the future. Some control systems in HGTRs may be new or unique and may have greater safety implications than control in traditional LWR power plants. Two such control systems which bear examination are the magnetic bearing control for the helium circulator and shaft seal controls.

One potential concern regarding the magnetic bearing controller is that a failure of the control device and catcher bearings could cause the displacement of the impeller and motor shaft leading to failure of the pressure boundary in the circulator. The magnetic bearing control design issue has been raised as a part of this review but no details of the magnetic bearing controls and their safety implications in plants which employ them have been found in literature. This event, a control system failure leading directly to a loss of coolant accident is a possible accident with a much higher severity category than other control system failures in licensing reviews.

A related problem is helium shaft seals. The helium circulator motor and shaft are likely to be externally sealed. That is, the motor and impeller are sealed within the helium pressure boundary. However, the main coolant cannot be allowed to circulate freely around the motor and impeller because of dust in the coolant which could damage the circulator components and radioactive contamination deposits which would greatly increase the radiation exposure of workers during maintenance. The helium from the main reactor circuit must be kept out of the internal motor and impeller space by internal seals and a flow of higher pressure clean helium into the space toward the reactor. Because the consequences of failure are severe, control of the seal flow and cooling becomes an issue for the regulator.

Draft Letter Report

TASK 2—HIGHLY AUTOMATED CONTROL ROOM DESIGN FOR VHTRS

R. T. Wood, M. S. Cetiner, D. L. Fugate, R. A. Kisner, and T. L. Wilson, Jr.
Oak Ridge National Laboratory

September 2011

Project JCN N6177

Technical Monitor: Y. Yang, NRC RES
Principal Investigator: T. L. Wilson, Jr., ORNL

Prepared for the
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

	Page
LIST OF FIGURES	v
LIST OF TABLES	vii
1. INTRODUCTION	1
1.1 Project Overview	1
1.2 Task Objectives.....	2
1.3 Organization of Report.....	2
2. AUTOMATION TECHNOLOGIES	3
2.1 Resilient Control	3
2.1.1 Framework	4
2.1.2 Features	6
2.1.3 Functions	7
2.1.4 Formulation.....	8
2.2 Autonomous Control.....	15
2.2.1 Experience.....	15
2.2.2 Characteristics and functionality.....	17
2.2.3 Functional architectures	18
3. AUTOMATION OF NUCLEAR POWER PLANT OPERATIONS.....	22
3.1 Plant Control	22
3.1.1 Integrated control systems.....	22
3.1.2 Supervisory control systems.....	24
3.2 Plant Limitation	27
3.2.1 Limitation philosophy	28
3.2.2 Limitation functions.....	28
3.2.3 Reactor limitation system architecture.....	29
3.3 Concepts of Operations.....	31
3.3.1 Scope.....	32
3.3.2 HTGR operations	32
4. REGULATORY BASELINE FOR HIGHLY AUTOMATED CONTROL ROOMS.....	40
4.1 Code of Federal Regulations.....	40
4.1.1 General design criteria	40
4.1.2 Criteria for safety-related I&C systems	42
4.1.3 Guidance for safety-related digital I&C systems	43
4.1.4 Control room staffing criteria.....	44
4.2 Interim Staff Guidance.....	45
4.2.1 Digital I&C ISG-02: Diversity and Defense-in-Depth Issues.....	45
4.2.2 Digital I&C ISG-04: Highly-Integrated Control Rooms—Communication Issues	48
4.2.3 Digital I&C ISG-05: Highly-Integrated Control Rooms—Human Factors Issues	53
5. NEXT GENERATION NUCLEAR PLANT AUTOMATION	59
5.1 Operational Requirements.....	60
5.2 Resilient Functionality	61

5.3	Automation Strategy	62
5.4	Integration with Industrial Processes	65
6.	KEY ISSUES FOR HIGHLY AUTOMATED CONTROL ROOM DESIGNS IN VHTRS.....	66
7.	REFERENCES	67

LIST OF FIGURES

Figure		Page
1	Resilient control capabilities	4
2	Relationship between communications (IT) cyber-security and resilient controls	7
3	Resilient control functional formulation	9
4	Real-time physics-based dynamic model examples	10
5	Formulation of real-time physics-based model usage for validating signals	11
6	Example of real-time physics-based model detection of an input signal failure	11
7	Historical knowledge function to create historical operating space and backup commands	12
8	Formulation of historical knowledge usage for validating input signals and commands.....	13
9	Example of mapping of commands to process conditions and states based on historical knowledge	13
10	Formulation of situational awareness system.....	14
11	Situational awareness methods.....	14
12	Typical three-level autonomous control architecture	18
13	Remote Agent architecture for Deep Space 1	20
14	CLARAty architecture with decision and functional layers.....	21
15	PCS integrated control design	24
16	Supervisory control architecture for multi-modular nuclear power plants.....	26
17	I&C architecture for German PWRs	31
18	MHTGR plant supervisory control system overview	38
19	Extended functionality provided by resilient control	62

LIST OF TABLES

Table		Page
1	Minimum requirements per shift for on-site staffing of nuclear power plant units.....	45

TASK 2—HIGHLY AUTOMATED CONTROL ROOM DESIGN FOR VHTRS

DRAFT LETTER REPORT

R. T. Wood, M. S. Cetiner, D. L. Fugate, R. A. Kisner, and T. L. Wilson, Jr.
Oak Ridge National Laboratory

September, 2011

1. INTRODUCTION

1.1 Project Overview

The objective of the project designated as Job Control Number (JCN) N6177 is to support the U.S. Nuclear Regulatory Commission (NRC) in identifying and evaluating the regulatory implications concerning the control and protection systems proposed for use in the U.S. Department of Energy's (DOE's) Next Generation Nuclear Plant (NGNP). The NGNP, using gas-cooled reactor technology, will provide the basis for the commercial industry to manage the heat for energy production and industrial processing including hydrogen production. The high temperature gas-cooled reactor (HTGR) can provide heat for industrial process at much higher temperatures than conventional light water reactors, from 700 to 950°C. (Note that for the upper range of these operating temperatures the HTGR is sometimes referred to as the Very High Temperature Reactor or VHTR. In this project, the gas-cooled reactor design for the NGNP is referred to as the VHTR even though DOE's current plans focus on the lower end of the above-noted temperature range for ultimate deployment of NGNP.)

The JCN N6177 project involves five tasks, which are titled:

- Task 1. Control and Protection Systems in VHTRs for Process Heat Applications
- Task 2. Highly Automated Control Room Design
- Task 3. Models for Control and Protection System Designs
- Task 4. Advanced Control and Protection System Design Methods
- Task 5. Develop Technical Guidance and Acceptance Criteria for Safety-Related Protection and Control Systems Designs

The overall objective of this research is to review potential technologies likely to be employed for the control and protection system design for the VHTR for process heat applications including possibly hydrogen production. The investigation also addresses modeling methods and plant models, including multi-modular models, as well as the level of automation that can be achieved and the degree of integration in control room designs that may result. In addition, this research examines such design aspects and issues as prediction of the state and effect of control systems actions, overall resilience of the control and protection systems designs, and fault detection capability. The culminating activity, to the extent possible based on the maturity of the VHTR design and particular process heat application, is to assist NRC in developing technical guidance and acceptance criteria for these safety-related protection and control systems designs for the VHTR.

1.2 Task Objectives

The principal objectives of Task 2 are to investigate automation features and approaches that may be considered in VHTR control room designs and to identify technical issues arising for high levels of automation that could impact safety. In order to assess the potential safety impact of highly automated control rooms for VHTRs, the research approach employed involves determining the extent of automation and identifying key design features. As part of the investigation of automation issues, consideration was given to increased complexity of control and protection that could arise from management of alternate generation products and implementation of multi-modular plants.

The investigation focused on the systems aspect of automation and integration within the VHTR and process heat plant control room(s). Specifically, the coordinated control and protection within a unit and/or among units, the impact of interconnected systems, and fault tolerance capabilities were considered. The primary emphasis of this investigation is the prospective application of state-of-the-art automation approaches and assessment of the impact on the degree to which the control room of a VHTR plant may be highly integrated.

As part of the research activity, issues associated with control and protection of multi-modular plants were investigated. These issues included integrated control of reactor and process heat plant systems, automated transition (e.g., switching or redistributing flow) among multiple heat transport systems to enable support of co-generation plants, complex dynamics for multiple reactors feeding a common process heat plant, and combined operation of multiple reactors. No concrete examples of existing plants or near-term designs were found that gave explicit examples of applications incorporating these characteristics. For example, the evolving NGNP design indicates that the nuclear power plant control room will be separate from management of any process heat plant (i.e., hydrogen production plant) and that isolation capabilities will be provided to decouple the plants as needed in the event of upsets. Thus, the extent of the investigation into unique (i.e., VHTR or process heat plant specific) issues for automation technologies and approaches was limited by the available information.

Since the treatment of plant staffing requirements and human-machine interfaces implementations are covered under regulatory reviews of nuclear power plant instrumentation and control (I&C) systems, this investigation did not address human factors considerations in any detail. However, potential challenges associated with operational approaches enabled by highly automated control rooms were considered to the degree supported by the available information.

1.3 Organization of Report

Task 2 involves an evaluation of automation technologies and operational approaches that are relevant in considering the safety implications of highly automated control room design for VHTRs. Chapter 2 presents the state of the technology for automation by describing the characteristics and capabilities associated with resilient control and autonomous control. Chapter 3 discusses automation for nuclear power plants. In particular, examples of integrated plant control, plant limitation strategies, and HTGR concepts of operations are documented. Chapter 4 summarizes relevant regulations and regulatory positions to establish the regulatory baseline for review of highly automated control rooms. Chapter 5 presents the design considerations and proposed strategies for automating NGNP. Finally, Chapter 6 discusses insights into key regulatory issues arising from highly automated control room design for VHTRs.

2. AUTOMATION TECHNOLOGIES

The operation of a plant or system is managed through the interaction of humans or electronic equipment with field devices (i.e., actuators) that can affect the process (i.e., control). The command for a specific action is initiated by either manual input or automatic control action (or some combination of each) based on information about the state of the plant systems or processes (e.g., measurements, diagnostics, constraints, procedures). For automated control, the command or control action is the result of calculations that are based on process measurements and accomplished by control algorithms implemented in hardware or software. No human intervention is required, although the automatic control function can be switched out to permit direct manual control.

In traditional control systems, the decision-making (i.e., the choice among valid solutions or options) is left to the human. Elements of the decision process, either during design or operation, include determination of the control strategy (i.e., goals, key variables, available actuators) to be employed, establishment of the acceptable range of actions, and the coordination among individual control loops during all events and conditions. Generally, the application of automation is limited to repetitive or sequential tasks for specific operational modes, continuous regulating control for well-defined normal-operation scenarios, and fast-acting predetermined protective actions for design basis event conditions. In many cases, human intervention is required to retain operability during off-normal or unanticipated events, especially under failed or degraded conditions.

Automation has been employed by various process, manufacturing, power and transportation industries to minimize active reliance on human operators while increasing cost and performance efficiencies. Most instances involve the implementation of modern control methods and digital electronics to achieve automation of control loops, often with some degree of high-level integration for coordination or supervision. However, there are approaches to plant control that invoke more extensive automation capabilities to provide enhanced fault tolerance and to enable significantly reduced demands for active engagement by human operators. These control approaches may be applied to operational control and plant management of VHTRs to minimize the burden on human operators, optimize operations staffing requirements, and increase plant operational efficiency. This chapter describes key technological approaches to achieving highly automated control.

2.1 Resilient Control

At its most basic level, a process control system implements algorithms with real-time hardware and software to reduce the error to zero between a command and the output of a process during various conditions. A control system consists of control algorithms, implementation hardware, and data links or communication networks between individual controllers. Traditionally, process control focuses on maintaining stable operation under a range of well-defined conditions of noise, changing parameters and exogenous inputs to the controlled system. The traditional approach, which may provide optimal control across a specified narrow range, does not incorporate a means for adapting to a wide range of disturbances, failure events, errors, subsystem losses and incorrect human intervention (accidental or malicious). Modern approaches to control system design treat fault tolerance, failure immunity, and reliability in addition to controller performance.

The concept of resiliency has been developed through control theory research to address issues such as disturbances, failure events, errors, incorrect human operation, and cyber-attacks.¹ A resilient control system is defined as “one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected or malicious nature.”² In this sense, state awareness involves knowledge of conditions and parameters relevant to control decisions, including an understanding of the status of the process being controlled and the control system itself. A primary goal in

achieving resiliency is to design, install, operate, and maintain control systems that can survive a natural disaster, human error, or intentional cyber-attack without the loss of any critical functions.³

Concepts and characteristics of resiliency are evident in aerospace, defense, and nuclear power industry applications. For example, provisions for independence and redundancy result in resiliency against single failures and propagation of effects while the incorporation of diversity in an I&C architecture provides resiliency against common-cause failure. Signal validation, error checking and recovery, and self-diagnostics are specific techniques that are widely implemented to detect failures and respond to their consequential effects.

Resilient control offers advantages with respect to traditional control. Unlike the primarily reactive nature of traditional control systems, a resilient control system is proactive in its approach. Resilience involves rapidly identifying threats, generating essential operational information, and enabling an adaptive response to events and conditions. The scope of control in a resilient strategy extends beyond traditional control to include detection of abnormal conditions, selection of mitigation strategies, and a large degree of freedom to implement solutions in real-time.

2.1.1 Framework

The realization of truly resilient control involves a comprehensive, integrated treatment of complex networked system design, human interaction, and cyber-security. Design for resilient control provides for state awareness, accommodates human-automation interaction, accounts for complex interdependencies and latencies in highly integrated control, enables adaptation to unexpected conditions, and addresses cyber-threat mitigation and response.⁴ Fundamentally, resilient control integrates traditional feedback control concepts with the capability to adapt to a wide range of degradation and failures. Figure Fig. 1 illustrates the integrated capabilities that characterize resilient control. These resilient control capabilities are intended to address all identified threats, supply the means to determine operational status, and provide mechanisms by which to assure proper operation. The adaptive capabilities indicated in the figure address process efficiency and stability, failure management, security (physical and cyber), and process compliance.

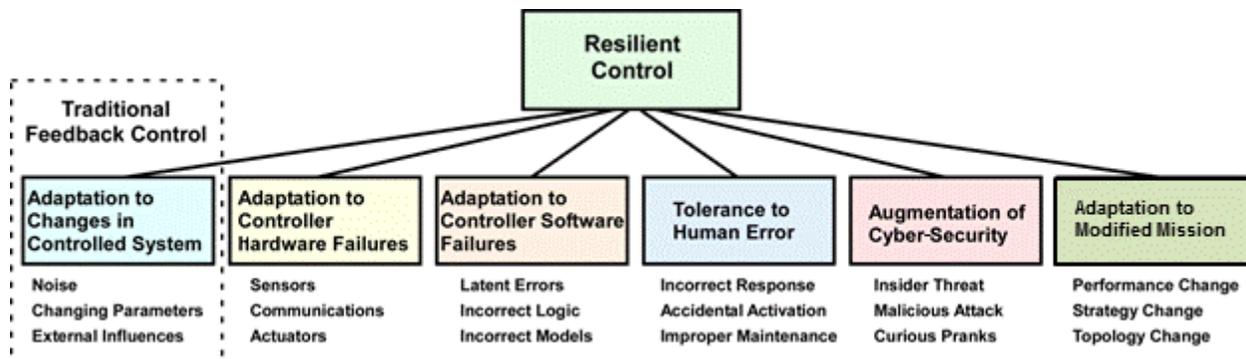


Fig. 1. Resilient control capabilities.

Reiger⁴ represents resilient control in terms of framework of three system elements: operational data and controls, intelligent interpretation and control, and operational state awareness dashboard. These framework elements roughly correspond to a physical architecture consisting of field equipment for measurement and actuation, computational electronics for control and monitoring, and human-machine interfaces for display and interaction. The operational data and controls element includes traditional control and measurement capabilities. The operational state awareness dashboard element includes information displays and operator support features, which can be tailored to meet the needs of specific

users based on access rights and experience. The intelligent interpretation and control element integrates knowledge extraction and human-automation interaction capabilities within a hierarchical, multi-agent* control system structure that can facilitate robust, adaptive control. The transition from data to information to knowledge is achieved through data fusion techniques while human-automation interaction support involves mixed initiative control (i.e., interfaces to support collaborative human response and automatic action).

Traditional measurement and controls focus on process stability and safety as principal goals. The operational data and controls element of resilient control systems introduces an expanded treatment of threats and events that could compromise operational control. The extended scope of resilient control is achieved by addressing process efficiency, security, and compliance in the control system design. As illustrated in Fig. 1, a resilient control system incorporates adaptive capabilities to address failure, error, intrusion, and management optimization. Adaptive and fault-tolerant controls are traditional means of promoting efficient performance and robustness against uncertainty, degradation, and failure. Resilient control extends these methods by taking a whole-plant approach employing integrated advanced control methods, embedding diagnostic and predictive capabilities to anticipate deviations from nominal behavior, and incorporating the capability to adapt and optimize from the local subsystem level to the global system level. Security is addressed through enhanced cyber awareness, with detection and mitigation capabilities embedded throughout the layers of control to ensure the integrity of the cyber environment. Compliance (e.g., inventory control, configuration management, nonproliferation and safeguards) is addressed through real-time knowledge management, tracking, and identification and accountability techniques.

The intelligent interpretation and control element of the resilient control framework facilitates the expanded capabilities of resilient control to anticipate, perceive, respond, and adapt to events, disturbances, and intrusions. In resilient control design, the collaboration of human and automation is taken into account in the implementation of monitoring and control. This consideration informs not only the allocation of roles and responsibilities but also impacts the selection of techniques and methodologies to provide the necessary information management and control capabilities to support both automatic and manual actions. In treating human support for mixed initiative control, the processing of data to generate information and extraction of knowledge from information must be addressed comprehensively to enable consistent, coordinated, and complementary interactions for optimal response of the human-system team. In addition, the mechanisms of human-automation collaboration are incorporated in the interface and communication capabilities of the control system design to enable access management with adaptation based on a user's needs and abilities.

The hierarchical, multi-agent structure adopts a supervisory design approach that allows the interrelated processes within a plant to be controlled in a coordinated, integrated fashion. Based on this approach, the global treatment of process (or plant) operation in the resilient control design is facilitated through integration and state awareness at higher levels of the hierarchy while fault tolerance and optimization are enabled through detection and adaption at the local levels of the hierarchy. The provision of knowledge generation and state identification capabilities allow for prioritization of information and tasks. The distributed, hierarchical structure permits semi-autonomous operation of local control within boundaries established for global coordinated control. Basically, the higher levels of the hierarchy 'oversee' the lower levels with goals, demands, and constraints being communicated downward and data to support

* An "agent" (sometimes called an "intelligent agent") is defined as "a person, a machine, a piece of software, or a variety of other things, i.e., one who acts."⁵ While the application of individual agents is possible, their greatest potential is realized when multiple-agents work together to achieve a common goal. These collectives are known as multi-agent systems. A requirement that is essential for multiple agents to cooperate is that they share a common "view" of their world and be able to communicate in a common "language" or ontology. An agent is characterized by knowledge (i.e., beliefs, goals, plans, assumptions, etc.), and it interacts with other agents using an agent communication language. An agent can also possess additional characteristics, such as being autonomous, interactive, adaptive, proactive, cooperative, competitive, etc.

state awareness being communicated upward. In addition, the flexibility and reconfigurability offered by the hierarchical structure facilitates real-time adaption (e.g., “autonomy on the fly”⁶).

2.1.2 Features

Resilient control is intended to reduce the likelihood of occurrence for adverse events and minimize the impact should such an event occur. Therefore, characteristics exhibited by a resilient control system must include features that allow it to anticipate, perceive, respond, and adapt.⁷ Perception and response are basic features of traditional control systems. These features correspond to measurement and control capabilities. However, resilient control systems have expanded capabilities to support perception of adverse situations and conditions and enable response to degraded or unanticipated circumstances. Detection and diagnosis of threats involves capabilities such as condition monitoring and state identification. Anticipation and adaption are not common features of traditional control systems. The anticipatory feature allows a resilient control system to predict disturbances, incipient failures, or other threats. Real-time simulation and model-based diagnostics and prognostics are examples of capabilities to support anticipation. The adaptive feature enables a resilient control system to adjust its control concept or mechanisms to accommodate extreme conditions or unanticipated events (e.g., system degradation or beyond-design-basis events). Basically, a resilient control system minimizes the consequences of events by perceiving disturbances and responding appropriately. Furthermore, a resilient control system reduces the likelihood of adverse events by anticipating challenges and adapting as necessary.⁸

A specific example of a control system feature that is unique to resilient engineering is embedded cyber-security. This feature involves more than imposed isolation and intrusion detection techniques that have been developed for the Information Technology (IT) application domain. A common characteristic of traditional supervisory control and data acquisition (SCADA) systems that differentiates them from IT systems is that communicated commands (internally or from operators) are treated as valid. This fundamental TRUST Model assumption poses a vulnerability that can be exploited by malicious intruders should they defeat the typical IT cyber-security measures. Thus, defensive capabilities are included in resilient control designs to confirm the authenticity of commands and the acceptability (e.g., safety, investment protection) of actions based on those commands.

Recently documented attacks on control systems, such as Night Dragon and STUXNET, demonstrate the potential for and consequences of this type of malicious cyber activity.^{9,10} These attacks have shown that vulnerabilities in SCADA systems can be used to acquire information and disable or disrupt physical processes and critical infrastructure. STUXNET was able to penetrate an air-gap isolated system in which it proceeded to destroy hardware process systems, devices and components while remaining undetected for a significant length of time. Attack vectors such as STUXNET could be successfully defended with resilient control capabilities that recognize the malicious behavior and maintain the system in a safe operating domain.

The resilient control cyber-security approach includes an embedded capability for the control system to identify and reject improper commands that could lead to damage or a catastrophic failure. There are two main approaches an attacker can use to exploit a real-time control system once penetrated: (1) commands can be issued that will cause the larger system to become unstable in some way, thereby causing damage or destruction or (2) sensor data can be modified or corrupted so as to essentially blind or confuse the control algorithm. The effect of these cyber-attack vectors is similar to control system failures. This overlap permits methodologies developed to detect and survive failures to be employed to support resilience against cyber-attacks that exhibit the similar characteristics. Consequently, resilient cyber-security features (i.e., diagnostic capabilities and design attributes) that are embedded in the control system design can augment more conventional defense-in-depth cyber-security methods^{11,12} (i.e., techniques developed for IT systems). The concept is illustrated functionally in Fig. 2.

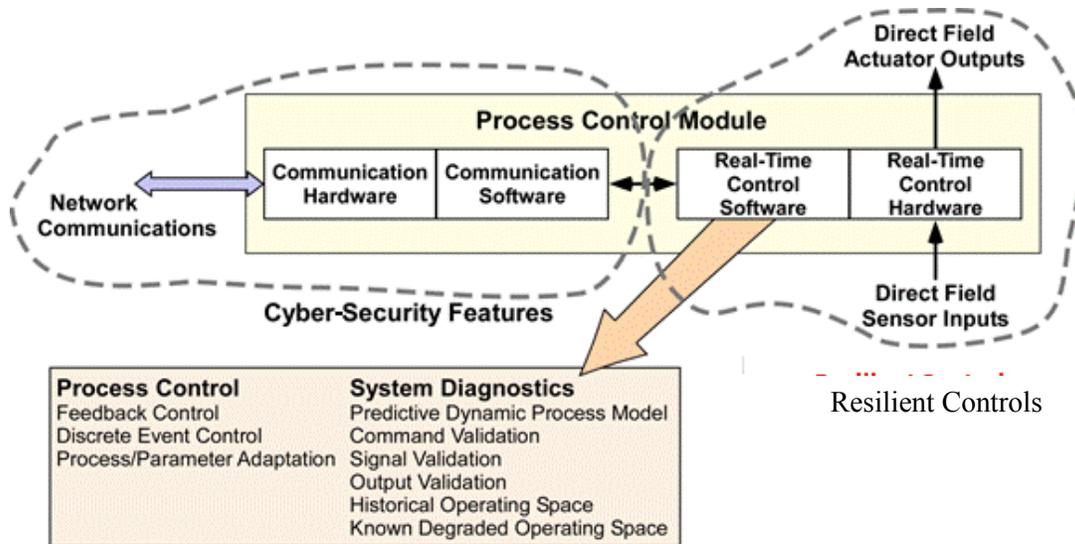


Fig. 2. Relationship between communications (IT) cyber-security and resilient controls.

After a cyber-intrusion has been detected, other resilient control features enable an appropriate response by the control system. To mitigate a cyber-attack penetration vector that is intended to manipulate commands, set points, or disable input signals, the resilient control responses can include:

- rejecting corrupted data and using substitute analytical data from a real-time model,
- avoiding the use of an incorrect operator command or set point and using a historical data-based or requirements-based substitute, or
- determination that the current degraded capability requires a revised modified mission, new operating mode, new commands, etc., to provide desired safety, stability, and performance.

2.1.3 Functions

Stevens⁶ characterizes a generic control system in terms of function to support a gap analysis in comparing traditional control and resilient control. The characterization consists of the following functions:

- monitor system,
- manage and process data,
- provide systems communication, and
- manage control processes.

The functions for monitoring the controlled system involve measuring state, input, and response data. The functions for managing and processing data from the system include collection, processing, storage, analysis, and retrieval of data. The functions for providing systems communication address the services and mechanisms for gathering or supplying information to the control system and operator as well as the interaction of the services and mechanisms with each other. The functions for managing control processes include regulating control and command issuance. Resilient control expands the basic functions customary for a traditional control system to enable the adaptive capacity to respond to threats and support the necessary level of state awareness to recognize or even anticipate disturbances.

For a resilient control system, system monitoring functionality includes additional functions to address cyber-security and optimization. The security functions provide for data authentication and diversity to promote data integrity. The optimization functions enable detection of incipient failure, prediction of abnormal behavior, and runtime condition-based adaptation. The extended functionality for data

processing and management include data validation, prioritization, and analytical prediction/simulation. In a resilient control system, communication functionality is augmented to provide for extensive security detection and response mechanisms (both passive and active) with an integrated approach to cyber-security for data transmission, information distribution, and knowledge display. The communication functions also facilitate adaptation to respond to cyber-threats, failures, and information needs (e.g., user access and display). Finally, control management functionality includes a hierarchical approach that enables semi-autonomous operation of subcontrollers, oversight provisions to ensure state awareness, and adaptation mechanisms for local optimization or graceful degradation of capabilities.

2.1.4 Formulation

Control systems configurations may be formulated as individual stand-alone systems or as distributed SCADA systems. SCADA systems consist of a supervisory controller that issues commands to distributed individual controllers that in turn regulate the behavior of physical processes under their control. As discussed above, a resilient control system constitutes a whole-plant, supervisory control system with extended capabilities. Key features include anticipation of failures or disturbances followed by adaptation to mitigate the potential consequences as well as perception of events and conditions followed by responsive action to ensure safety, stability, and performance. Detection of a failure, human error, or change in status and modification to accommodate degraded or altered conditions requires that a control system have the capability to identify abnormalities and to adapt as needed. Prevention of a cyber-attack penetration from sabotaging a physical process (e.g., by issuing damaging commands to the controllers) requires that the control system have the capability to determine if a command is destructive to the process directly under control and how a change in that process will affect the larger system.

To facilitate the necessary capabilities to achieve resilience, additional knowledge and tools must be available for the control system implementation:

- *Physics models*—information about the physics of the system so that it can estimate the current and future responses;
- *Historical knowledge*—previous safe operating parameters that provide command validation, input validation, redundancy and security in the decision-making process; and
- *Situational awareness*—information about the coupling between the controller’s processes and other processes that allow the controller to react in real-time to changes in process requirements, upsets, attacks and hardware failures.

Figure Fig. 3 illustrates the functional formulation for resilient control.

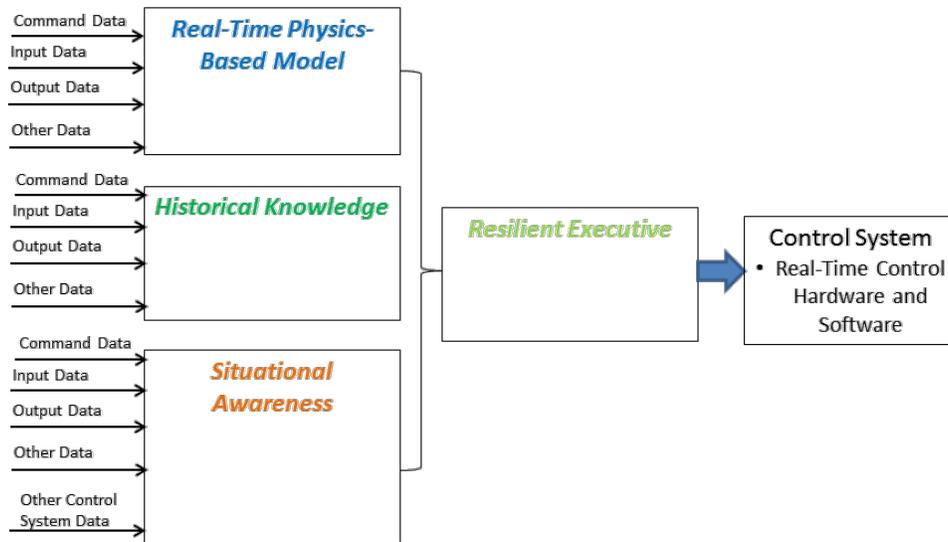


Fig. 3. Resilient control functional formulation.

In addition to detecting an abnormality with real-time physics-based models, situational awareness and historical knowledge, a Resilient Executive is required to manage the resilient capabilities and properly manipulate the real-time hardware and software control (Fig. 3). This would include concepts such as defined safe states in the event of catastrophic failure through stability landscapes from ecological resilience and reliability theory. These descriptions of stability regions for the system can then be used to provide boundaries for individual processes that guarantee the safety and performance of the larger system.

These capabilities require information about overall state awareness. As the availability of this information decreases, resilience of the control system will degrade until it eventually becomes comparable to a traditional control system. Basically, the availability of information and adaptive capabilities of the control system effectively serve as the equivalent of a margin between resilient control and the minimum acceptable control. Thus, the availability of status information allows the control system to determine the validity of commands and prevent the process (or plant) from being damaged by evolving to an unstable state.

2.1.4.1 Real-time physics-based models

Real-time physics-based models simulate the process and control system behavior over the correct range of conditions and operation. Real-time physics-based models are standard practice for various purposes in the aerospace and power industries. These dynamic models provide estimates of both the current and future state for desired parameters to facilitate the following: (1) comparison of input signals for validity to detect failures or cyber-attack events, (2) state estimation of key system parameters, (3) determination of system stability, and (4) determination of parameter sensitivities.

Figure Fig. 4 illustrates various examples for dynamic system modeling. Figure Fig. 5 illustrates a system using real-time physics-based models to detect valid input signal data. Figure Fig. 6 contains an example of a process input failure event. At T_0 , the input signal x_2 fails and is detected by the system at T_1 and declared not valid.

Methods such as integration, persistence and limit thresholds can process the disagreement of the model estimate and signal to determine possible input signal validity. System requirements for performance, stability and reliability can determine proper thresholds for input signal validity.

Model estimates can be used as control system inputs during conditions with invalid input signals. Models can also estimate and synthesize parameters that are not measured or cannot be measured to improve control system stability.

Proper requirements for the model design relating to the goals and objectives of the model for the desired parameter estimation are vital. The models must be validated and verified to the true system and must include considerations for uncertainties.

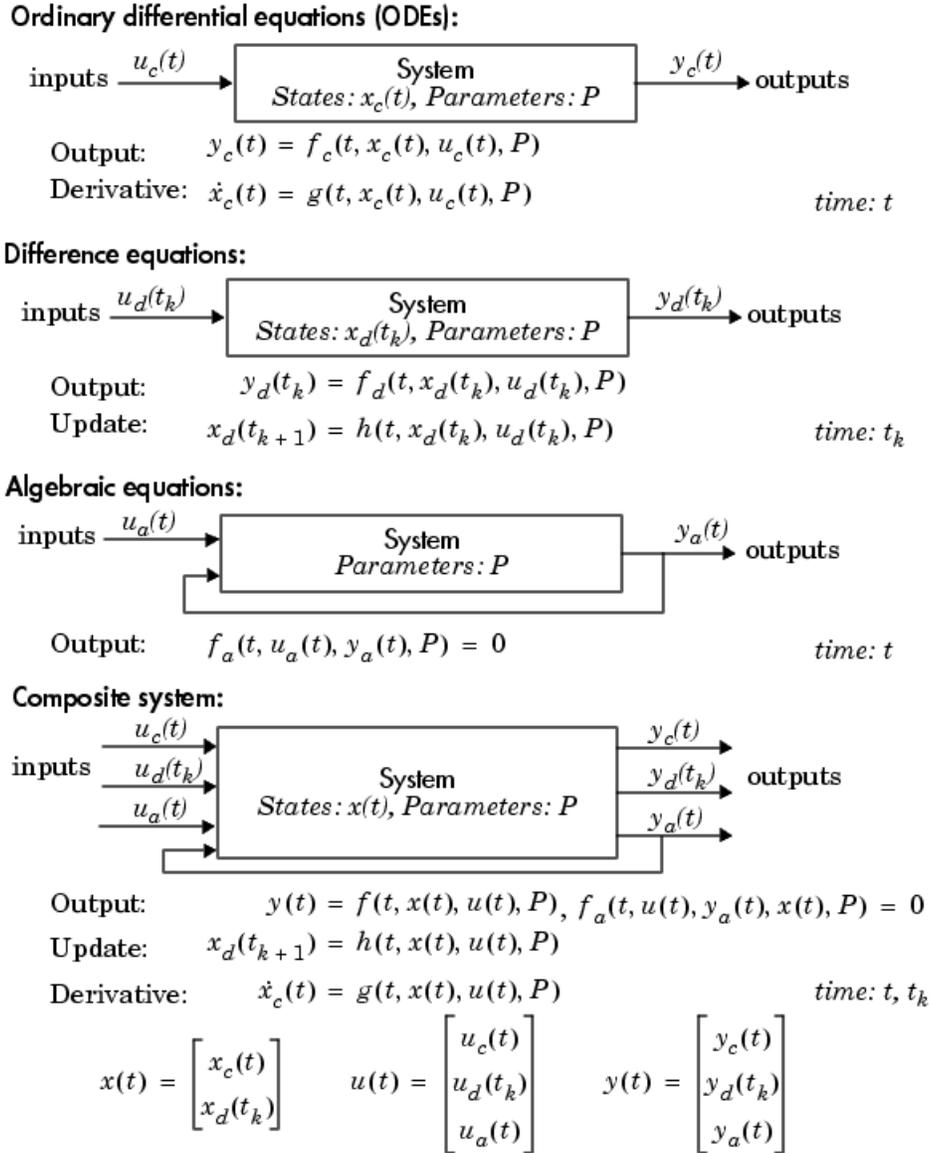


Fig. 4. Real-time physics-based dynamic model examples.

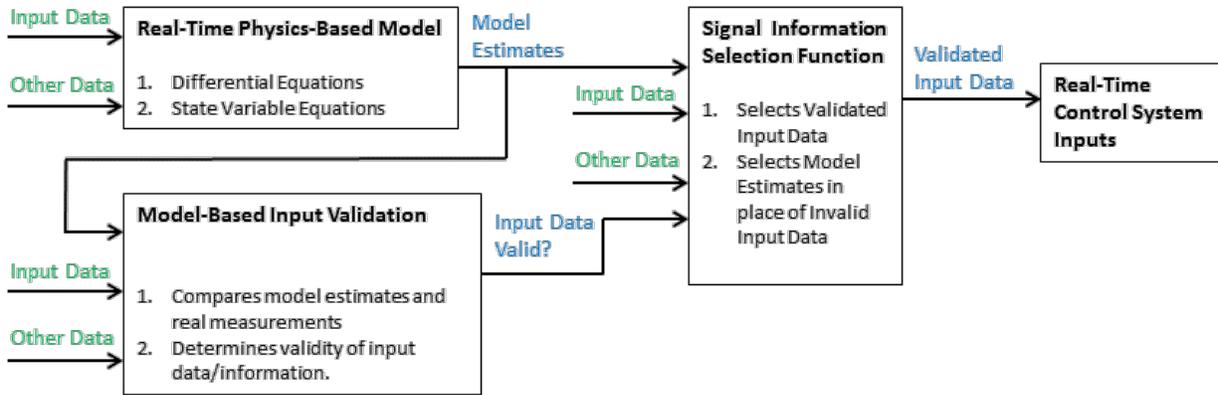


Fig. 5. Formulation of real-time physics-based model usage for validating signals.

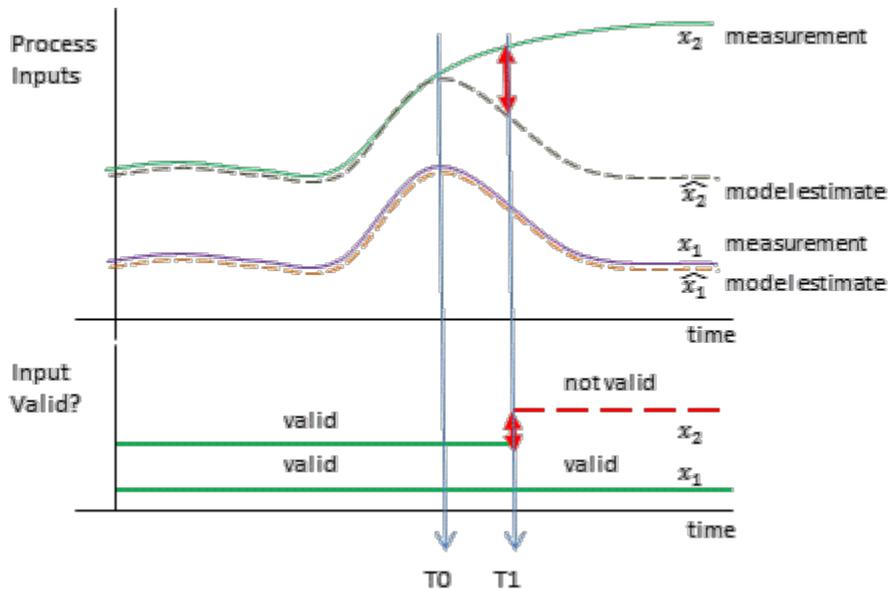
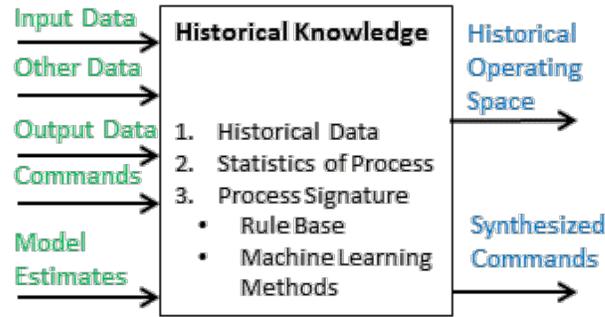


Fig. 6. Example of real-time physics-based model detection of an input signal failure.

2.1.4.2 Historical knowledge

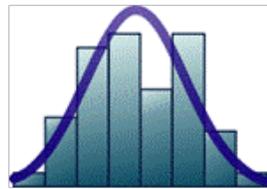
Historical data can be processed using various statistical methods, machine learning techniques and rule-based methods to create signatures of the process. These signatures can be used to compare present time input signals, commands and other data for validity to detect a failure or a cyber-attack event. Figure Fig. 7 illustrates a system using historical data with various methods (e.g., statistical estimation, mean, distribution, Bayesian, and Artificial Neural Networks) to generate a historical operating space and synthesized commands.



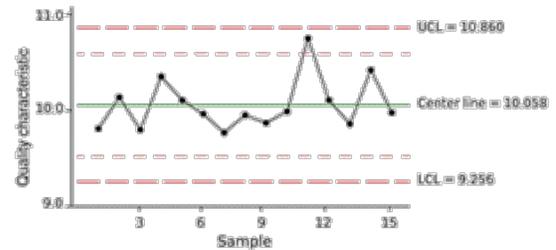
Expected Value

$$E[x] = \int_{-\infty}^{\infty} x f_x(x) dx$$

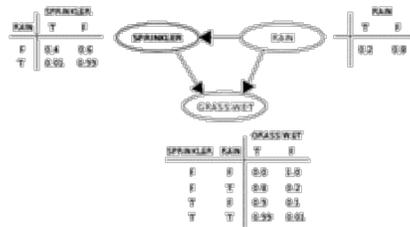
Distribution



Control Chart



Bayesian Network



Artificial Neural Network

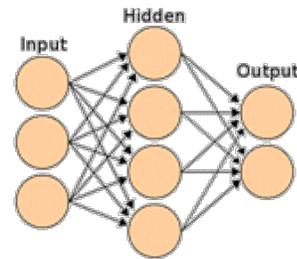


Fig. 7. Historical knowledge function to create historical operating space and backup commands.

The historical operating space describes typical process behavior and maps the system inputs and commands to operating conditions based on such behavior. The historical operating space is used to verify input signals and commands with respect to historical information for validity. Synthesized commands are generated from a mapping of system commands to operating conditions.

Figure Fig. 8 illustrates a system using historical data to validate input signals and commands. If an input signal is determined to be invalid, then actions can be taken. For example, the model estimate can be selected for control purposes. If a command is determined to be invalid, then several actions can be taken. For example, synthesized commands (from historical data) can be chosen with respect to the operating conditions.

Figure Fig. 9 illustrates the transformation and mapping that can be generated from the historical data to determine a valid command with respect to the current process conditions. An example of this concept follows:

1. A person drives an automobile on the same highway every day to work.
2. Historical data are developed for a particular stretch of the highway in the form of commands (speed, steering vector, and other relevant information), operating conditions, and location.
3. If on a particular day, the driver provides a suspect speed command, the system could determine that the command was not appropriate. The authority of the control to take action would have to be determined based on desired safety and other considerations.

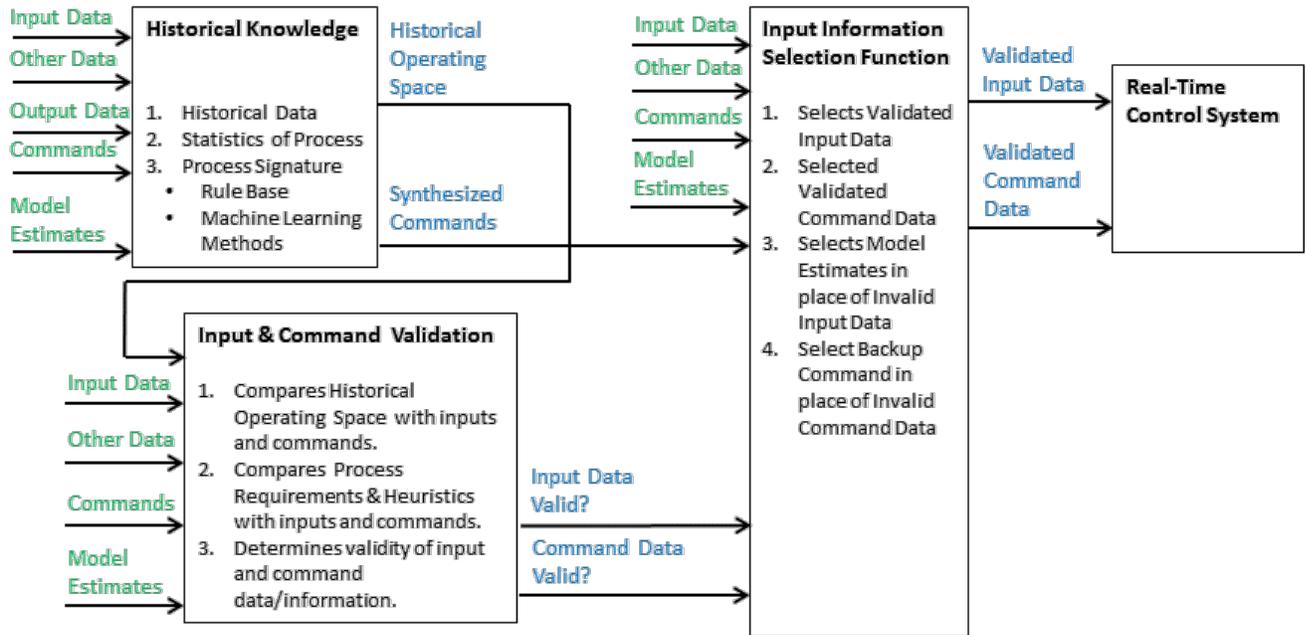


Fig. 8. Formulation of historical knowledge usage for validating input signals and commands.

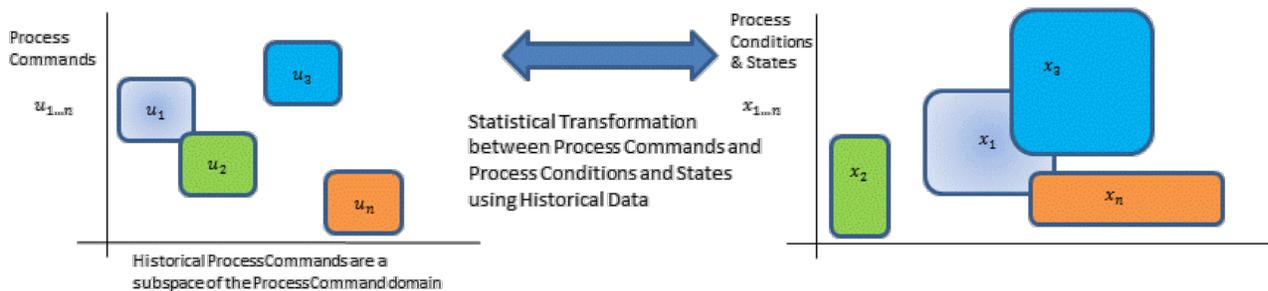


Fig. 9. Example of mapping of commands to process conditions and states based on historical knowledge.

2.1.4.3 Situational awareness

Situational awareness can be defined as “the combining of new information with existing knowledge in working memory and the development of a composite picture of the situation along with projections of future status and subsequent decisions as to appropriate courses of action to take.”¹³

Situational awareness is a method of examining the present states and information and determining if an abnormal condition exists and what options should be pursued as a countermeasure to maintain stability,

safety and performance. This examination capability will consist of systems such as a Heuristic Rule-Base, Fuzzy Logic Inference Rule-Base and other methods that describe the intended system behavior over the full range of operating conditions as shown in Figs. Fig. 10 and Fig. 11. In practice, situational awareness involves examining input data, output data, commands, model estimates, historical operating space, data from other control systems and synthesized commands with respect to the system and process requirements and to process uncertainty.

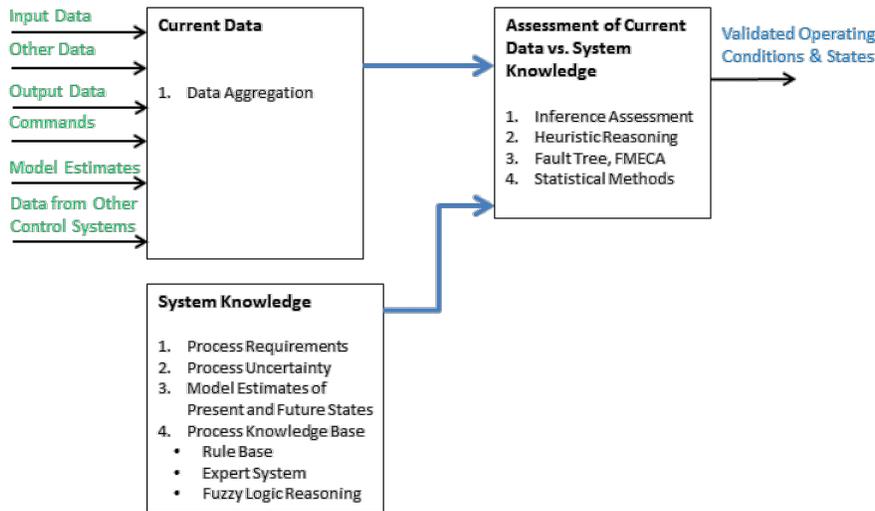
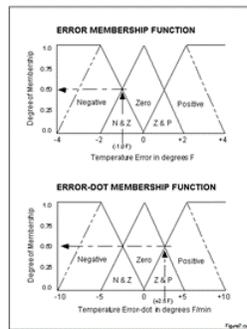


Fig. 10. Formulation of situational awareness system.

Fuzzy Logic



1. If (e < 0) AND (er < 0) then Cool 0.5 & 0.0 = 0.0
2. If (e = 0) AND (er < 0) then Heat 0.5 & 0.0 = 0.0
3. If (e > 0) AND (er < 0) then Heat 0.0 & 0.0 = 0.0
4. If (e < 0) AND (er = 0) then Cool 0.5 & 0.5 = 0.5
5. If (e = 0) AND (er = 0) then No_Chng 0.5 & 0.5 = 0.5
6. If (e > 0) AND (er = 0) then Heat 0.0 & 0.5 = 0.0
7. If (e < 0) AND (er > 0) then Cool 0.5 & 0.5 = 0.5
8. If (e = 0) AND (er > 0) then Cool 0.5 & 0.5 = 0.5
9. If (e > 0) AND (er > 0) then Heat 0.0 & 0.5 = 0.0

Expert System

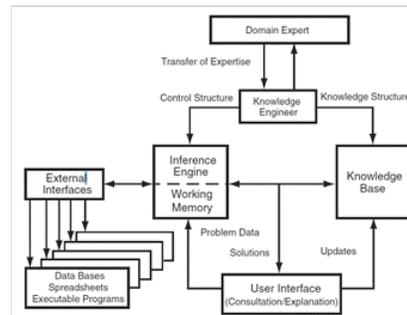


Fig. 11. Situational awareness methods.

One key characteristic is the ability to compare data from other control systems in a distributed architecture. If a measurement or condition is common to multiple control systems, then it is more likely

to be genuine. In other words, if an attack causes one control system to differ from the others in its behavior, a capability to compare with other control systems should detect the abnormal condition.

2.1.4.4 Resilient Executive

The Resilient Executive (see Fig. 3) manages the interface between the traditional real-time control system and the resilient features that detect an abnormal condition (e.g., hardware failure, cyber-attack, or incorrect operator command) and manipulate the information provided to the control system to maintain stability, safe operation and acceptable levels of performance. This management utilizes the results of physics-based dynamic model signal validation, historical data signal and command validation, and situational awareness validated operating conditions and states to manage the information provided to the control system. This would be realized using a rule-base and expert system based on requirements of reliability, robustness, failure immunity, safety, and desired levels of acceptable performance during an abnormal event.

2.2 Autonomous Control

There is a distinction between automated control and autonomous control. Consideration of the Greek root words illustrates the difference. *Automatos* means self-acting while *autonomos* means independent. Similarly, automated control involves self action while autonomous control involves independent action. Autonomous control implies an embedded intelligence. Although automation includes at least a limited inherent authority within the control system, automated control often consists of straightforward automatic execution of repetitive basic actions. It is clear that autonomous control encompasses automated control.

Automated control provides control actions that result from fixed set of algorithms with typically limited global state determination. As a result, automated control is often implemented as rigidly defined individual control loops rather than as fully integrated process/plant control. Although automated control requires no real-time operator action for normal operational events, most significant decision-making is left to the human rather than incorporated as part of the control system. In contrast, autonomous control integrates control, diagnostic, and decision capabilities without required human interaction. In particular, control decisions are the responsibility of the autonomous control function and can perform independently of any supervising operator. Control decisions may be model-based, derived from heuristics (i.e., rule-based) or experience (knowledge-based), learned over short and long periods (i.e., data-driven), or acquired from data mining of other systems. Diagnostics may execute at several levels: local process, equipment/components, and across multiple processes or modules. A flexible functional architecture provides the capability to adapt to evolving conditions and operational constraints. While automated control is common in numerous applications, autonomous control is more difficult to achieve and the experience base is very limited. Overviews of autonomous control characteristics, capabilities, and applications are given by Antsaklis,^{14,15,16} Astrom,^{17,18} Basher,¹⁹ Chaudhuri,²⁰ Passino,^{21,22,23} and Zeigler.²⁴

2.2.1 Experience

Control systems with varying levels of autonomy have been employed in robotic, transportation, spacecraft, and manufacturing applications. Space usage provides the most fertile application domain for the development of autonomous control. In fact, although autonomous control has not been developed for an operating terrestrial nuclear power plant, it has been the subject of research investigations for space-based reactors.^{25,26} However, since consideration of autonomous capabilities for space reactor control has primarily been conceptual to this point, this overview will focus on realized implementations of autonomous control for space exploration.

For more than a decade, the National Aeronautics and Space Administration (NASA) has pursued autonomy for spacecraft and surface exploration vehicles (e.g., rovers) to reduce mission costs, increase efficiency for communications between ground control and the vehicle, and enable independent operation of the vehicle during times of communications blackout. For rovers, functional autonomy addresses navigation, target identification, and science package manipulation. For spacecraft, functional autonomy has focused on automated guidance, navigation, and control. These include target body characterization and orbit determination, maneuver planning and execution, precise pointing of instruments, landmark recognition and hazard detection during landing, and formation flying.²⁷ The capabilities that have been addressed in research for and applications of spacecraft autonomy include the following:

- intelligent task planning, scheduling, and resources management with limited available resources and time constraints for high-level mission goals;
- intelligent task-level execution including software fault tolerance, efficient control and control performance monitoring, fault reconfiguration control, and supervisory control over the coordination of many spacecraft activities;
- model-based fault detection, isolation and recovery with model based reasoning techniques used for automatic fault protection and immediate request for ground intervention; and
- onboard data processing using knowledge discovery methods to prioritize data for ground connection.

Autonomy for rovers has progressed over the last decade with prominent examples from efforts to explore the surface of Mars. The Mars Pathfinder rover, Sojourner, explored the Martian terrain beginning in July 1997.²⁸ The Sojourner had very limited autonomy to enable navigation and provide for resource management and contingency response. Because it only provided supervised autonomy, repetitive ground monitoring was required. In January 2004, the Spirit and Opportunity, twin Mars Exploration Rovers (MER), began a surface exploration mission that has continued through 2011. These rovers employ expanded autonomy over what was feasible for Sojourner and provide model-based recovery, resource management, and autonomous planning capabilities in addition to autonomous obstacle detection and navigation. The integration software architecture used to facilitate MER autonomy is the “Coupled Layer Architecture for Robotic Autonomy” (CLARAty).²⁹ CLARAty provides a dual layer architecture consisting of a decision layer for artificial intelligence (AI) software and a functional layer for controls implementations. Implicit granularity in each layer allows for a functional hierarchy with nested capabilities. The functional layer provides the interface to the rover hardware while the decision layer manages high level goals by breaking them down into smaller objectives, scheduling them according to known constraints and the current rover state, and directing the functional layer to execute the objectives.

Spacecraft autonomy has been demonstrated with the Deep Space 1 mission. Deep Space 1 was launched in October 1998 as a test platform to validate high-risk advanced technologies in space.³⁰ In addition to demonstrating autonomous navigation of the spacecraft, a principal experiment involved demonstration of an AI system for on-board planning and execution of spacecraft activities. The remote agent (RA) architecture used for this mission includes a mission manager with a planning and scheduling engine, an executive module, and a mode identification and recovery (MIR) module. The mission manager develops a mission plan based on high-level goals to generate a set of time-based or event-based activities. The executive module executes the mission plan by generating a sequence of commands and then it monitors the spacecraft performance to ensure proper action. The MIR module assesses the spacecraft state and supports recovery from faults. During the Deep Space 1 mission, the RA was activated to control the spacecraft for a limited period. Testing of the RA capabilities involved an experiment that included the injection of four simulated faults. A software flaw in the executive module was detected and diagnosed so a second experiment was conducted to fulfill the remaining objectives of the test.

2.2.2 Characteristics and functionality

Autonomy extends the scope of primary control functions. Such capabilities can consist of automated control during all operating modes, process performance optimization (e.g., self-tuning), continuous monitoring and diagnosis of performance indicators as well as trends for operational and safety-related parameters, diagnosis of component health, flexible control to address both anticipated and unanticipated events and to provide protection of life limited components (such as batteries and actuators), adaptation to changing or degrading conditions, and validation and maintenance of control system performance. Thus, functionalities that enable monitoring, trending, detecting, diagnosing, deciding, and self-adjusting are relevant within the autonomous control context.

Key characteristics of autonomy include intelligence, resilience, optimization, flexibility, and adaptability. Intelligence facilitates minimal or no reliance on human intervention and can accommodate an integrated, whole system approach to control. It implies embedded decision-making and management/planning authority. Intelligence in control provides for anticipatory action based on system knowledge and event prediction. To support control and decision, real-time diagnostic/prognostic capabilities are important for state identification and health/condition monitoring. Additionally, self-validation is an aspect of intelligence that addresses data, command, and system performance assessment and response.

In addition to providing an environmentally rugged implementation, resilience is addressed by accounting for design uncertainties and unmodeled dynamics. Fault management is an important consideration in achieving resilience. Fault management involves fault avoidance, fault removal, fault tolerance, and fault forecasting. Fault avoidance can be accomplished through approaches such as the use of formal methods for software design, the application of an object-oriented paradigm for the software architecture, and software module reuse. Fault removal can be promoted through formal inspections of software, data flow testing, and fault injection testing (e.g., either state-based or code-based). Fault tolerance can involve redundancy, design diversity, high-reliability implementation or error detection and recovery functionality. Fault forecasting techniques include reliability modeling, data collection and data-driven modeling, operational profiling, and rare event prediction. Finally, resilience can also involve self-maintenance or self-healing. This capability is promoted through means such as captured design knowledge and self-correcting features, prognostics to identify incipient failure, and fault detection and isolation.

Optimization implies rapid response to demands, minimal deviation from target conditions, and efficient actuator actions. Optimized control can be facilitated by self-tuning and other forms of adaptation. Flexibility and adaptability are enabled by diverse measurements, multiple communication options, and alternate control solutions. Functional reconfigurability facilitates the effective use of these systems options while an inherent redesign capability permits adaptation to unanticipated conditions.

Autonomous control functionality can be decomposed into several elements. These include data acquisition, actuator activation, validation, arbitration, control, limitation, checking, monitoring, commanding, prediction, communication, fault management, and configuration management. The validation functionality can address signals, commands, and system performance. The arbitration functionality can address redundant inputs or outputs, commands from redundant or diverse controllers, and status indicators from various monitoring and diagnostic modules. The control functionality includes direct system/component control and supervisory control of the plant control system itself. The limitation functionality involves maintaining plant conditions within an acceptable boundary and inhibiting control system actions. The checking functionality can address computational results, input and output consistency, and plant/system response. The monitoring functionality includes status, response, and condition or health of the control system, components, and plant and it provides diagnostic and prognostic information. The commanding functionality is directed toward configuration and action of individual controllers and diagnostic modules. The prediction functionality can address identification of plant/system

state, expected response to prospective actions, remaining useful life of components, and incipient operational events or failures. The communication functionality involves control and measurement signals to and from the field devices, information and commands within the control system, and status and demands between the control system and a supervising authority (e.g., plant operators). The fault management and configuration management functionalities are interrelated and depend on two principal design characteristics. These are the ability of the designer to anticipate a full range of faults and the degree of autonomy enabled by the control system design.

The characteristics and functionality discussed above represent the possibilities of autonomy but they do not constitute a necessary set. Therefore, autonomous control can be viewed as providing a spectrum of capabilities with automated control representing the lowest extreme or baseline of the continuum. The incorporation of increasing intelligence and fault tolerance moves the control capabilities further along the spectrum. The higher degrees of autonomy are characterized by greater fault management, more embedded planning and goal setting, and even self-healing. The realization of full autonomy involves learning, evolving, and strategizing independent of human interaction or supervision.

2.2.3 Functional architectures

In most cases involving development and application of autonomous control, the principal functional architecture utilized some form of hierarchical framework with varying distributions of intelligence. A three level hierarchy is typical for robotic applications.^{14,31,32} Figure Fig. 12 illustrates the allocation of function within this hierarchy. The general concept of the hierarchy is that commands are issued by higher levels to lower levels and response data flows from lower levels to higher levels in the multi-tiered framework. Intelligence increases with increasing level within the hierarchy. Each of the three interacting tiers has a principle role. Basically the functional layer provides direct control, the executive layer provides sequencing of action, and the planner layer provides deliberative planning.

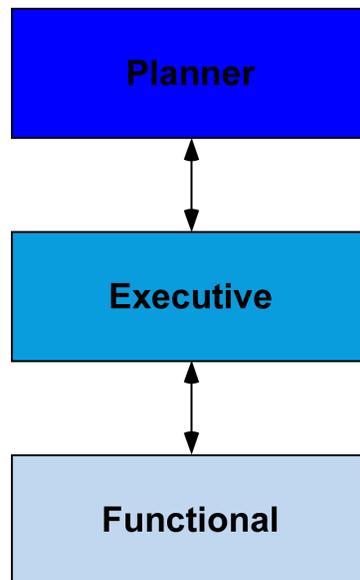


Fig. 12. Typical three-level autonomous control architecture.

The purpose of the functional level is execution of control. It is essentially comprised of algorithms in software and hardware. At this level, conventional control loops are implemented in which the control actions are generated based on specified control algorithms and communicated to plant/system actuators for execution. The functional level is also responsible for data acquisition using the plant/system sensors.

Before using the signals in its own control algorithms, the functional level typically processes the measurements through some signal validation algorithms. The signal validation results are also communicated to the higher architectural levels. At the functional level, model adaptive control is frequently used and monitoring and diagnostic capabilities, such as failure detection and isolation algorithms, state estimators, and parameter identifiers.

The purpose of the executive level is to provide coordination of plant/system control and to supervise the execution of that control at the functional level. The executive level contains decision-making and learning capabilities as well as some control algorithms. The executive level receives commands from planner level that schedule predetermined activities. These high-level commands are translated into sequences of control actions that are communicated to the functional level for execution. At the executive level, a supervisory function can assess the performance of the lower level controllers and the state of the plant/system to determine what models are to be used, how to tune parameters for control, and when to switch the control laws and perform parameter adaptation. A control coordination function at the executive level can deal with detected failures and anticipated events by issuing commands adhering to pre-defined procedures.

The purpose of the planner level is to provide management and organization of the overall plant/system control. The planner level consists of planning, decision-making, and learning capabilities. At this level, system goals are determined, the communication interface to operators is provided, and direction for the lower levels of the hierarchy is provided. The planner level performs high level performance monitoring, plant/system health evaluation, capability assessments, and task planning.

As previously described, an autonomous control architecture for spacecraft was developed and tested as part of the Deep Space 1 mission. The RA architecture³³ is illustrated in Fig. 13. In this representation, the mission manager (MM) and planner/scheduler (P/S) are shown as separate elements. Their coupled functionality results because the MM maintains the mission profile that guides the planning for the mission lifetime. The P/S develops flexible concurrent temporal plans for a time horizon (typically two weeks) based on goals from the mission profile supplied by the MM. The plans are provided to the smart executive (EXEC), which is a control manager that executes the sequence of activities and reacts to failed responses. It is responsible for coordinating resource management, action definition, fault recovery, and configuration management. The MIR component is a model-based module that monitors the condition of the spacecraft, identifies failures, and provides recovery procedures to the EXEC. On request from the EXEC, the MM and P/S will develop a revised plan to account for failures or recoveries. Through its multi-module approach, the RA is able to provide a reactive response to failures (EXEC) and a deliberative response to events (P/S). The reactive response provides real-time action to address the immediate consequences of failures. The deliberative response (i.e., replanning) provides the capability to assess the impact of failures or events on the mission goals and then determine how to proceed with the mission while accommodating those conditions.

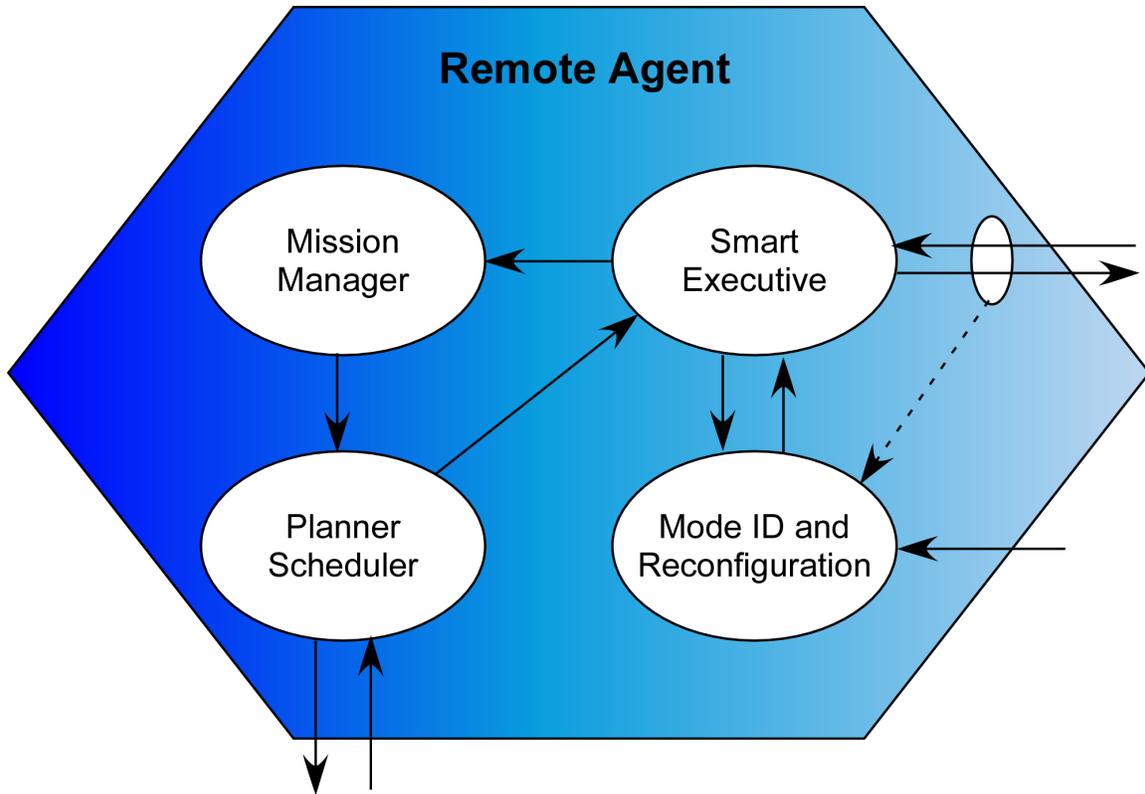


Fig. 13. Remote Agent architecture for Deep Space 1.

The Mars Technology Program has funded development of an autonomous control architecture to support the MER mission. As noted above, the CLARATy software environment supports autonomy for Spirit and Opportunity. The dual layer architecture of CLARATy is illustrated in Fig. 14, which was derived from a paper by Volpe on developments for the Mars Mobile Science Laboratory.³⁴ The CLARATy architecture provides an upper (decision) layer for AI software and a lower (functional) layer for controls implementations. The development of CLARATy addresses perceived issues with the three-tiered architecture,²⁹ which is typical of robotic autonomy. Those issues are the tendency toward a dominant level that depends on the expertise of the developer, the lack of access from the deliberative or planner level to the control or functional level, and the difficulty in representing the internal hierarchy of each level (e.g., nested subsystems, tress of logic, and multiple time lines and planning horizons) using this representation. In one sense, the CLARATy architecture collapses the planner and executive levels, which are characterized by high levels of intelligence, into the decision layer. Essentially, the deliberative and procedural functionalities are merged into an architectural layer that parallels the functional layer and provides a common database to support decision-making. Additionally, a system granularity dimension is maintained to explicitly represent the system hierarchies of the functional layer and the multiple planning horizons of the decision layer.

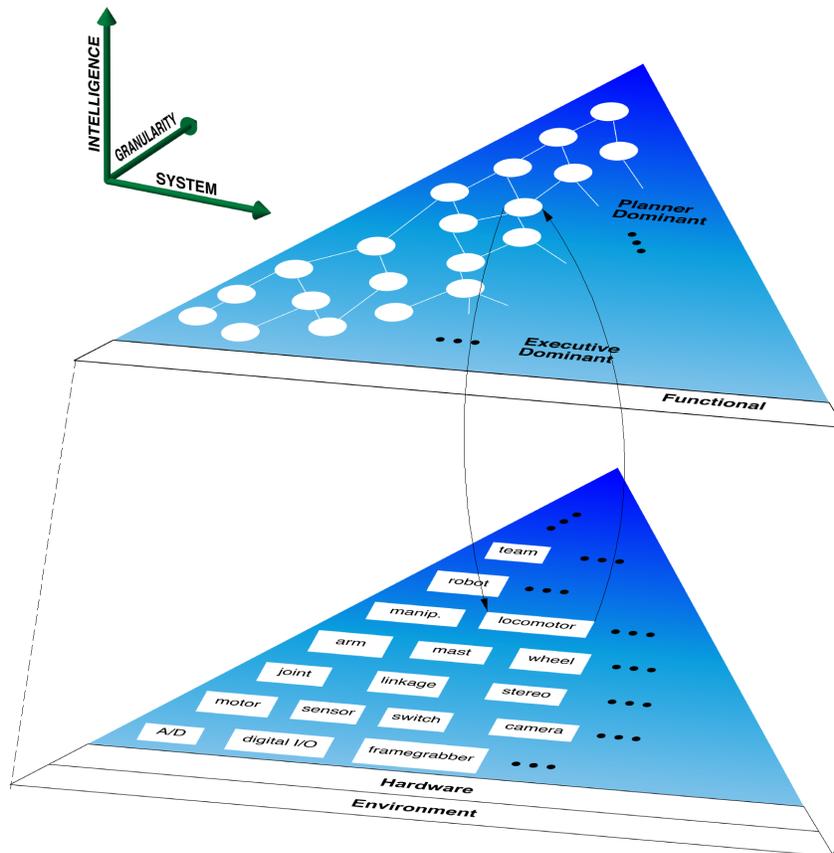


Fig. 14. CLARAty architecture with decision and functional layers.

The functional layer is an object-oriented hierarchy that provides access to the capabilities of the plant/system hardware and serves as the interface for the decision layer to the subject (robot, spacecraft, plant) under control. The interaction between the two layers depends on the relative granularity of each layer at the interface. At lower (i.e., fine) granularity, the decision layer has almost direct access to the basic capabilities of the plant/system. At higher (i.e., coarse) granularity, the decision layer provides high level commands that are broken down and executed by the intelligent control capability of the functional layer. The decision layer provides functionality to break down goals into objectives, establish a sequential task ordering based on the plant/system state and known constraints, and assess the capability of the functional layer to implement those commands. At lower granularity within the decision layer, executive functions such as procedure enforcement are dominant while, at higher granularity, planning functions such as goal determination and strategy development are dominant.

3. AUTOMATION OF NUCLEAR POWER PLANT OPERATIONS

This chapter presents an overview of approaches to automation that have been developed for and applied to nuclear power plant operation. In addition, concepts of operation for existing HTGRs and recent VHTR designs are described. The goal is to provide a general context for the state of the practice in automation in the nuclear power industry to establish the basis for considering the extent to which automation may be applied to VHTRs.

3.1 Plant Control

In the nuclear power industry, single-input, single-output (SISO) classical control has been the primary means of automating individual control loops. The use of multivariate control, such as three element controllers for U-tube steam generators of pressurized-water reactors (PWRs), has been employed in some cases. In very limited instances, efforts have been made to coordinate the action of individual control loops based on an overall control goal. Beginning in the mid-1980s, more integration of control loops as part of distributed control systems was accomplished, such as through digital feedwater control system demonstration projects sponsored by the Electric Power Research Institute (EPRI).^{35,36} Current modernization projects at existing reactors have primarily involved upgrades of individual control systems rather than an attempt to transition to an integrated control system approach on a plant-wide basis. The more extensive use of digital technology in the control systems defined for advanced light-water reactor (ALWR) designs enables I&C architectures with integrated information access and greater automation support. However, the ALWRs have adopted architectural approaches and implementation philosophies that are fundamentally the same as for operating plants, building on the experience gained over the years.

The application of most advanced techniques to nuclear power control issues has primarily been through simulation as part of research by universities and national laboratories. Some of the techniques employed in controls application research for both power and research reactors include adaptive robust control for the Experimental Breeder Reactor II (EBR-II), fuzzy logic control for power transitions, H-infinity control and genetic algorithm-based control for steam generators, neural network control for power distribution in a reactor core, and supervisory control for multi-modular reactors. A useful compendium of findings from such research activities is found in the proceedings of a series of Topical Meetings on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies sponsored by the American Nuclear Society.³⁷⁻⁴³

3.1.1 Integrated control systems

As noted above, automatic control systems for most existing nuclear power plants consist of individual control loops employing classical feedback control methods. Current control systems marketed for the nuclear power industry are based on computers or programmable logic controllers (PLCs). Most of these systems provide control application software containing basic control blocks that can be graphically configured into a control algorithm. These systems offer classical control modules as well as model-based control options. The control systems for ALWRs take advantage of these capabilities to enable more extensive use of integrated control features, such as incorporating feedforward action with normal feedback control to provide faster automated response and facilitate control loop coordination. Plant-wide integrated control allows for a greater range of operational automation that can reduce the demands for immediate active engagement of operators in routine procedures.

A primary example of the implementation of control system integration is the Integrated Control System (ICS) for nuclear power plants of the Babcock and Wilcox (B&W) design. The ICS is an analog control system based on the integrated control approach developed for B&W fossil-fired boilers. The integrated

control strategy utilizes a common feedforward power set point to coordinate boiler and turbine control. At the time it was introduced, the B&W nuclear ICS scheme was more advanced than other nuclear controls in the sense that it was a multivariate control system with scheduled feedforward action whereas other nuclear plants were operated using isolated SISO feedback control loops that offered considerably less automation of power maneuvers. The ICS was designed to take advantage of the capability of the B&W nuclear steam supply system's once-through steam generators to maneuver rapidly in response to load demand.

In the mid-1990s, the B&W Owner's Group developed a digital replacement to the analog ICS.⁴⁴ The Plant Control System (PCS) was designed to coordinate control of the reactor, feedwater system, and steam system. The PCS design contains many advanced features to add expanded capability over the analog ICS. For example, it includes digital switching logic to reconfigure the control system to match the plant as valves are sequenced and pumps are started. In addition, automation provided by the PCS design more fully addresses transitions among operating modes to avoid the need for manual actions that had been found to be a frequent source of plant trips.

Features of the PCS include:

- full automatic control from 1% to 100% of full power;
- prioritized control of system parameters to maintain control of the most important parameters despite saturation of some actuators or manual control switching for some actuators;
- automatic loading and unloading of the main turbine and the turbine-driven feedwater pumps;
- elimination of windup problems in the integral functions of the controller to provide bumpless transfer between automatic and manual control and to improve controller performance; and
- improved transitions between control modes.

Like the ICS, the PCS control strategy is based on the feedforward-feedback approach. The feedforward input is a centrally-generated core thermal power demand. Proportional and integral feedback actions add stability. The feedforward term places the demand for each constitute control loop at approximately the correct value for a given power level. The proportional and integral error terms correct any errors in the feedforward demand and compensate for normal drift and disturbances. The feedback terms are multivariate. That is, several values are summed to create the feedback contribution. Deadbands on all but one primary variable cause the controller to simplify down to an SISO formulation when the plant is near steady state. The SISO loops that exist near steady state can be thought of as the primary error control responsibility of each subsystem. The additional terms are secondary errors that enable faster or stronger control reaction for rapid transients. The secondary errors improve the capability for rapid response while leaving the stability characteristics and approach to steady state as the main responsibility of the primary control loop.

An overview of the PCS control algorithm is shown in Fig. 15. The top-level box is the core thermal power demand (CTPD) calculator. This module computes the allowable ramp rates and applies event-based power limits (for example, the CTPD would limit the maximum power demand if one reactor coolant pump were tripped). The integrated master is the control manager that directs the feedback errors determined from plant measurements to the actuators that provide the needed control action to reverse the error. The integrated master implements the control priority strategy. Logical switching based on plant mode and status is primarily implemented at this level. The other control boxes represent individual system controllers. These controllers sum and integrate the feedback and feedforward control signals passed to them by the integrated master.

The hardware architecture developed for the PCS was based on an implementation using triple-modular-redundant (TMR) microprocessor-based controllers. The goal was to achieve very high reliability by ensuring that the control system would remain fully functional given the failure of any single component.

The selected architecture was implemented as a composite system consisting of three identical channels of Foxboro (now Invensys) Intelligent Automation™ (I/A) modules, each of which computed the control algorithm, and a Triconex (now Invensys) TRICON™ module to perform system voting based on median select. A full prototype of the PCS was tested using a whole-plant simulator so that all aspects of operation could be functionally validated.

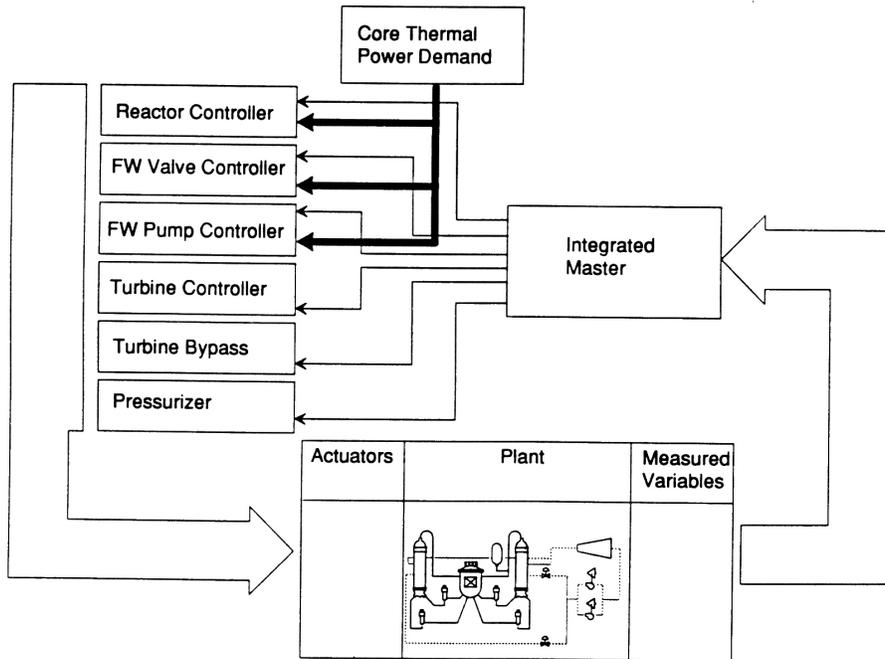


Fig. 15. PCS integrated control design.

Because of cost considerations, the PCS was never installed at a power plant. However, the PCS became the basis for modernization of the ICS at Duke Power’s three-unit Oconee Nuclear Power Plant in South Carolina.⁴⁵ In the late 1990s, Duke Power installed a digital replacement of the ICS using the AREVA (formerly Babcock and Wilcox) Control STAR™ modules. This control system was an updated digital implementation of the ICS algorithm with many of the corrections and improvements from the PCS added. Rather, than adopting the TMR architecture, the digital ICS architecture is simplex for most control functions but with fault tolerance (i.e., self testing). The exceptions to simplex operation are the reactor and feedwater controls, which are implement using dual channels. Reactor control is based on dual coincident logic for control rod movement and feedwater control is based on average controller output with predefined bounds. Experience with the digital upgrade has shown that automated operation over the full power range is very reliable and the capability to automatically control low power operations has proven to be particularly effective in reducing operator burden and eliminating unnecessary plant trips.

3.1.2 Supervisory control systems

In most large-scale systems, there exist many processes that must coordinate to achieve system-wide performance. Supervisory control provides management or coordinated control of many individual controllers or control loops. Within the nuclear power industry, supervisory control systems are generally implemented with coupling for a limited number of control loops. A common function of supervisory control systems is to provide parameter and set point modification specific to known operating conditions.

Interlocking logic for control system actions is also a common practice for regimenting controlled responses to achieve defined states.

Hierarchical supervisory control, whose purpose is to achieve total plant coordination, permits individual process control by local controllers while exercising top-down coordination across multiple process controllers. The coordination achieves an optimization of materials and energy flow by adjusting local controller set points and other parameters. Coordination also involves switching of controller operational modes (e.g., for different output demands, to transition among multiple product streams, or to support maintenance cycles). Automated start up and shutdown, as well as system-wide diagnostics, are possible with supervisory control.

As part of research to support advanced multi-modular nuclear reactor concepts, such as the International Reactor Innovative and Secure (IRIS) and the advanced liquid metal reactor (ALMR), supervisory control methods for operational management of multiple units were developed and demonstrated through plant simulation.^{46,47,48} The IRIS approach involves a multi-modular plant with multiple individual or paired units forming power blocks. The ALMR plant design involved three power blocks, with each block consisting of three reactor systems coupled to a common energy conversion system (i.e., balance of plant). The programmatic goal for the ALMR was for the overall supervisory control system to enable operation of the plant with as few as one operator per power block.

To address the highly complex plant management and reactor system control issues associated with multi-unit control, a hierarchical supervisory control system was developed. For the ALMR supervisory control application, the reallocation of power demand among units within a power block was accomplished using heuristic rules and was demonstrated under transient and degraded conditions. Additionally, various foundational methods, such as adaptive and nonlinear control, control mode selection among algorithms, command and signal validation, and on-line state identification, were demonstrated using more detailed plant simulation models.

The supervisory control approach developed for multi-modular plants provides the framework for highly automated control while supporting a high-level interface with operations staff, who can act as plant supervisors. The final authority for decisions and goal setting remains with the human but the control system assumes expanded responsibilities for normal control action, abnormal event response, and system fault tolerance. The supervisory control framework allows integration of controllers and diagnostics at the subsystem level with command and decision modules at higher levels.

The supervisory control system architecture shown in Fig. 16 is hierarchical and recursive. Each node in the hierarchy (except for the terminal nodes at the base) is a supervisory module. The supervisory control modules at each level respond to goals and directions set by modules above it within the hierarchy and to data and information presented from modules below it within the hierarchy. Each module makes decisions appropriate for its level in the hierarchy and passes the decision results and necessary supporting information to the functionally-connected modules.

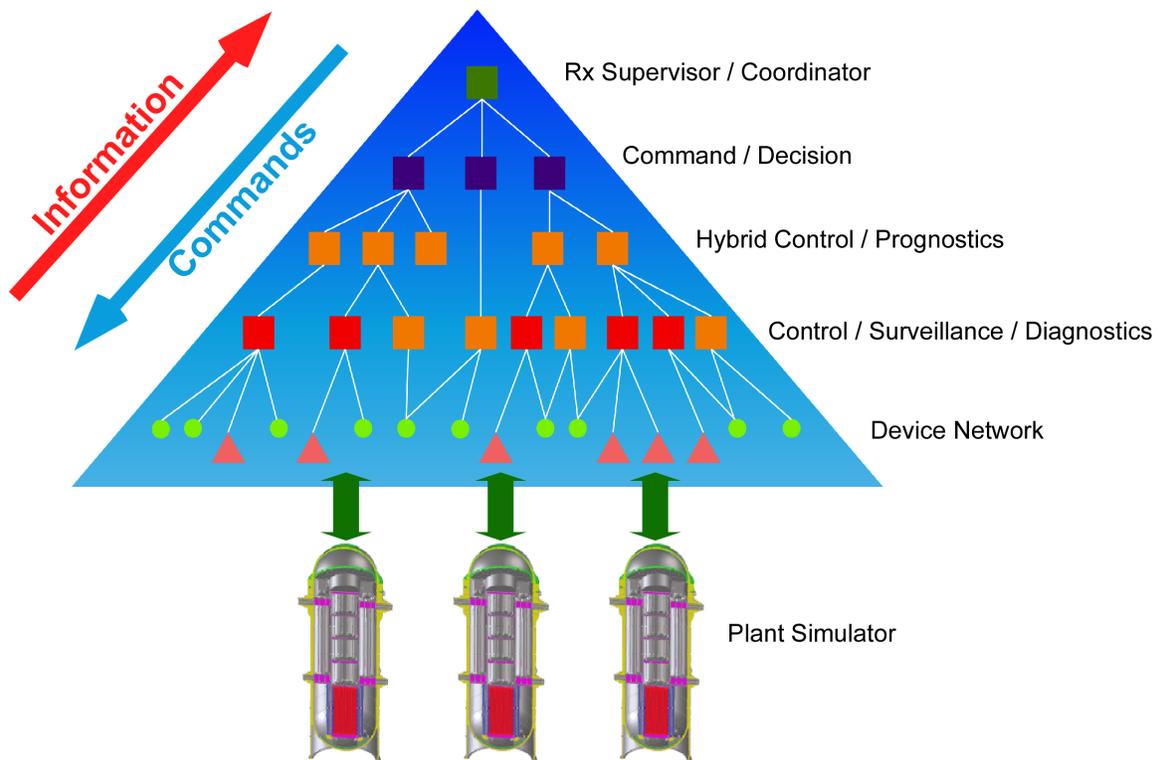


Fig. 16. Supervisory control architecture for multi-modular nuclear power plants.

The device network level consists of sensors, actuators, and communications links. The next highest level consists of control, surveillance, and diagnostic modules. The coupling of the control modules with the lower-level nodes is equivalent to a conventional automated control system composed of controllers and field devices. The surveillance and diagnostic modules provide derived data to support condition determination and monitoring for components and process systems. The hybrid control level provides command and signal validation capabilities and supports prognosis of incipient failure or emerging component degradation. At this level, fault identification occurs. The command level provides algorithms to permit reconfiguration or adaptation of the control system to accommodate detected or predicted plant conditions. At this level, active fault tolerance is accomplished. For example, if immediate sensor failure is detected by the diagnostic modules and the corresponding control algorithm gives evidence of deviation based on command validation against pre-established diverse control algorithms, then the command module may direct that an alternate controller, which is not dependent on the affected measurement variable, be selected as principal controller. The actions taken at these lower levels can be constrained to predetermined configuration options implemented as part of the design. In addition, the capability to inhibit or reverse automated control actions based on operator commands can be provided. The highest level of the supervisory control architecture provides the link to the operational staff.

The functionality that is embodied in the hierarchy can be decomposed into several elements. These include data acquisition, actuator activation, validation, arbitration, control, limitation, checking, monitoring, commanding, prediction, communication, fault management, and configuration management. The validation functionality can address signals, commands, and system performance. The arbitration functionality can address redundant inputs or outputs, commands from redundant or diverse controllers, and status indicators from various monitoring and diagnostic modules. The control functionality includes direct plant or system control and supervisory management of the control system itself. The limitation functionality involves maintaining plant conditions within an acceptable boundary and inhibiting control

system actions. The checking functionality can address computational results, input and output consistency, and plant/system response. The monitoring functionality includes status, response, and condition or health of the control system, components, and plant and it provides diagnostic and prognostic information. The commanding functionality is directed toward configuration and action of lower level controllers and diagnostic modules. The prediction functionality can address identification of plant/system state, expected response to prospective actions, remaining useful life of components, and incipient operational events or failures. The communication functionality involves control and measurement signals to and from the field devices, information and commands within the control system, and status and demands between the supervisory control system and the operational supervisors (i.e., operations staff). The fault management and configuration management functionalities are interrelated and depend on two principal design characteristics. These are the ability of the designer to anticipate a full range of faults and the degree of automation enabled by the control system design.

3.2 Plant Limitation

The concept of a staggered defense in depth (i.e., echelons of defense) was developed at the outset for nuclear power plant I&C technology. This concept supports a range of operation extending from manual control to automatic control to reactor protection. A key driver in the evolution of this concept is the goal that immediate human action should not be necessary to maintain the nuclear power plant in a safe state and avoid potential radiological release. At one end of the control and protection spectrum is the human operator, who can manually control the state of the plant. At the other end of the spectrum is the protection system, which automatically and dramatically brings the plant into a safe state when conditions indicate an abnormal or accident state is being approached. In between these two extremes is the automated control portion of the I&C architecture.

Initial I&C system implementations at nuclear power plants provided independent systems dedicated to strictly separate protection and regulating control functions. However, aspects of the control system were expanded in later designs to include detection of and response to operational transients that are precursors to plant trip conditions. These expanded capabilities provide limitation functions that detect and minimize incidents in their incipient stages through less severe actions than a reactor scram. Most current light-water reactors (LWRs) include some modest limitation functions and control interlocks as elements of the automated control system. These functions include local core protection and integral reactor power limitation (e.g., power runbacks and rod withdrawal interlocks). In most cases, these functions are embedded in the control system and are treated as normal control capabilities. Effectively, these functions enable trip avoidance to promote availability or provide mechanisms to ensure investment protection.

German nuclear power plants demonstrate the most extensive and formalized use of limitation functions within the defense-in-depth hierarchy of nuclear power plant I&C architectures.⁴⁹ The German regulatory authorities require that the plant must be designed so that the operators do not have to intervene for 30 minutes in the sequences of events that occur during major operational incidents. Additionally, the plant must be capable of remaining autonomous (i.e., “hands off”) for 10 hours, even in case of massive external influences such as an airplane crash, earthquake, or sabotage. As a result, a “multi-barrier” approach to the plant I&C architecture was developed that involves staggered levels of control, limitation, and protection. In practice, a separate limitation system was devised that intervenes earlier and in a more differentiated manner than the reactor protection system (RPS) but that also permits continued operation through many events. Thus, the reactor limitation system (RLS) is an integral element of the safety-related I&C systems in German nuclear power plants and contributes to a staggered defense in depth with progressively corrective actions and multiple sequential and/or parallel measures.

Limitation systems in Germany were originally developed as limit control systems for PWRs and employed quadruple redundancy with no special qualification. The first implementation was at the Stade nuclear power plant in the early 1970s. As the benefits of the limitation approach were demonstrated

throughout the decade in the Biblis-type PWRs, the approach was accepted within German safety rules and limitation systems became qualified as parts of the overall plant protection architecture. Subsequently, all modern German nuclear power plants of the Grafenrheinfeld-type included the RLS as an element of the safety-related I&C architecture. In recent years, a digital version of the RLS, implemented using the AREVA (formerly Siemens) TELEPERM XS™ safety qualified platform, has been installed through I&C upgrades at the Unterweser and Neckarwestheim nuclear power plants.

3.2.1 Limitation philosophy

The limitation philosophy employed in German PWR I&C systems is based on the understanding that preventing damage is just as important as managing or reducing damage. Essentially, the German approach is to enable protection of the components and systems of the plant upon occurrence of potential incidents rather than to rely upon action by the operator or RPS. As a result of this staggered defense-in-depth scheme, it is more likely that the resistance of the plant to future incidents will be maintained.

For German PWRs, the plant I&C architecture consists of a hierarchy of systems that provide progressive levels of protection. The automatic control system provides the first level of protection by maintaining the reactor within operational limits for effective power generation. These operational limits are kept sufficiently below plant safety limits to ensure safety during normal power demand variations or anticipated operational disturbances. The reactor trip system and the engineered safety feature actuation systems provide the final level of protection. These systems, which are considered part of the RPS in Germany, are designed to shut the reactor down, keep it shut down, and ensure adequate core and system cooling if plant parameters exceed plant safety limits. In German PWRs, an intermediate level of protection between the control and protection systems is provided by a distinct limitation system. The basic responsibility of the RLS is to monitor the plant state and act to prevent operation outside the “safety envelope” (i.e., the set of parameter safety margins) that would trigger RPS action.

The goal of the RLS is to prevent transients from resulting in scrams or trips through early, responsive, rapid and forceful but, if possible, reversible countermeasures. The RLS achieves its protective purpose by identification of a deviation from normal conditions and by initiation of specific actions necessary to limit and smooth the transient. The built-in capability for diagnosis enables the RLS to detect the transients it is designed to address during their incipient stages. In response to violations of the limitation envelope, the RLS intercedes and drives the plant back towards normal operating conditions. When the disturbance has been eliminated and the plant returns to its acceptable operating range, plant control is returned to the normal control system without interruption.

In the German implementations, the RLS is a multiply-redundant system with an optimal balance between functionality and reliability. The RLS is typically quadruple redundant with generally no internal functional diversity. Like protection systems, the RLS cannot be manually overridden. When actuated, the RLS works like a symptom-oriented control system, providing control reversal in a feedback mode. When not actuated, RLS status is analogous to that of protection systems. In effect, the RLS is ready to operate with settings slightly outside the normal operating envelope.

3.2.2 Limitation functions

The foundational application of limitation functions in German PWRs was through the use of limit control systems, for which the actuation limits are set outside a dead band around the normal operational regime plus a margin for overshoot of the controlled variable. The approach to limitation evolved to include two types of limitation functions: protection limitation and condition limitation. Protection limitation functions protect against anticipated operational occurrences (AOOs) whose consequences may still be acceptable in the event of limitation malfunction. Clearly, the more severe AOOs that would unquestionably lead to accident conditions are addressed by the RPS. Condition limitation functions are designed to ensure that, at any time, the initial conditions assumed in the plant safety analysis are

maintained. Limitation actions include dropping an individual rod (or pairs or groups of rods) for a rapid, controlled power runback and separating coolant systems by stopping the relevant pump and, additionally, closing the associated valve.

The principle power limitation functions include limitation of integral reactor power, limitation of local power density in the upper and lower segments of the core, and balancing of reactor and generator powers by quick adjustment of the reactor power. Other limitation functions that are related to reactor power involve limitation of the average coolant temperature, control of local departure from nucleate boiling ratio (DNBR) by power density limitation derived from in-core detector signals, and limitation of control rod/bank movement to ensure adequate shutdown margin. Additional limitation functions focused on the coolant system are limitation of reactor coolant system inventory changes during normal operation, limitation of coolant temperature gradients, and limitation of coolant pressure fluctuations.

3.2.3 Reactor limitation system architecture

In Germany, the I&C system encompasses all equipment and systems used for sensing, signal transmission and conversion, indication generation, computing, data storage and actuation for the functions of protection, limitation, normal (feedback) control, sequence control, monitoring, surveillance, display, modeling and the relevant power supplies. The main I&C systems are the RPS, RLS, and reactor control system (RCS).

The purpose of the RPS is to ensure that safe shutdown is achieved and maintained for any event that challenges the safety envelope (i.e., safety limits) of the plant. Its function is to detect incidents and initiate protective action, such as reactor trip, emergency cooling, and residual heat removal. The RPS provides simplified, fixed, uninterruptible, irreversible, highly reliable protective actions. Its design requirements are intended to achieve maximum availability, testability, and simplicity of design. German regulatory requirements also demand that at least two diverse initiation channels in the RPS must detect key design basis events to address the potential for common mode failure.

The purpose of the RLS is to enable the avoidance or, at least, the favorable influence of operational incidents (e.g., transients) and to thereby minimize their impact on the plant. Its function is to smooth transients and avoid reactor trips through early detection of plant events or equipment failures and subsequent corrective response such as enforced limits on reactor power or other plant process variables. The RLS provides flexible, limiting, reversible, early, sensitive and reliable protective actions. Its characteristics are high availability, redundancy, diagnosability, and graduated corrective measures.

The purpose of the RCS is to permit optimized control for start up, power maneuvering, steady state power operation, and shut down. Its function is to provide sequence of event and feedback control for normal power operation and permit operator interaction for manual control. The RCS provides universal, optimized control actions that are typically determined without embedded protective constraints (i.e., the limitation function is incorporated in the RLS). It is characterized by high functionality and condition sensitivity, fast response, manual and automatic operation and reliability managed through maintenance and, in some cases, redundancy.

Figure Fig. 17 shows the typical I&C architecture for German nuclear power plants illustrated from the measurement instrumentation to the command actuators. At the top of the figure, the sensors are indicated, along with signal transmitters. The signal path for safety-related I&C systems includes isolation, amplification, preprocessing, and comparison (e.g., validation or plausibility). Below these elements are the processing modules that perform computational functions to accomplish the initiation, management, and termination of protective or control actions. These functions perform control algorithm calculations and set point comparisons and account for logical dependencies, data trends, and calculated values. At the bottom of the figure, the output signals of the processing modules are communicated to the actuators with the appropriate isolation and safety priority. These signals trigger the necessary actions for the control and protection of the plant. Also shown in the figure are the power supplies supporting the

sensor strings and the actuator power supplies to support both autonomous (i.e., automatic) control of the safety-related actuators (e.g., de-energized to drop rods) and operational control of the nonsafety-related actuators.

From left to right, the figure indicates the staggered defense-in-depth approach to plant control and protection that is employed in German PWRs. On the extreme left-hand side is the RPS, followed by the RLS, the reactor output control (ROC) element of the RCS (i.e., the safety-related reactor control system), the post-accident monitoring (PAM) incident instrumentation, and the plant process operational control (POC) element of the RCS (e.g., balance of plant control). The far right-hand side of the figure indicates the control room human machine interface segment of the I&C system.

The RPS is implemented as redundant asynchronous channels based on at least two-out-of-three logic (in some cases, quadruple redundancy is employed). As indicated in the figure, redundancy and diversity are employed to satisfy the regulatory requirements. Internal diversity is used to provide protection against common mode failures by means that include functional and/or equipment diversity. As an example of functional diversity, some system trip functions are assigned to mutually diverse processing chains within a channel, so that the different chains process the measurements on different variables. The processing chains may also incorporate diverse logic. This approach minimizes susceptibility to errors because the applications in the individual chains process different data and are thus, at least to some extent, structurally different. In final element of the RPS, logic gating for trip determination is accomplished using a dynamic (pulsed) magnetic core system to provide a higher degree of failure detection than is possible with static signals. Control rod drop is accomplished by de-energizing the rod coils via mechanical switches.

The RLS is implemented as synchronous quadruple-redundant channels based on two-out-of-four logic. This quad-redundancy is employed so that the minimum requirement of two-out-of-three logic is complemented by a hot testing and repair channel. The fourth channel contributes significantly to the overall reliability of the system. Internal diversity is not required for the RLS but the addition of the intermediate limitation functionality contributes to the overall I&C system diversity within the staggered defense-in-depth approach. The RLS combines the intelligent features of closed loop control systems with some degree of the higher reliability afforded in reactor protection systems. Since the consequences of failure for the RLS are less severe than that of the RPS, it is permitted reduced reliability requirements. This condition enables more complex functionality to be embodied in the RLS than is desirable in the RPS. Thus, greater intelligence in the form of more complex algorithms and embedded plant state identification diagnostics is incorporated in the RLS to detect incipient transients and invoke optimized countermeasures (e.g., slow or fast runbacks to specific power levels, power density limitations for local DNBR management). Redundant sensor inputs are provided to each RLS channel and the signal arbitration selects the second highest value in the safety relevant direction for processing. Measured or computed parameters are compared against set points or operational diagrams to determine the need for limitation action and the nature of the limitation (e.g., graded actions of increasing intensity). Finally, the limitation signals are processed through two-out-of-four voting (or two-out-of-three voting if one channel is out of service). Controlled rod insertion for fast runbacks is accomplished by de-energizing each gripper coil via electronic switches. This provides diversity compared to the rod drop mechanism of the RPS.

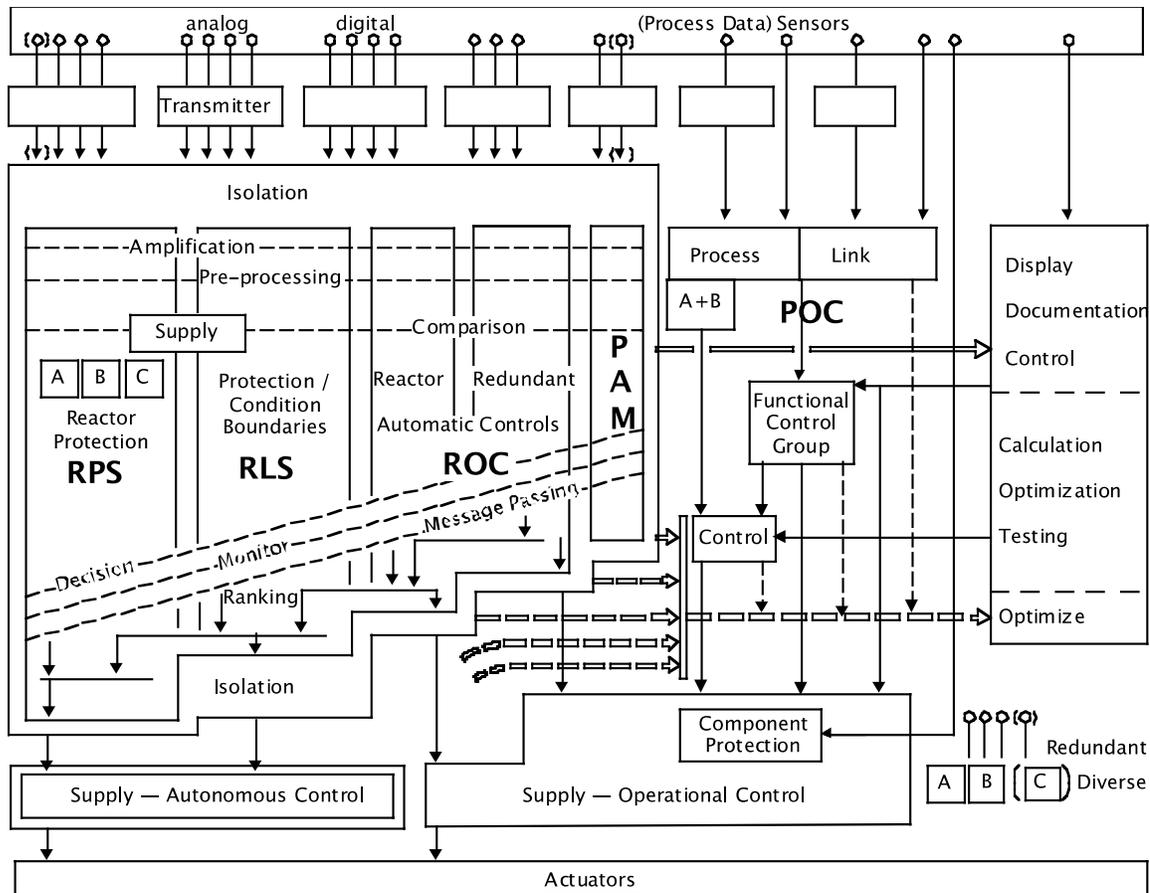


Fig. 17. I&C architecture for German PWRs (adapted from Ref. 50).

The RCS control function is performed by two effectively separate control systems, one for the generator and one for the reactor. Well-balanced collaboration between these systems for startup, power operations of all kinds and, if possible, for the most frequent disturbed situations is achieved partly by design and partly by the action of limitation functions. The ROC consists of those safety-related control functions whose failure can directly result in reduced power output or possibly even a reactor trip. The most significant control actions (e.g., rod control) are implemented on redundant controllers. The ROC is grouped within the safety-related “isolation island” with the RLS, PAM, and RPS. The POC provides automated functional groups or single controllers to drive nonsafety-related plant process systems.

3.3 Concepts of Operations

Modern nuclear power plants have moved toward greater automation but still rely of human interaction for supervision, system management, and operational decisions. More importantly, the human is also given the responsibility to serve as the last line of defense should I&C system failure prevent automatic plant protective measures from actuating, particularly in the case of prospective common cause failures that could disrupt multiple safety-related systems. The operational concepts include how the plant is operated under normal and abnormal conditions; including loss of equipment or displays and how the operators are expected to interface with each other, etc. This section discusses the scope encompassed within the concept of operations for a nuclear power plant and presents available examples of operational approaches developed for HTGRs.

3.3.1 Scope

While the human factors aspects of the concept of operations for VHTRs are beyond the scope of this investigation, it is appropriate to consider the full breadth of the subject. From this consideration, the potential impact of a high degree of automation on operational approaches is clarified. Of particular interest are I&C and operational aspects such as the modes of operation for the plant, the automation capabilities incorporated in HTGR control rooms, and the range of operational strategies support by highly automated control room designs.

The idea of a concept of operations is a fundamental component of systems engineering, especially for the design of any complex system.⁵¹ Concept of operations is a significant consideration in the NRC's review of the nuclear power plants.⁵² A top-down treatment of the concept of operations for a nuclear power plant addresses the high-level goals for system operations. From the bottom-up perspective, the concept of operations for the plant rests on the technological infrastructure needed to support the operational approach and human-system interaction. Concept of operations can be characterized in terms of five dimensions:⁵³

- Role of Personnel and Automation
- Staffing and Training
- Normal Operations Management
- Disturbance and Emergency Management
- Maintenance and Change Management

The Roles of Personnel and Automation dimension encompasses the relative roles and responsibilities of personnel and plant automation and their interrelationships. The allocation of function within a system and between the human and the system is central to achieving human system integration. Of particular significance beyond basic control loop automation is automation to support all human cognitive functions, including: monitoring, disturbance detection, situation assessment, response planning, and response execution.

The dimension of Staffing and Training involves approaches to staffing the plant, including operational staffing levels and personnel qualifications. Traditional functional staffing models do not reflect the optimization that can be achieved through highly automated, yet highly reliable control room design.

The dimension of Normal Operations Management reflects the approach to how the plant will be operated and considers the means by which personnel manage normal operational modes, such as startup, low power, full power, and shutdown. Specifically, this dimension addresses mechanisms and resources that personnel use to interact with plant functions, systems, and components in accomplishing their main tasks of monitoring and controlling the plant.

The Disturbance and Emergency Management dimension provides concepts for how degraded conditions, disturbances, and emergencies can be handled, and how responses to such situations are determined.

The Maintenance and Change Management dimension addresses methods for system maintenance, modernization installation, and configuration management.

3.3.2 HTGR operations

HTGR control schemes involve different modes and functions depending on the plant state. Most of the main control systems have four distinct control modes: offline, startup, normal operation and shutdown. The offline and normal operation modes are typically the continuous static states; startup/shutdown modes are transitional between normal operation and offline. In normal operation, the control systems regulate the process using feedback control. In modern plants and recent designs, automatic feedback regulation control is extensively used for the full range of normal power operation. The normal operation

mode encompasses both steady state and power maneuvering at rated ramp rates for power change. Additional submodes in normal operation may exist for low power, rapid runback, and special plant configurations (e.g., operation on turbine bypass versus normal turbine). Simple, automatic protection systems provide rapid event response to address accident conditions and ensure the plant achieves a safe state.

In the limited examples of HTGR control rooms, the experience base ranges from primarily manual operation to extensive automation of startup/shutdown and normal operation. Design concepts for VHTRs anticipate more comprehensive automation with the operator fulfilling the role of supervisor, possibly for multiple units. This section discusses the operational control approaches employed by existing plants or defined for proposed reactor designs. The discussion below constitutes a high level overview of operational approaches employed or proposed for HTGRs. The available information offers meager details about operator roles, interface mechanisms, or control room configurations. More detailed descriptions of the HTGRs and their I&C systems are provided by Wilson et al.⁵⁴

3.3.2.1 Fort St. Vrain nuclear power plant

The Fort St. Vrain nuclear power plant was the second commercial HTGR to be operated in the United States.^{55,56} The helium-cooled reactor, located in Colorado, began power operation in 1976 and ended operations in 1989. The reactor consisted of two helium primary loops with six parallel steam generators and two steam-driven helium recirculators in each loop. Heat was removed from the primary loops via the steam generators and was then conveyed to a conventional steam turbine for power conversion.

The Fort St. Vrain plant operated in fully automatic control mode from 25 to 100% of full power. The plant was designed for base load operation at a fixed power level but was also capable of following load changes. The automatic control system regulated the system to the operating point and responded to load changes and gradual changes in the plant. The control system was also designed to respond automatically to larger disturbances such as loss of feedwater, turbine-generator trip, and reactor scram. The plant started up under manual control by the operator. From 0 to 30%, individual systems were switched into automatic control mode as the plant reached the normal power range.

The control scheme for normal power operation was a turbine-following strategy in which load changes were introduced by changing the position of the turbine admission valves. The feedwater valve position, circulator speed, and reactor rod position were operated in feedforward plus feedback control scheme to respond to the load change promptly and then regulated the plant to the operating point. Feedwater flow was adjusted to control steam pressure. The feedwater flow controller also contained a fast runback mode that was initiated following most scrams. The helium circulators were used in a closed loop control to maintain main steam temperature at its set point. Reheat steam temperature was controlled by controlling reactor power via flux controllers. A flux controller operated one control rod drive for automatic power regulation. Only one pair of control rods was automatically controlled. Since one rod pair is insufficient for the 25 to 100% normal load swing, manual shimming of three symmetrically located rod drives was required occasionally. Helium temperature was not directly controlled but was uniquely determined by the other controlled variables. Alarms for abnormal values of plant parameters were provided. The control system allowed operators to intervene to take manual control to avoid initiation of protective functions of the safety system. An orifice control system in Fort St. Vrain positioned variable orifices in inlet coolant passages within the reactor to control the distribution of flow of helium coolant through each region of the core to compensate for variable power generation in each region. The orifice valves were manually controlled from the control room.

Fort St. Vrain did not employ a separate, dedicated shutdown cooling system or a passive reactor cavity cooling system for decay heat removal. Instead, the safe shutdown cooling system was a function or mode of operation of the same systems used for normal heat removal. Fort St. Vrain was a larger core and required forced helium circulation to be started within 60 minutes of depressurization from equilibrium

full power. Thus, the plant protection system (PPS) consisted of the I&C systems and functions required to initiate automatic corrective actions upon onset of an unsafe condition. The PPS functions included reactor scram, loop shutdown and steam/water dump, circulator trip, and rod withdrawal interlock. These actions, which took precedence over normal operational control, were directed toward reducing plant power and shutting down reactor plant equipment. The PPS achieved reliability through redundancy and coincidence and was designed to perform its function in the presence of any single failure and consequential effects. The system also used channel independence to guard against propagation of failure and common-cause failure vulnerability.

3.3.2.2 Arbeitsgemeinschaft versuchsreaktor–AVR

The Arbeitsgemeinschaft Versuchsreaktor (AVR) was an experimental reactor that operated from 1967 until 1988 at the Jülich Research Center in the Federal Republic of Germany.⁵⁷ The AVR's mission was to demonstrate the concepts and safety features of the pebble bed high temperature reactor design. The AVR was a complete power plant equipped with a turbine generator and was connected to the electrical grid in normal operation. The I&C architecture for the AVR was based on analog technology and its operation was primarily based on manual action by plant operators.

The AVR relied on the stability and thermal inertia of the heat transport processes to allow the operators to control the plant in manual (except turbine admission valve). The operational approach was for the operators to use the three manually manipulated variables (circulator speed, feedwater valve, and reactivity) to hold three measured variables (secondary heat balance power, steam temperature, and core outlet temperature) to desired values. Load change in the AVR was accomplished primarily by changing the helium circulator speed using a variable frequency generator. In effect, neutron power was controlled based on negative temperature feedback rather than direct reactivity insertion/withdrawal through rod motion. A given neutron power level could be achieved with a range of values of circulator speed and core outlet temperature. To set the core outlet temperature to an operating point, the operating scheme for the AVR involved a coarse adjustment of core reactivity via the fuel pebble charging and precision regulation by the positioning of the shutdown rods. Online refueling enabled long-term reactivity control to account for burnup and manage the total reactivity available in the fuel. Feedwater flow adjustments were used to control steam temperature. The operator would follow a feedwater flow change with manual circulator speed and rod position adjustments to maintain the other measured variables at their set points. The turbine was equipped with an automatic pressure regulator that used the turbine admission valves to control steam pressure to a set point. Thus, the turbine was operated in a reactor-following mode, in which the automatic pressure regulators respond to steam load.

Startup and shutdown operations were accomplished manually through sequential steps. Startup was accomplished manually through sequential steps in which the operator adjusted the rod position, feedwater flow, and helium circulator speed. Normal shutdown was based on negative temperature feedback following manual switching off of the helium circulators. The AVR did not use a separate active shutdown cooling system for decay heat removal. Following a normal shutdown, feedwater flow was maintained to the steam generator in water-cooling mode to provide core cooling. In the event of a failure of the secondary side cooling, passive cooling of the reactor by radiation and conduction through the vessel and containment walls was adequate to limit temperatures in the core and vessel to safe levels.

Automatic reactor shutdown is enforced on the AVR by two means, scram and rod drive run-in. The scram method is the faster method. The rod driving method is slower but places less stress on equipment. In most major accident scenarios, the AVR employed passive features and characteristics to achieve a safe shutdown. However, a water ingress accident required detection and an active response. Following identification of an event through moisture detection, the affected steam generator's tubes must be isolated, the core must be shutdown by rod insertion, and active cooling of the core must be provided to reduce temperatures to below the chemical reaction point.

3.3.2.3 High temperature engineering test reactor—HTTR

The Japanese high temperature engineering test reactor (HTTR) is a low power, helium gas-cooled and graphite-moderated test reactor.⁵⁸ The purposes of the HTTR are establishment of the HTGR and nuclear heat utilization technologies, development and analysis of innovative high temperature new technologies, and demonstration of safe HTGR operations and safety characteristics. The HTTR possesses separate automatic control and protection systems.

The reactor control system of the HTTR is designed to assure high stability and reasonably damped characteristics against the various disturbances during operation.⁵⁹ The system consists of the operational mode selector, reactor power control, and plant control systems. The mode switch selects several operational modes, such as rated power operation, high temperature test operation, safety demonstration test operation, irradiation test operation, etc. The reactor power control system consists of the power control and reactor outlet coolant temperature control devices. The signals from each channel of the power range monitoring instrumentation are fed to three microprocessor-based controllers. If there is a deviation, between the process and set points, a pair of control rods is signaled to insert or withdraw at variable speed, depending on the deviation. A control rod pattern interlock is used to prevent abnormal power distribution. The reactor outlet coolant temperature control system gives a demand to the power control system and changes the coolant outlet temperature by moving the control rods. The plant control system also encompasses the reactor inlet coolant temperature control system, intermediate heat exchanger primary coolant flow rate control system, primary pressurized water cooler primary coolant flow rate control system, primary helium pressure control system, primary-secondary helium differential pressure control system, primary pressurized water differential pressure control system, and pressurized water temperature control system.⁵⁹

The safety protection system consists of the reactor protection and engineered safety features actuating systems. It is designed with two-out-of-three circuit logic and two trains. The multiple channels are separated physically as reasonable achievable.

3.3.2.4 High temperature gas-cooled test reactor—HTR-10

The 10 MW(t) High Temperature Gas-Cooled Test Reactor (HTR-10) is a Chinese pebble bed reactor core with online refueling based on a German HTGR module design.^{60,61} The objective of the HTR-10 is to verify and demonstrate the technical and safety features of the modular HTGR and to establish an experimental base for developing nuclear process heat applications and the gas turbine cycle for electricity production. The HTR-10, in its initial configuration, provides co-generation of electricity using a once-through steam generator and conventional steam turbine as well as district heating with its rated 10 MW thermal power.

The HTR-10 control system is fully digital and provides for automated operation. Based on descriptions in the available literature,⁶¹ the control system provides distributed control using field stations employing redundant computer-based controllers and local control networks. The local control loops are interconnected through a higher-level supervisory network that interactions with the control room operator workstation. Local control and monitoring loops are identified as control rod drive system, in-core monitoring system, primary control system, auxiliary control system, and turbine generator control system.

The HTR-10 provides two operational test phases.⁶² The first phase has a steam turbine cycle for electricity generation, and maintains a capability for district heating. The second, higher-temperature phase has a combined cycle gas turbine and steam turbine for electricity generation.

The HTR-10 reactor protection system is a fully digital automatic protection system. The protective actions it provides include:

- drop of the reflector rods by gravity,
- shutdown of the primary circuit blower,
- isolation of the secondary system,
- isolation and draining of the steam generator,
- isolation of the primary system,
- dropping of the small absorbed balls by gravity,
- startup of the helium purification system, etc.

The reactor protection system performs different protective measures depending on the measured conditions. For example, when the protection system detects that the primary circuit humidity exceeds the limit value, the isolation of the secondary system will be implemented. The HTR-10 provides normal and backup shutdown systems. The normal system consists of control rods that are inserted into drilled holes in the reflector blocks. The backup system consists of boronated absorber balls that also are inserted into channels in the reflector. In an event in which rods fail to scram, an automatic trip of the helium circulator causes the reactor to shut down due to the strong negative temperature reactivity coefficient. Subsequently, the absorber balls are manually triggered to maintain subcriticality as decay heat diminishes and the reactor approaches cold shutdown.

3.3.2.5 Modular high temperature gas reactor—MHTGR

The modular high temperature gas reactor (MHTGR) is a modular HTGR design whose development was primarily supported by DOE.⁶³ The MHTGR was originally conceived as four identical prismatic core reactor modules cooled by helium. Steam generators provide heat removal from the helium coolant loop in each reactor module. The steam lines for four reactors are coupled to a steam header. Two steam turbine-generators are connected to the steam header for electric power generation. Later design concept variations incorporated Brayton cycle gas turbines for higher thermal efficiency either via a direct cycle or through an intermediate helium loop. The Brayton cycle design is called the gas turbine, modular helium reactor (GT-MHR).

The design of the MHTGR provides for interconnected and integrated automatic control of the four reactor modules and two turbine generator systems that comprise the plant. Automatic control is used for normal operations and for abnormal events; no operator actions are required to shut down the reactor for event categories included in the safety analysis. The plant safety/protection function is provided by separate, redundant safety-related I&C components. The plant control systems are to provide complete, computerized, automatic control of the plant using hardware platforms characterized as redundant and fault tolerant. Consequently, an operator and an assistant are capable of accomplishing operational control of the plant from the main control room (MCR). Additional monitoring and control capabilities are provided at a remote shutdown area room in the reactor service building and in plant protection and instrumentation system rooms in each reactor building.

MHTGR plant protection and automatic control are provided by the partly safety-related plant protection and instrumentation system (PPIS); the plant control, data, and instrumentation system (PCDIS); and the miscellaneous control and instrumentation group (MCIG).

The MHTGR instrumentation and control system has several novel features compared with the existing reactor fleet. These features include:

- All four reactor modules and the two turbine generators are monitored and controlled from a single control room via a modular, distributed control system that allows load to be allocated automatically among the reactor modules and the two turbine generators.
- An independent, redundant, and fully automated protection system, including a remote shutdown area is provided. The safety-related portions of the system (reactor trip and main coolant loop

shutdown) are fully automatic; no safety-related operation actions are necessary or are even available in the control room.

- Most of the PPIS circuitry is contained in reactor module equipment rooms. The control room is not deemed as safety-related by the applicant.
- Control room operator actions are not viewed as safety-related but as a monitoring function and performance of plant mission management activities.
- Manual initiations of protective functions may be carried out in the remote shutdown area (RSA) or reactor module PPIS equipment rooms.

The control room, RSA room, and reactor module PPIS rooms are designed to limit operator exposures during accident conditions.

The PPIS indicates plant status and automatically actuates safety-related control systems and investment protection control systems. It consists of the safety protection, special nuclear area instrumentation, and investment protection subsystems. The safety protection subsystem initiates a reactor trip and shuts down the main cooling system. The safety protection subsystem is safety-related and quadruple-redundant protection channels are employed for each reactor module. In effect, each module has a separate and independent, remotely multiplexed, centrally controlled, microprocessor-based safety protection system. As originally planned, separate and independent safety protection system operator interfaces for each reactor module were to be provided in the plant's RSA room. It is postulated that this interface capability would likely have been extended to the MCR.

The investment protection subsystem monitors plant conditions and initiates protective actions to limit plant investment risk. It was proposed as a nonsafety system whose functions include:

- reactor trip with inner control rods,
- steam generator isolation and dump,
- shutdown cooling system initiation,
- primary coolant pumpdown, and
- shutdown cooling heat exchanger isolation.

Operator interfaces for safety protection equipment are provided for each reactor module in PPIS equipment and RSA rooms. An operator may initiate reactor trips and main cooling system shutdown from the remote shutdown areas, separate from the MCR. In the proposed design, manual inputs (e.g., manual reactor trips) to the safety protection system could not be made from the MCR; however, a normal shutdown could be accomplished from the MCR. The operator interfaces are separate and independent of all other plant I&C interfaces.

The nonsafety-related PCDIS is a network of integrated, hierarchical digital computers and control and monitoring instrumentation that permits the modular reactor units and two turbine generators to be operated and controlled from startup to power operation to normal shutdown. It is comprised of four subsystems: (1) plant supervisory control subsystem (see Fig. 18), (2) nuclear steam supply system control subsystem, (3) energy conversion area control subsystem, and (4) data management subsystem.⁶⁴

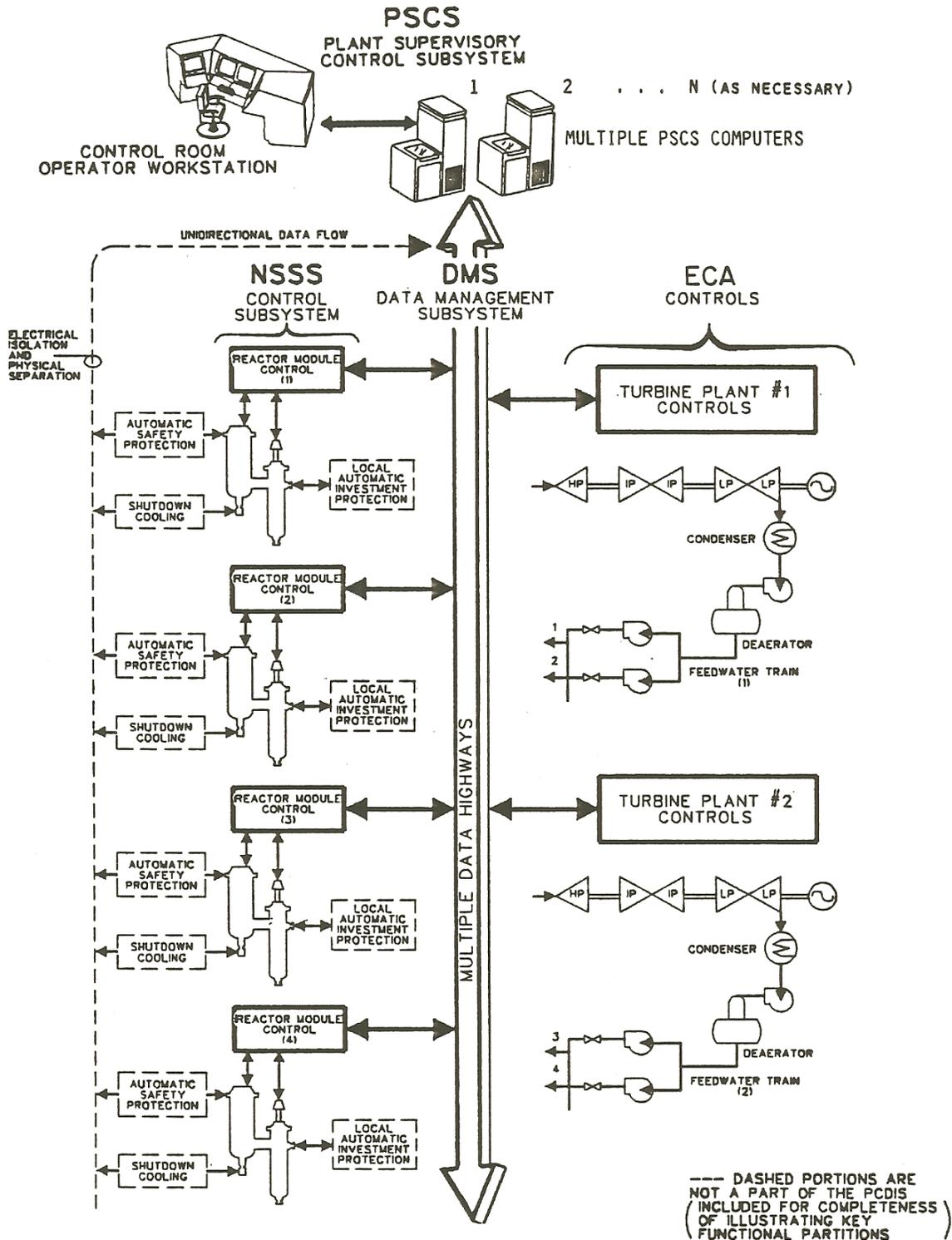


Fig. 18. MHTGR plant supervisory control system overview.⁶⁵

The plant supervisory control subsystem (PSCS) coordinates plant control during operation, shutdown, refueling, and startup/shutdown. The PSCS determines the distribution of overall plant load demand among individual reactor modules and turbine generators. It determines main steam and feedwater flow

rates necessary to meet load maneuvers that may arise from the plant operator, grid operator, or reactor module or plant conditions. The PSCS computers manage the plant through selection of the necessary mode of plant operation and control strategy for best operation of the reactor modules and turbine generators independently at various power levels and then validates appropriate plant response. The PSCS has startup/shutdown, normal operation, refueling, shutdown, and abnormal operating modes. Startup and shutdown operation is achieved by bringing the modules to minimum stable operating conditions sequentially through series of operator checkpoints several times during the startup/shutdown. For abnormal operating modes, the PSCS coordinates continuous plant operation during and following transient conditions associated with problems with major systems or components of the reactor module and turbine generator. The PSCS implement control strategies for reloading the plant once problems have been corrected. The PSCS is capable of recovering from generator load rejects and turbine trips (except on low condenser vacuum) from any power level without requiring a reactor trip, even if reactor modules or turbine generators are constrained for some reason.

Each reactor module has its own nuclear steam supply system (NSSS) control subsystem that controls reactor conditions and supply of steam to the main steam header. The NSSS control subsystem responds to demands from the PSCS through appropriate local control action. The major functions of the NSSS control subsystem are to manage module feedwater flow control demand, circulator speed control, power characterization, main steam temperature control, and main steam pressure during startup. The NSSS control subsystem reactor module control loops are configured to accommodate feedwater, reactor module, and turbine trips. In addition, the control loops minimize transient extremes to protect plant equipment and optimize NSSS availability. The NSSS control subsystem provides startup/shutdown, normal operation, refueling, shutdown, and abnormal operation functions.

The energy conversion area control subsystem provides monitoring and control for electrical power generation. The data management subsystem provides the data communication between the subsystems.

The MCIG systems provide additional data to the operator and for retention. These systems are (1) the NSSS analytical instrumentation system, (2) radiation monitoring system, (3) seismic monitoring system, (4) meteorological monitoring system, and (5) the fire detection and alarm system.

4. REGULATORY BASELINE FOR HIGHLY AUTOMATED CONTROL ROOMS

4.1 Code of Federal Regulations

The Code of Federal Regulations (CFR) is a compilation of rules published in the Federal Register by the executive departments and agencies of the Federal Government. Title 10 provides regulations addressing Energy. Regulations associated with the NRC are contained in Title 10 – Energy, Chapter I – Nuclear Regulatory Commission, Parts 0-199. Part 50 of 10 CFR Ch I (usually abbreviated as 10 CFR 50) primarily applies to NRC licensed commercial nuclear reactors. Criteria identified in 10 CFR 50 are typically met by licensees through adherence to industry standards (such as applicable Institute of Electrical and Electronics Engineers standards) and NRC regulatory guides. Part 52 addresses regulations for early site permits, standard design certifications, and combined licenses for nuclear power plants. Under the provisions of the certification and licensing process established in this part, compliance with the standards and criteria set out in Part 50 is required.

This section contains an overview of key regulations related to I&C systems in nuclear power plants. These regulations are a foundational element of the regulatory baseline for evaluating the safety characteristics of highly automated control room designs.

4.1.1 General design criteria

The top level regulatory requirements for I&C systems are stated in the General Design Criteria (GDC) in Appendix A of Title 10, Part 50 of the Code of Federal Regulations (10 CFR 50). The GDC are specified for LWRs of the types previously licensed by the NRC but are considered generally applicable to other types of reactors like HTGRs. The GDC governing I&C systems are primarily 13 and 20 through 29. These GDC state the main underlying principles for I&C systems in providing a high degree of assurance that the plant will operate as designed and public health and safety will be protected. Wilson et al.⁵⁴Error! bookmark not defined. discussed the application of the GDC to HTGR safety structures and components (SSCs) and identified differences that may need to be addressed by the NGNP safety systems. In this section, specific considerations for I&C systems and highly automated control room designs are discussed.

GDC 13, “Instrumentation and Control,” requires that instrumentation shall be provided to monitor variables and systems over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Controls must be provided to maintain systems within their prescribed ranges.

This criterion applies to all I&C systems and supporting data communication systems. Specific elements of the I&C system needed to meet the intent of GDC 13 include:

- instrumentation to monitor plant variables and systems,
- instrumentation to monitor the status of protection systems,
- I&C for manual initiation of safety functions,
- I&C to support diverse actuation of safety functions,
- I&C to regulate engineered safety features,
- interlocks to maintain variables and systems within safe states,
- I&C to maintain variables and systems within normal operational limits,
- protection of instrument sensing lines from environmental extremes,
- set points for instrumentation system alarms and control system actions, and
- data communication systems that support plant I&C.

GDC 19, “Control Room,” requires that a control room be provided from which actions can be taken to operate the plant safely under normal conditions and to maintain it in a safe condition under accident conditions. In addition, equipment must be provided at appropriate locations outside the control room that supports achieving prompt hot shutdown of the reactor and maintaining a safe condition during shutdown.

This criterion is applicable to all I&C systems and supporting data communication systems. It involves establishment of the provision for I&C equipment to operate the nuclear power plant under normal and accident conditions; reactor trips, interlock functions, and diverse I&C functions that support safe operation; and safe shutdown and remote shutdown capabilities.

GDC 21, “Protection System Reliability and Testability,” requires that protection systems shall be designed for “high functional reliability and inservice testability commensurate with the safety functions to be performed.” GDC 21 also stipulates the single failure criterion and a design that is capable for test for failures and losses of redundancy.

Compliance with Criterion 21 is established by addressing the following characteristics in design, development, implementation, testing, and installation of the plant I&C systems:

- design basis reliability requirements and reliability determination methods,
- single-failure criterion,
- completion of protective action once initiated,
- quality,
- system integrity,
- physical, electrical, and communication independence,
- capability for test and calibration,
- indication of bypass,
- control of access to safety system equipment,
- repair and troubleshooting provisions,
- identification of protection system equipment,
- auxiliary features,
- multi-unit stations,
- human factors considerations,
- reliability,
- manual controls,
- derivation of system inputs,
- operating bypasses,
- multiple set points, and
- power sources.

GDC 22, “Protection System Independence,” stipulates the independence principle. Protection systems “shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.” The application of GDC 22 results in design techniques known commonly as diversity and defense-in-depth.

Compliance with Criterion 22 is established by addressing the following characteristics in design, development, implementation, testing, and installation of the plant I&C systems:

- single-failure criterion,
- equipment quality,
- equipment qualification,
- system integrity,
- physical, electrical, and communication independence,

- manual controls, and
- set points.

GDC 23, “Protection System Failure Modes,” requires that protection system failure modes terminate in a “into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.”

Compliance with GDC 23 involves ensuring system integrity requirements such that the protection system can accomplish its safety functions under the full range of applicable conditions enumerated in the design basis. For computer-based protection systems, the integrity requirements also involve software quality assurance (including software hazard analyses) and design for test (e.g., self-testing and diagnostics).

GDC 24, “Separation of Protection and Control Systems,” specifies separation of protection and control systems. “The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.”

Compliance with Criterion 24 is established by addressing the following characteristics in design, development, implementation, testing, and installation of the plant I&C systems:

- single-failure criterion,
- independence,
- control-protection interaction,
- auxiliary features, and
- power sources.

4.1.2 Criteria for safety-related I&C systems

Paragraph 55a of 10 CFR 50 (10 CFR 50.55a) identifies codes and standards that each operating license for a light-water reactor facility must satisfy. The relevant standard for I&C systems is identified in 10 CFR 50.55a(h). In essence, safety systems of nuclear power plants are required to meet criteria stipulated in IEEE 603-1991, “Standard Criteria for Safety Systems for Nuclear Power Generating Systems.”⁶⁶ IEEE 603-1991 addresses the design of systems performing safety functions. Issues such as design bases, redundancy, independence, single failures, qualification, bypasses, status indication, and testing are addressed.

Treatment of the safety system design criteria in IEEE 603 includes the following considerations:

Single Failure Criterion

Establish that any single failure within the safety system will not prevent proper protective action at the system level when required.

Completion of Protective Action

Ensure that “seal-in” features are provided to enable system-level protective actions to go to completion.

Quality

Confirm that quality assurance provisions of Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” to 10 CFR 50 are applied to the safety system.

Equipment Qualification

Validate that the safety system equipment is designed to meet the functional performance requirements over the expected range of environmental conditions (including abnormal and accident conditions) for the area in which it is located.

System Integrity

Confirm that the design includes the qualification of equipment for the conditions identified in the design bases.

Independence

Assess independence between (1) redundant portions of a safety system, (2) safety systems and the effects of design basis events, and (3) safety systems and other systems.

Three aspects of independence should be addressed in each case:

- physical independence,
- electrical independence, and
- communications independence.

Capability for Test and Calibration

Assess the provision in the design for test and calibration.

Information Displays

Evaluate the characteristics of safety-related information displays.

Multi-unit Stations

Confirm that shared systems and resources does not impair the capability to simultaneously perform requires safety functions in all units.

4.1.3 Guidance for safety-related digital I&C systems

Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. The complexity of most digital I&C system designs means that the performance of digital systems over the entire range of input conditions cannot generally be inferred from testing at a sample of input conditions. Thus, acceptance criteria for digital safety-related I&C systems address the high-quality development process as well as the system testing to establish qualification for safety application.

Regulatory Guide 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” endorses the design criteria of IEEE 7-4.3.2, “Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations,”⁶⁷ as an acceptable method for complying with NRC’s regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. IEEE 7-4.3.2 provides computer specific requirements to supplement the criteria and requirements of IEEE 603 to establish minimum functional and design requirements for computers used as components of a safety system.

At the highest level, the review of safety-related digital I&C systems considers evidence regarding the system design, development process, and implementation. Essentially, the reviewer is assessing whether the following characteristics and conditions have been demonstrated:

1. Plant and overall I&C system requirements are correctly decomposed into the digital I&C system requirements for each digital I&C system under review. Critical hardware and software characteristics are identified;

2. A development process is specified and documented such that implementation of the process gives a high degree of confidence that the functional requirements will be or are implemented in the computer system. The life cycle process plan describes a coordinated engineering process in which design outputs at each planned stage of the design process are verified to implement the input requirements of the stage;
3. The specified process and products, including design outputs, are designed to be inspected at staged checkpoints; and
4. The installed system functions as designed. Validation and integration tests, acceptance tests, and on-site pre-operational and start-up functional tests demonstrate that the identified critical hardware and software characteristics are verified.

The review of any digital I&C system addresses key topics such as adequacy of design criteria and guidance, application of defense-in-depth and diversity, adequacy of system functions for the individual I&C systems, execution of life cycle process planning, adequacy of the software life cycle process implementation, and characteristics of software life cycle process design outputs. For life cycle process planning, the review specifically addresses confirmation that software life cycle plans have commitments to coordinated execution of activity groups and staged checkpoints at which product and process characteristics are verified during the development process. For life cycle software process implementation, the review includes audits of a sample of verification and validation, safety analysis, and configuration management documentation for various life-cycle phases. Regarding the characteristics of software life cycle process design outputs, the review involves conformance of the hardware and software to the functional and process requirements derived from the design bases, confirmation that software design outputs address the functional requirements allocated to the software and that the expected software development process characteristics are evident, and assessment of adequacy of the system test procedures and test results to provide assurance that the system functions as intended.

In digital I&C systems, data, software, communications, and hardware may be common to several functions to a greater degree than is typical in analog systems. Thus, the acceptance review of digital I&C systems emphasizes quality and defense-in-depth and diversity as protection against propagation of common-mode failures within and between functions. Additional system aspects that may pose assurance challenges include real-time performance, independence, and online testing.

4.1.4 Control room staffing criteria

NRC regulations and policies stipulate operator staffing requirements for licensed nuclear reactor facilities. In particular, reactor plant control room staffing requirements are mandated in 10 CFR 50.54(m)(2)(i). These requirements are based on experience with the operation of the large, base-loaded reactors currently in use in the United States.

Each plant must meet a minimum licensed operator staffing requirements. The required minimum control room staffing is given in Table 1. The number of required licensed personnel when the operating nuclear power plant units are controlled from a common control room are two senior operators and four operators.

Table 1. Minimum requirements per shift for on-site staffing of nuclear power plant units

Number of nuclear power units operating	Position	One unit	Two units		Three units	
		One control room	One control room	Two control rooms	Two control rooms	Three control rooms
None	Senior Operator	1	1	1	1	1
	Operator	1	2	2	3	3
One	Senior Operator	2	2	2	2	2
	Operator	2	3	3	4	4
Two	Senior Operator		2	3	3	3
	Operator		3	4	5	5
Three	Senior Operator				3	4
	Operator				5	6

4.2 Interim Staff Guidance

To help reduce regulatory uncertainty in the review of safety-related I&C systems, NRC established the Digital I&C Steering Committee to direct its activities toward achieving the goal of an enhanced regulatory review process that facilitates efficient, predictable licensing while maintaining the necessary assurance of safety. Specific Task Working Groups (TWGs), composed of NRC staff, were formed to address the following topics: I&C Technical Issues (i.e., Digital Communication as well as Diversity and Defense-in-Depth), Human Factors, Cyber Security, Risk Informed Digital I&C Regulation, and the Digital I&C Licensing Process. Numerous public meetings were conducted to facilitate technical information exchange and enable public involvement in the discussion of regulatory needs. The principal products resulting from these interactions are Interim Staff Guidance (ISG) documents developed by the TWGs to capture the current regulatory positions on significant digital I&C issues related to nuclear power plants. Some of these ISG contain regulatory positions that are relevant to the assessment of highly automated control room design for VHTRs. The positions of key ISG are discussed below.

4.2.1 Digital I&C ISG-02: Diversity and Defense-in-Depth Issues

Digital I&C ISG-02, “Task Working Group #2: Diversity and Defense-in-Depth Issues,” Rev. 2, provides acceptable methods for implementing digital system designs that comply with NRC policies on diversity and defense-in-depth (D3) issues. In particular, this ISG is intended to serve as clarification on the criteria to be used in evaluating consistency of a digital system design with the NRC’s D3 guidelines.

4.2.1.1 Adequate diversity

Determining the level of “diversity” of an engineered system—if not assigning a “quantity” to that determination—has been a challenge, particularly for digital systems. There are credible questions:

- How much D3 is considered adequate?
- Are there precedents for good engineering practice?
- Can sets of diversity attributes and criteria provide adequate diversity?
- How much credit can be taken for designed-in robustness in determining the appropriate amount of diversity?
- Are there standards that can be endorsed?

Staff Position

The D3 guidance for digital RPS designs, which includes the reactor trip system (RTS) and the engineering safety features actuation system (ESFAS), applies equally for new nuclear power plants and current operating plants. While common-cause failures (CCFs) in digital systems are classified as beyond design basis events, reasonable assurance should be provided that the digital RPS is protected against CCF.

A D3 analysis should be performed to demonstrate that potential CCF vulnerabilities are properly addressed. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,”⁶⁸ and Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” of NUREG-0800, “Standard Review Plant (SRP)” provide methods acceptable to the NRC staff for performing a D3 analysis.

The D3 analysis should reveal if any of the safety functions to be performed by the RPS could become subject to a CCF. Based on the outcome of the analysis, designers can add backup systems or provide diverse methods to perform a safety function found to be vulnerable for potential CCF.

If additional diversity is found to be necessary for a safety function, the backup function can be performed automatically or by manual operator actions in the MCR. Typically, the preferred method is to perform the safety function via an automated system.

If an automated system is used as the backup, the licensee should demonstrate that the equipment involved in the safety function would not be affected by the postulated CCF in the RPS. Furthermore, the system should be sufficient to maintain plant conditions within the recommended acceptance criteria, as identified in BTP 7-19, for any particular anticipated operational occurrence and design basis accident. The automated backup functions can be performed by nonsafety systems, so long as such systems meet the quality requirements for systems intended for protection against anticipated transients without scram (ATWS), as required by the ATWS rule [10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants”].

4.2.1.2 Manual operator actions

This position is intended to address the use of operator action as a defensive measure against CCF and clarify the corresponding acceptable operator action times.

Staff Position

If the D3 analysis reveals that additional diversity is necessary, the licensee may choose to use manual operator actions as the backup function. In this case, a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions could be maintained within the recommended acceptance criteria given in BTP 7-19 for a particular anticipated operational occurrence or design basis accident. Acceptability of such actions is subject to staff review in accordance with Digital I&C ISG-05,

“Highly-Integrated Control Rooms—Human Factors Issues,” Rev. 1. For actions with limited margin, such as less than 30 minutes between time available and time required for operators to perform the protective actions, a more rigorous staff review should be expected.

In addition to the guidance in ISG-05, a set of displays and controls (safety or nonsafety) should be provided in the MCR for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal, reactor coolant system integrity, and containment isolation and integrity. The manual actuation should be implemented in accordance with existing regulations, and the displays and controls should be unaffected by the CCF in the RPS.

4.2.1.3 BTP 7-19 Position 4 challenges

This position is intended to clarify Position 4 of BTP 7-19, which specifies the provision of a set of displays and controls in the MCR for manual system-level actuation of critical safety functions. The intent is to resolve uncertainty about whether credit can be taken for component-level versus system-level actuation of equipment.

Staff Position

A revision of BTP 7-19, Position 4 is recommended to clarify the scope of the MCR displays and controls necessary to satisfy the position. The revision specifies that diverse manual initiation of safety systems should be performed on a system-level basis for each division. However, manual control of individual safety system components can also be provided in addition to system-level manual controls. If their primary function is to serve as diverse backups to automatic systems, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same CCF that necessitated the diverse backup system.

With this position, emphasis is placed on minimizing the number of discrete operator actions to initiate operation of the minimum-required safety equipment to implement manual initiation of safety functions at the division level. The important considerations are that the manual actuation is performed at the division level from within the control room and that appropriate displays are adequate to support sufficient being time available for the operators to determine the need for protective actions, even with malfunctioning indicators. Sufficient instrumentation should exist to indicate that (1) protective action is needed, (2) the automated safety system did not perform the protective functions, and (3) the manual action successfully accomplished the safety function.

4.2.1.4 Effects of common-cause failure

This position is intended to clarify whether spurious actuations should be considered when evaluating software CCF.

Staff Position

The primary concern in a situation that disables a safety function involves an undetected failure that could prevent system actuation when required. It is observed that spurious actuations are self-announcing so they can be detected and corrective action taken. The NRC staff position is that spurious trips or actuations of safety-related digital protection systems resulting from CCFs are generally of a lesser safety concern than failures to trip or actuate. Therefore, they do not need to be addressed beyond what is already set forth in plant design basis evaluations (i.e., the effects of spurious trips are bounded by the plant design basis).

However, the design of a diverse automated or diverse manual backup actuation system should address how to significantly reduce or eliminate the potential for spurious actuation of the protective system.

4.2.1.5 Common-cause failure applicability

This position is intended to clarify the identification of design attributes (e.g., simplicity) that are sufficient to eliminate consideration of CCF.

Staff Position

Two design attributes are identified that are sufficient to eliminate consideration of CCF:

1. Diversity: If sufficient diversity is demonstrated in the protection system (e.g., through a D3 analysis) such that the potential for CCF is fully addressed. [Sufficient diversity is treated on a case-by-case basis considering the design and process attributes that resolve CCF vulnerability.]
2. Testability: If a system sufficiently simple, such that every possible combination of inputs, internal and external states, and every signal path can be tested, the system is said to be fully testable.

4.2.1.6 Echelons of defense

BTP 7-19 references the echelons of defense described in NUREG/CR-6303 for maintaining the key safety functions within the prescribed margins. This position provides additional clarification regarding how the echelons of defense for maintaining the safety functions should factor into D3 analyses. Of particular concern is that the current BTP 7-19 guidance does not fully consider the impact of plant design characteristics and operating procedures on implementation of those safety functions.

Staff Position

Since the echelons of defense are conceptual, the RTS and ESFAS functions may be combined into a single digital platform as part of a comprehensive RPS. There is no requirement that they be independent or diverse. However, this approach could introduce new CCF mechanisms that otherwise would not exist if separate software applications were to be used. Thus, an assessment of postulated CCFs must demonstrate that the safety functions of the digital RPS is not impaired and that an acceptable plant response is ensured regardless of the echelons of defense that may be affected.

4.2.1.7 Single failure

This position is intended to clarify classification of digital system CCFs as single failures in design basis evaluations.

Staff Position

Postulated CCFs for a digital system, including software CCFs, are not classified as single failures and, thus, are not subject to treatment in accordance with the single failure criterion applied to safety system designs. Consequently, postulated digital system CCFs should not be included among the single random failures accounted for in design basis evaluations.

4.2.2 Digital I&C ISG-04: Highly-Integrated Control Rooms—Communication Issues

Digital I&C ISG-04, “Task Working Group #4: Highly-Integrated Control Room—Communications Issues (HICRc),” Rev. 1, addresses known issues for digital I&C systems related to interactions among safety divisions, and between safety-related equipment and equipment that is not safety-related. Interactions among safety-related equipment that are entirely within one safety division or among other equipment that do not perform safety-related functions are not within the scope of this ISG. However, the positions of this ISG are relevant in considering aspects of digital control systems that are may not be safety-related but may affect the plant conformance to safety analyses.

The term “Highly-Integrated Control Room” (HICR) is coined to refer to a control room in which the traditional control panels are replaced by computer-driven consolidated operator interfaces. ISG-04

describes how to maintain separation, isolation and independence among redundant channels for HICR in which controls and indications from all safety divisions may be combined into a single integrated workstation.

4.2.2.1 Interdivisional communications

Interdivisional communications includes transmission of data and information (both unidirectional and bidirectional) among components in different safety divisions, as well as communications between a safety division and equipment that is not safety-related. It does not include internal communications within a single division.

Staff Position

Interdivisional communications and bidirectional communications between a safety division and nonsafety equipment are acceptable with certain restrictions. The restrictions that should be enforced are summarized as follows:

1. A safety channel should not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.
2. The safety function of each safety channel should be protected from adverse influence from outside its division.
3. A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function.
4. The communication process itself should be carried out by a communication processor separate from the processor that executes the safety function, so that communication errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information.
5. The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory, which should include the response time of the memory itself and of the circuits associated with it, as well as the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor.
6. The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.
7. Only predefined data sets should be used by the receiving system. Message format and protocol should be pre-determined. Every datum should be included in every transmit cycle. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with pre-specified design requirements.
8. Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.
9. Incoming message data should be stored in fixed, predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

10. Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.
11. Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service.
12. Communication faults should not adversely affect the performance of required safety functions.
13. Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provision for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid untimely or otherwise questionable data.
14. Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable).
15. Communication for safety functions should transmit a fixed set of data at regular intervals.
16. Network connectivity, liveness and real-time properties essential to the safety application should be verified in the protocol. Liveness means that no connection to any network outside the division can cause an RTS/ESFAS communication protocol to stall.
17. Medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments.
18. Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.
19. All links and nodes should have sufficient capacity to support all functions, such that data throughput will not exceed the capacity of a communications link.
20. The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate, and is supported by the error rate observed in design and qualification testing.

4.2.2.2 Command prioritization

This position is intended to provide guidance applicable to a prioritization hardware or software function block, which is referred to as a priority module.

A priority module, which should be considered to be a safety-related device, receives device actuation commands from multiple safety and nonsafety sources, and transmits the command having highest priority to the actuated device.

Staff Position

Pursuant to the existing D3 guidance, priority modules that combine diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to CCFs. Also, it should be demonstrated that adequate configuration control measures are in place to ensure that software-based priority modules, which might be subject to CCF, will not be used at a later time to replace modules credited for diversity. In effect, provisions of an overall quality assurance program should address version control, component inventory management, and maintenance process as part of configuration management to ensure that credited diversity is not compromised over the plant lifetime.

Priority modules of various forms are acceptable subject to certain conditions. The conditions that should be met are summarized as follows:

1. A priority module must be treated as a safety-related device or function and meet all of the applicable regulatory requirements for safety-related hardware or software.
2. Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function, as per requirements and specifications, independent of the state or the condition of the digital system.
3. Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. For cases where a “safe state” definition is ambiguous, the ranking rationale must be presented and explained in detail by the licensee.
4. If a priority module controls more than one component, all of these provisions apply to each of the actuated components.
5. Communication isolation of each priority module should be as described in the guidance for interdivisional communications.
6. Software used in the design, testing, maintenance, etc. of a priority module should conform to all the requirements of IEEE Std. 7-4.3.2-2003, as endorsed by Regulatory Guide 1.152. Of particular note is whether design tools used for programming a priority module require validation. If the priority module is 100% testable, then no validation is required for the design tools. Complete testing involves every possible combination of inputs and every possible sequence of device states, with all outputs being verified for every case. The testing should not involve the use of design tool.
7. Any software code that is used in support of the safety function within a priority module should be designated as such. Nonvolatile memory should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. Field programmable gate array (FPGA) contents should be considered software, and should be developed, maintained, and controlled accordingly.
8. The priority module design should be fully tested to minimize the probability of failures due to common software. If the tests are generated by any automatic test generation program, then all the test sequences and test results should be manually verified. If the testing of all possible combinations of inputs is not considered practical, then the applicant should identify the testing that is excluded and justify that exclusion.
9. Automatic testing within a priority module—such as testing during plant operation—should not inhibit the safety function of the module in any way.
10. The priority module must ensure that the completion of a protective action is not interrupted by commands, conditions or failures outside the module’s own safety division.

4.2.2.3 Multidivisional control and display stations

This position is intended to provide guidance for operator workstations used for control of the plant equipment in more than one safety division, and for display of information from sources in more than one safety division. The position addresses independence and isolation, human factors considerations, and D3 considerations.

4.2.2.3.1 Independence and isolation

Staff Position

In instances where a nonsafety station receives information from one or more safety divisions, all communications by nonsafety equipment with safety-related equipment should conform to the guidelines for interdivisional communications (see section 4.2.2.1).

Where a safety-related station receives information from outside its own division, all communications originating from other divisions (either from safety-related or nonsafety equipment) to safety-related equipment should conform to the guidelines for interdivisional communications (see section 4.2.2.1).

Nonsafety stations may control the operation of other safety-related equipment provided that the following restrictions are enforced:

- Nonsafety equipment can communicate with a safety-related equipment only through a priority module associated with that equipment.
- Nonsafety equipment must not affect the operation of other safety-related equipment when the latter equipment is performing its safety function. This provision must be an inherent and permanent feature of the safety-related equipment.

Safety-related stations controlling the operation of equipment in other divisions are subject to similar constraints:

- Safety-related equipment may access other safety-related equipment outside its own division only through a priority module associated with that equipment.
- Safety-related equipment must not affect the operation of other safety-related equipment when the latter equipment is performing its safety function. This provision must be an inherent and permanent feature of the safety-related equipment.

The result of malfunctions of control system resources shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria include the following:

- Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.
- Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor.
- Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations. The likelihood and consequences of malfunction of multiple processors as a result of a CCF must be addressed.
- Any command to control plant equipment should be generated by at least two deliberate operator actions.
- Each control processor or its associated communication processor should be capable of detecting and blocking instructions that do not pass the error checks.
- Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, electromagnetic interference and radio-frequency interference (EMI/RFI), power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location.
- Loss of power, power surges, power interruption and any other credible event to any operator workstation or controller should not result in spurious actuation or interruption of any plant service or system unless these provisions are enveloped in the plant safety analyses.
- The design should have provision for an “operator workstation disable” switch to be activated upon abandonment of the MCR to preclude spurious actuations.
- Failure or malfunction of any operator workstation must not result in a plant condition that is not enveloped in the plant design bases, accident analyses and ATWS provisions, or in other unanticipated abnormal plant conditions.

4.2.2.3.2 Human factors considerations

Staff Position

Safety-related equipment should have safety-related controls and displays. For any safety-related equipment not conforming to this requirement, the license applicant should demonstrate that safety-related controls and displays are not needed in consideration of these requirements.

It may be acceptable for operators to use nonsafety controls and displays in lieu of safety-related controls and displays to perform safety functions. However, it must be possible for operators to perform all safety functions using safety-related controls and displays, and without the need for any nonsafety equipment.

If nonsafety-related multidivisional control and display stations are used, operators are expected to confirm that appropriate responses have been achieved for the actions taken. The license applicant is expected to demonstrate that the nonsafety control and display stations will withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges and other plant design-basis conditions for the purpose of surviving in the environment they are intended to function. If the response of the actions taken by use of nonsafety control stations cannot be confirmed, then operators are required to confirm the desired response from the safety-related controls and displays. If confirmed that operation through the use of nonsafety multidivisional control and display station is compromised, subsequent safety-related actions must be taken from safety-related control and display stations.

The applicant is also required to demonstrate that human factors considerations (e.g., operator response time and situation awareness) are consistent with the system design bases, operating procedures and accident analyses. These considerations must be reasonable and adequate given the possibility of erroneous indications from nonsafety equipment.

4.2.2.3.3 Diversity and defense-in-depth (D3) considerations

Staff Position

D3 considerations may influence the number and disposition of operator workstations, and possibly of backup controls and indications that may or may not be safety-related. D3 considerations may also impose qualification or other measures. Additional guidance is provided in ISG-02.

4.2.3 Digital I&C ISG-05: Highly-Integrated Control Rooms—Human Factors Issues

Digital I&C ISG-05, “Task Working Group #5: Highly-Integrated Control Room—Human Factors Issues (HICR-HF),” Rev. 1, provides acceptable methods for addressing human factors issues to comply with NRC regulations regarding nuclear power plant control rooms.

4.2.3.1 Computer-based procedures

This position provides clarification on acceptance criteria for computer-based procedure systems and computer-based procedures. It is intended to complement guidance provided in NUREG-0700, “Human-System Interface Design Review Guidelines,”⁶⁹ and NUREG-0899, “Guidelines for the Preparation of Emergency Operating Procedures.”⁷⁰

Descriptions of a computer-based procedure system should address the following items:

- interaction between the operator and the computer-based procedure,
- interaction between the computer-based procedure and the control and process systems,
- use of plant data, if any,
- use of automation, if any,
- use of operating controls, if any,

- presentation of procedures on the computer-based procedure system, and
- implementation of a backup system to the computer-based procedure system.

4.2.3.1.1 Computer-based procedures systems

Staff Position

A general review criterion for computer-based procedures systems is that the system that displays operating procedures should be designed as an integral part of the MCR. The overarching goal of such a system is to allow operators to easily transition from one procedure to another.

The procedure system should accomplish a procedure step by step at the direction of the operator. The information should be furnished with sufficient displays to show that the operators are indeed in control of the system. This basis of being in control of a procedure system is rooted in the availability and suitability of information displays, control and system processes. Further guidance on defining the information, control and process specifications can be found in NUREG-0711, “Human Factors Engineering Program Review Model.”⁵² Important parameters include, but are not limited to, the following: (1) system response time, (2) system feedback, (3) information representation, (4) information format, (6) information quality (validity), (7) range of control options, (8) user expectations, and (9) providing current information.

It should be demonstrated that the computer-based procedure system will present the most recently approved and issued version of a procedure. Measures should be in place to inform the operators if a selected procedure cannot be displayed.

Incorporation of plant data into the computer-based procedure system is optional. If the system requires user input, a data entry method should also be implemented. Measures should be in place to ensure that the plant data displayed in the computer-based procedure system is consistent with the actual plant data. The system should inform the operator if the information displayed is questionable, or cannot be validated.

Automation of displaying procedure steps is also optional. Automatic sequencing should be initiated by the operator, and it should be predictable. Operators should be able to interrupt the automatic sequencing at any time, and should be able to step through the procedures.

The procedure should be selected by the operator, not automatically by the procedure system. However, the computer-based procedure system can recommend a procedure.

Initiation of a procedure should be done at the discretion of the user, not automatically by the system. This provision also applies to initiation of control actions: control actions can be recommended, but operator confirmation is required in each instance. The system can prompt operators to take specific manual action. Hold points, such as a “Caution” or “Warning” sign, should be established.

If computer-based operating procedures are implemented for emergency operating procedures, or any procedure needed for accident mitigation, safe shutdown, emergency response, severe accident management, or the performance of other critical manual actions identified in the plant probabilistic risk assessment (PRA), then certain features and characteristics should be provided. These features include notifying the operator of concurrent steps, informing the operator of incomplete results with contingency actions, identifying applicable steps to the operator, managing concurrent use of multiple procedures, providing integration with alarms, system status, and critical safety functions, and monitoring procedure entry and exit conditions.

The use of “soft control” is optional in the design of computer-based procedure systems. These interfaces should provide feedback to the user regarding the state of the plant. Control of any equipment should require at least two actions by the operator. The displays for the procedure system should be presented to mimic the monitoring and control panels in the MCR.

For modernizations projects, human-system interface design should follow the plant-specific conventions and standards to minimize operator error.

4.2.3.1.2 Computer-based procedures

Staff Position

The review criteria for computer-based procedures are based on fundamental tenets of information presentation. The procedures should be easily legible on the display device. If scrolling is necessary, up/down scrolling should be opted. If left/right scrolling is unavoidable, the presence of extra information should be obvious to the operator without equivocation.

The computer-based procedure should be based on approved and issued procedures; not the other way around. These procedures should provide the user with a minimum set of information about the state of the plant and the procedure system. As a minimum, the procedure title should be displayed at all times. Other relevant data can be made accessible at operators' discretion; but do not need to be presented continuously.

Backup procedures in an alternative medium—such as a paper-based system, or safety-related computer-based procedure system—should be maintained to perform all necessary operating procedures and mitigatory measures. The alternative media should be available and easily accessible. These procedure systems should have the same content, and should be subject to the same procedural controls as the primary computer-based procedure system.

4.2.3.2 Minimum inventory

This position is intended to clarify the requirements for minimum inventory of human system interfaces (i.e., alarms, displays and controls) needed to implement the emergency operating procedures, bring the plant to a safe state, and execute those operator actions shown to be risk important by the plant's PRA.

Staff Position

The minimum inventory of human-system interfaces should be developed for the MCR and the remote shutdown facility (RSF).

The MCR minimum inventory should ensure that human-system interfaces are always available to enable the operator to accomplish the following:

- monitor the status of fission product barriers,
- perform and confirm a reactor trip,
- perform and confirm a controlled shutdown of the reactor using normal or preferred safety means,
- actuate safety-related systems that have the critical safety function of protecting the fission product barriers,
- analyze failure conditions of the normal human-system interfaces, while maintaining the plant operating condition and power level until the human-system interfaces are restored in accordance with applicable regulatory requirements,
- implement the plant's emergency operating procedures,
- bring the plant to a safe condition, and
- carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment.

The RSF minimum inventory should ensure that human-system interfaces are always available to enable the operator to accomplish the following:

- perform and confirm a reactor trip and
- place and maintain the reactor in a safe condition using the normal or preferred safety means.

Applicants should include a description of the process that will be used to identify the minimum inventory in the MCR and at the RSF within their Tier 1 information in the design control document. The description should include an in-depth description of the selection criteria, and how these functions and tasks will be identified. These systems should also conform to the Commission's rules and regulations.

Applicants also should provide a description of a method to verify the completeness of the minimum inventory for the MCR and the RSF. The description should include discussion of generic and design-specific guidelines for developing emergency operating procedures. It should also include a task analysis to bring the reactor to safe shutdown state with and without primary instrumentation. Risk-important operator actions should be described identified through the plant-specific PRA or plant-specific human reliability analysis. Critical operator actions, such as those credited in the D3 analysis, should be identified. A discussion of a full-scope simulator should also be included.

The Tier 1 information in the design control document should also include a description of the information that will be available to implement Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) to verify that the minimum inventory implementation processes are in compliance with the Commission's requirements.

A description of the minimum inventory of human-system interfaces should be included in Tier 2* information of the design control document for approval of a MCR or RSF. The completeness of the minimum inventory should be verified once the control room design is implemented (e.g., through construction of a full-scope simulator). The as-built MCR and RSF should be evaluated.

4.2.3.3 Crediting manual operator actions in diversity and defense-in-depth analyses

This position is intended to define a methodology for evaluating manual operator action as a diverse means of coping with AOOs and postulated accidents (PA) that are concurrent with a software CCF of the digital I&C protection system. It provides guidance for demonstrating how manual operator actions that can be performed inside the control room are acceptable in lieu of automated backup functions through a suitable HFE analysis.

Staff Position

Manual operator actions for AOO or PA scenarios should be based upon the Emergency Operating Procedures (EOP), and should be executed from the MCR.

In order to take credit from manual operator actions, the applicant should demonstrate that (1) the manual actions are both feasible and reliable given the time available, and (2) the ability of operators to reliably perform credited actions will be maintained for as long as the manual actions are necessary to satisfy the D3 analysis.

The time available for manual actions should be based upon the methods and criteria prescribed in BTP 7-19, and the time required for manual operator action should be estimated and validated using the guidance in in this ISG.

Credited manual operator actions and their associated interfaces (i.e., controls, displays and alarms) must be specifically addressed in the applicant's HFE program.

4.2.3.3.1 Analysis

Staff Position

The D3 analysis used for crediting manual operator actions must demonstrate that (1) the time available to perform the required manual actions is greater than the time required for operators to perform the actions, and (2) the operators can perform the actions correctly and reliably within the time available.

The time required for manual operator actions should be based on an HFE analysis of operator response time. The HFE analysis should evaluate the sequence of necessary operator actions that ultimately achieves the objectives. The applicant should establish an estimate for each individual task components, including cognitive tasks such as diagnosis.

A time margin should be added to the analyzed time. One acceptable method is to equate the time margin to the maximum recovery time for any single credible operator error.

The time available for manual operator action(s) is determined with a method consistent with the guidance of BTP 7-19. The time required for actions is based on acceptable analyses (e.g., task analysis). The sequence of manual actions requires only the interfaces available in the MCR that are demonstrated to be operable in a failure modes and effects analysis (FMEA). The estimated time response of operators should be sufficient. The initial MCR operating staff size is the same as minimum MCR staff defined in technical specifications. If manual actions require additional operator(s), the justification for timely availability of personnel should be provided. The analysis of the action sequence should capture the critical elements of the progression of the event. The analysis should identify credible operator errors, and should give an estimate of time required for recovery from any single credible error.

4.2.3.3.2 Preliminary validation

Staff Position

Preliminary validation should provide independent confirmation of the validity of the analysis for determining the time required for manual operator actions using several diverse methods. This step is not required for upgrading existing plants. Individuals who were not involved in the time analyses for manual operator actions should conduct the preliminary validation. The processes of validation and design are iterative in nature so feedback between the two groups should be used to refine the design, the procedures, and the training.

The preliminary validation activity should be conducted rigorously, and it should include a rich set of experts such as operators, system technical experts and human factors experts. The personnel involved in the process should be instructed to verify the correspondence between the documented sequence of manual operator actions and the displays and controls to be used by operators.

The preliminary validation provides an independent confirmation of the analysis used to determine the time available and the time required. The preliminary validation should be conducted by a multi-disciplinary team to confirm the analysis using several diverse methods, with a minimum of two alternative methods employed. The results should support the conclusions of the first analysis. If a successful manual action strategy cannot be achieved, diverse automation will be required.

4.2.3.3.3 Integrated system validation

Staff Position

Integrated system validation (ISV) is an evaluation using performance test to determine whether an integrated system design meets performance requirements and supports safe operation. An ISV should be conducted for the manual actions credited in the D3 analysis by using a plant-referenced simulator in real time. Response times of the operating crew should be measured using the validation guidance in NUREG-0711 during an AOO or PA with concurrent software CCF. Personnel selection should be done with both a nominal and minimum crew configurations.

Acceptable validation results will provide the basis for meeting the approval requirements. Vice versa, unacceptable results will require modification of the D3 strategy. Validating should be based on a simulator that accurately represents systems, human-system interfaces, operational transients, and the digital I&C CCFs and digital failure modes. Postulated software CCF conditions should be sufficiently represented. Simulated events for the ISV should include wide range of CCF and digital failure modes,

postulated human-system interaction failures, and operational conditions for which credited actions may be required. Mean performance time of the crew should be less than the calculated time determined by the analysis.

4.2.3.3.4 Maintaining long-term integrity of credited manual action in the D3 analysis

Staff Position

A strategy should be established to cope with variations in operator training as well as possible changes in plant design and the EOPs. This strategy should provide assurance that integrated system performance will be maintained within the bounds established by the ISV, and support the D3 analysis. Configuration and design control procedures should be established to protect the validity of credited manual actions from inadvertent system modifications.

Training programs for plant operators should emphasize the philosophy of credited manual actions in implementing the EOPs. A formal process should be implemented by which operating experience is captured and the feedback is brought to management's attention. A long-term program can be established for monitoring operator performance through periodic operator surveys or license operator training. The established programs should be structured such that corrective actions are formal, effective and timely.

5. NEXT GENERATION NUCLEAR PLANT AUTOMATION

The DOE established the NGNP program to integrate high-temperature reactor technology with the production of electricity, process heat, and hydrogen. The scope of the NGNP program includes design, construction, licensing, and operation of a full-scale prototype HTGR plant. This chapter provides a summary of the control room automation features being considered for the NGNP.

Under the DOE NGNP program, pre-conceptual design activities were completed in 2007 to define the characteristics of HTGR plants based on prismatic block and pebble bed reactor technologies. Three plant design concepts were addressed: a pebble bed reactor developed by a Westinghouse-led team and prismatic core reactors developed separately by General Atomics and AREVA. Programmatic goals moving forward included plans to complete the conceptual and preliminary design work necessary to support final design, licensing, and construction of a first-of-a-kind (FOAK) HTGR plant. In 2008, DOE, the HTGR designers, and an industry alliance of potential end users and prospective owner-operators performed a comprehensive review of industry needs and program objectives. The NGNP 2009 Status Report⁷¹ summarizes the results of this review. Important conclusions from the review include the expectation that HTGR technology will be supplied by the early 2020s, specification that a commercial plant will be constructed rather than a demonstration plant, determination that reduced outlet temperature requirements would be suitable for initial applications, and clear preference for implementation of a multi-module plant coupled to an industrial process application. Subsequently, DOE developed a Funding Opportunity Announcement to share cost in the development of up to two conceptual designs. In May 2010, General Atomics was selected to prepare a conceptual design for an FOAK plant based on a HTGR prismatic block reactor. No award has yet been made to further develop a conceptual design for the pebble bed reactor.

Wilson et al.⁵⁴ provides an overview of the pre-conceptual designs from the three development teams. In general, the NGNP plant can be represented by a nuclear heat supply system (NHSS) and an energy conversion system (ECS). The NHSS is comprised of the reactor (i.e., pressure vessel, internals, and core), shutdown and support systems, and primary helium heat transport circuit. The ECS includes those transport, power generation, and industrial process interface systems required to convert the thermal energy from the NHSS to the form(s) required to meet the demands of the HTGR application. Identified applications for the NGNP include “supplying: electricity to the grid; co-generation of steam; electricity and/or high temperature heat to industrial facilities; process heat and electricity for hydrogen production; steam or other high temperature fluid for bitumen recovery from oil sands or enhanced oil recovery from oil shale; process heat, steam and electricity for petro-chemical and refining processes; and process heat for conversion of coal to synthetic transportation fuels and hydrocarbon feedstock.”⁷²

In the available documentation on the General Atomics conceptual design of a HTGR prismatic block reactor, the main I&C systems of the NGNP are identified as the RPS, investment protection system (IPS), and PCDIS. General Atomics estimates the technology readiness level for these systems at level 4,⁷³ which corresponds to demonstrated technical feasibility and functionality at a level commensurate with bench-scale testing. The basis for this determination is the foundation drawn from the conceptual design of the control and protection architecture that was developed by General Atomics for the New Production Reactor (NPR) in the early 1990s, coupled with the further development achieved to support the GT-MHR commercial design. As indicated in the Technology Development Road Mapping report,⁷³ General Atomics is employing the “top level requirements for control room layout, plant control architecture, utilization of digital equipment and software for operator interactions, capability for multi-function plant control and safety, etc.” defined in the heritage work as the basis for the reactor control and protection approach of the NGNP conceptual design.

While design details for the I&C systems of the NGNP have not been developed, a reasonable expectation for the evolution of the NPR control and protection concept would likely lead to an automation approach similar to that employed by ALWRs. However, advanced methods have been investigated under the NGNP program to enable extended automation capabilities in support of the NGNP goals to enhance efficient operation while providing capital investment protection for key equipment, systems, and structures. In particular, the Idaho National Laboratory (INL) has been investigating resilient control as a basis for automation of the NGNP plant. The following sections describe operational requirements established for the NGNP, discuss extended functionality for resilient control of nuclear power plants, present the NGNP resilient control strategy devised by INL, and identify the expected approach to integrating NGNP with industrial processes.

5.1 Operational Requirements

From the beginning, the NGNP program has emphasize operational efficiency and optimal use of human resources. The highest-level functions and requirements were defined for NGNP to facilitate future NGNP missions, such as a demonstration-testing program, that could be conducted after the initial licensing of the plant.⁷⁴ These functions and requirements served as input to the pre-conceptual design effort and addressed a range of goals and features that include an integrated control room, optimal operational and maintenance staffing, and minimization of the need for operator action. Specifically, it was required that the NGNP design must “permit the operators to take control of the reactor and support processes from within a single integrated control room using the manual mode at any time.” In addition, the design must “minimize the need and maximize the time available for operator actions in response to plant transients, and other routine/non-routine activities during normal operations, startup, shutdown, and surveillance/testing.”

Following completion of the pre-conceptual development phase of the program, generation of more detailed systems requirements was initiated. The NGNP Systems Requirements Manual⁷⁵ establishes a requirements hierarchy intended to reflect the physical structure of the plant and its associated areas, systems, subsystems, and components for both power and industrial applications. Within this hierarchy, the NGNP and its associated industrial facility are represented in terms of five areas: Nuclear Heat Source (NHS), Heat Transport System (HTS), Power Conversion System (PCS), Balance of Plant (BOP), and Hydrogen Production System (HPS). The HPS is specific to the original mission to demonstrate hydrogen production and can be generalized to represent industrial production systems. The NHS area addresses the reactor and its shutdown and support systems, including the NHS protection and control systems. The operator interfaces and control room for operational management of the NHS are treated in this area as well. The key systems within the HTS area include the primary heat transport circuit, the secondary heat transport circuit, gas circulators, and heat exchangers and/or steam generators. The PCS area includes the turbine-generator and the steam, feedwater, and condensate systems. The BOP area includes auxiliary systems, electrical systems, plant control room systems, and safeguards and security systems.

Operational requirements are addressed in the NGNP Systems Requirements Manual. Specifically, the NGNP is required to capable of load following the interconnected ECS. In particular, the NGNP must provide for load following of electricity generation and hydrogen production (or, by extension, other industrial process heat demands). Of particular note, the NGNP must be able “to operate during loss of a secondary heat process, such as hydrogen production, and stabilize in the electricity generation phase.”

The NGNP systems requirements specify that the plant must be “capable of being controlled from a single control room.” In particular, the original high-level requirement for the capability to manually control of the reactor from a single integrated control room is retained. This requirement is applied to the specific NHS Control Room and Operator Interface System and the overall Plant Control Room System. The Plant Control Room System is specified to “provide an interface between the plant operators and each of

the necessary systems within the plant.” The I&C requirements for NGNP specify that the “main control room shall include controls for the PCS and high-temperature heat transport system” (i.e., the HTS).

The high-level requirement that the NGNP design “optimize the staffing needed for integrated operation and maintenance activities” is also supported through a maintenance requirement that provisions exist “for monitoring equipment status, configuration, and performance and for detecting and diagnosing malfunctions” to enable predictive maintenance.

While the conceptual design of a multi-unit HTGR plant by General Atomics indicates a single Operations Center, there is no clarification given in the requirements or available design information to indicate anything other than co-located but separate operator interface systems for each reactor. Thus, without further design details, the expectation is that separate regions of the Operations Center will be dedicated to the control of individual reactors and support systems.

5.2 Resilient Functionality

As discussed in Section 2.1.3, resilient control expands the basic functions customary for a traditional control system to enable the adaptive capacity to respond to threats and support the necessary level of state awareness to recognize or even anticipate disturbances. In support of the NGNP program, Stevens⁶ performed control system functional analysis to identify gaps in functionality between a traditional control system and a resilient control system in the context of HTGR operational control. It was noted that resilience treats the multiple aspects of control system performance in a holistic fashion. Thus, security is considered in addition to stability and efficiency. In addition, human performance and complex interdependences are addressed in control system requirements. Consequently, a resilient control system can adapt to situations or respond to threats while remaining operational with at least a minimum acceptable functionality. Examples of resilient functionality include:

- detection of degradation and failures through process diagnostics,
- substitution of estimated or synthesized parameters to correct invalid data,
- switching among alternate control modes and strategies to maintain desired performance in the presence of significant failure events,
- limitation of operation to avoid stressful conditions and protect high value components, and
- adaptation of system architecture to mitigate the impact of failures or intrusions.

For an HTGR application, a resilient control system can accommodate loss of signal events by employing inferred or analytic operating parameters or can provide for graceful degradation of hierarchical control (e.g., revert to isolated, single-loop controllers) in the face of a cyber attack.

The extended functionality provided through resilient design is intended to enhance the capability of the control system to monitor the plant and its systems, manage and process data, provide networked whole-system communications, and manage control processes in a secure, proactive, and adaptive manner. Based on the gap analysis conducted by Stevens, the resilient functions that supplement traditional control functions are illustrated in Fig. 19.

The resilient control treatment of cyber and physical security in system monitoring involves use of data authentication and diversity of indication within an embedded security structure that imposes layers of detection fidelity for systems and communications. Enhanced process stability and efficiency is achieved through diagnosis, and even prognosis, of deviations from expected behavior and through local optimization of subsystems within an integrated hierarchical functional architecture. Consideration of nonproliferation and safeguards within the resilient control functionality includes timely knowledge of the location and movement of special materials coupled with real-time awareness of plant activities.

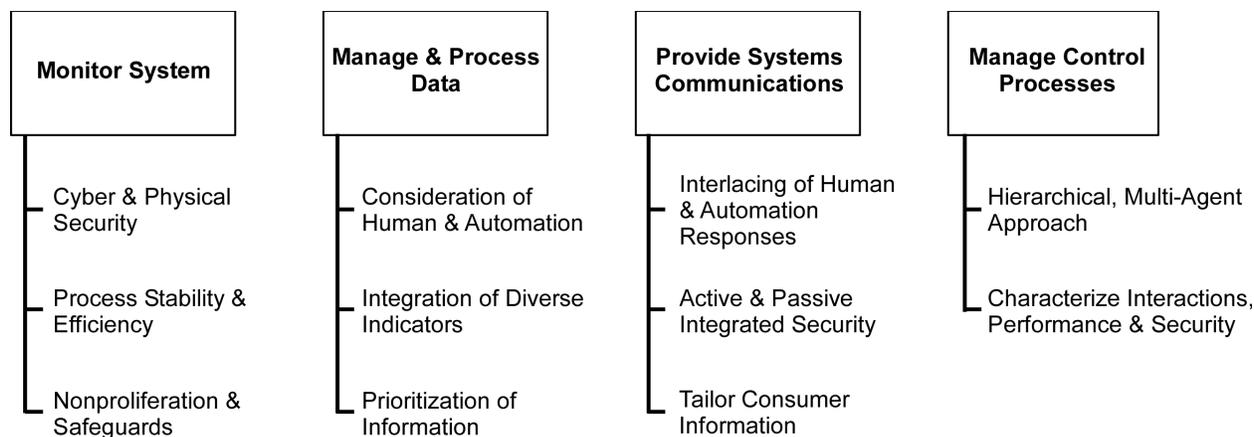


Fig. 19. Extended functionality provided by resilient control.

The management and processing of data within a resilient control approach includes consideration of human information needs and involvement in the determination of control and display functions. As part of this extended functionality, diverse indicators of plant and system conditions, including cyber security status, are integrated to establish a more comprehensive state awareness capability. In prioritizing information, data can be fused and thereby reduced to necessary information to improve state characterization and aid in identifying event causes. Through provision of this increased knowledge, real-time predictive models can be kept current to facilitate anticipation of future states and events.

In providing communications, a resilient control system addresses internal and external interaction with automation and human operators. In doing so, human responses are integrated into the command and control functionality through continuous measurement of the operator interaction, monitoring of performance, and adaptation based on the user defined roles and responsibilities. Security is embedded in the control system hierarchy to provide both passive and active mechanisms to supplement plant-wide IT security processes. Examples include layered active network detection and response mechanisms for cyber threats and passive features such as atypical architectures and randomized system attributes. The adaptive nature of the systems communications functionality for resilient controls can permit user definition of information access and feedback (i.e., the display content and navigation interface can be adapted to the individual user). This capability supports optimal reaction to enable effective cognitive decision making for human-automation collaboration.

A resilient control system manages control processes through a flexible supervisory control structure based on a hierarchical architecture in which multiple semi-autonomous tasks (i.e., agents) are employed throughout various layers of the distributed control system. The distribution of system resources with oversight of semi-autonomous functions permits flexibility in operation. Specifically, task execution can be validated at higher levels of the hierarchy and tasks can be prioritized based on situation, load, and measured performance. Predictive models can facilitate anticipation of future states so that the resilient control system can proactively adapt to minimize threats and mitigate the potential for disturbances. The promotion of state awareness, based on characterization of conditions such as system interactions, performance, and security, permits global optimization of the resilient control system to help ensure that operational and safety goals are satisfied under all situations.

5.3 Automation Strategy

A strategy for automating NGNP control and operations based on resilient control has been recommended by INL.⁸ The motivation for adopting resilient control is economic and practical. The basis for the strategy is that control systems can incorporate increasing degrees of resilience to enable higher levels of

performance, quicker response to disturbances, increased operational efficiency, and improved protection of investment and public health. Specifically, resiliency in automation of plant operations facilitates “extending the longevity of the equipment, making operations more efficient, better utilizing existing operators and support staff, increasing stability when coupling with multiple processes, and integrating process measures, such as cyber security and process efficiency.”

In advocating resilient controls for NGNP, INL notes that systems, structures, and components for HTGR plants represent significant capital investments that are susceptible to reduction in useful life due to fatigue and thermal cycling. An automation approach that promotes stable operation and minimizes upsets can contribute to preserving component health. Also, perturbations in the process heat applications of interconnected industrial facilities can introduce transients through dynamic coupling with the NHSS. Because resilient control methods can account for complex system interactions, the means of advanced automation can improve efficiency, enhance performance, and mitigate the propagation of perturbations.

Stevens et al.⁸ present several notional scenarios to discuss the prospective approach to applying resilient controls to NGNP. These scenarios indicate how operation of NGNP could be enhanced through the use of resilient control systems that can perform higher-level management functions, respond more quickly to disturbances, provide for optimal operations, and contribute to safety. Specific scenarios include treatment of undetected changes, inference of unmeasured parameters, accommodation of product stream transients, and the impact of a cyber attack.

One scenario involves undetected changes or lack of plant condition awareness. Given the high temperature operation expected of NGNP, significant sensor drift, or even outright failure, should be anticipated. Such conditions can impact the performance of automatic control functions that provide investment protection to critical, high-cost equipment. The prospective benefits of resilient control can be realized by way of perception of sensor failure through surveillance, response through operator notification, anticipation of effect through simulation, and adaption of automatic control to permit continued operation. The suggested means of adaption involves substitution of the invalid signals by inferred parameters based on other validated measurements and operational models.

Inference of parameters that are not directly measured is addressed in another scenario. The specific example involves the determination of the impact of fouling in once-through steam generator tubes. The goal would be to infer the boundaries for secondary coolant phase transitions (i.e., subcooled water to boiling water to saturated steam to superheated steam) and thereby enable appropriate operational conditions to be maintained in the tubes to ensure the integrity of key welds (i.e., control conditions such that the welds remain within the superheated steam region during operation, as intended by design). The resilient control approach begins with perception of the presence, degree, and impact of fouling. Estimation of the transition boundaries based on changes in available sensor data and modeled behavior (i.e., employ data fusion techniques to generate analytic data) permits anticipation of the progression of the fouling phenomenon and its operational consequences (i.e., aging and degradation of the welds). The resilient control response can include notification of the evolving conditions to operators and relevant plant personnel (e.g., maintenance staff) while prospective adaption of control can include changes to control settings to address the fouling effect and optimize steam generation operation.

An additional scenario encompasses transients induced by end-use/product-steam transients. Examples of upsets and conditions related to end-use effects include frequent load-following demands, rapid heat removal changes (e.g., isolation of the heat transfer system between the nuclear plant and process-heat industrial facility), and loss-of-heat-sink events. Without control system mitigation, these events could lead to undesired thermal cycling and potentially significant thermal shock to critical equipment (e.g., steam generators, intermediate heat exchangers, helium circulators). The consequence of these types of unmitigated events could be a reduction of equipment life or even damage. A resilient control design is based on a comprehensive treatment of the whole plant and its coupled processes to promote efficiency and stability. Advanced process surveillance and event detection enable a resilient control system to

perceive operational challenges. The provision of data-driven diagnostics and condition estimators in conjunction with fatigue-life usage models permits the impact of events to be anticipated. The resilient control response can be to mitigate the likelihood and severity of thermal excursions through proactive control measures (e.g., feedforward control, reactor runback) and to adapt the operational schemes to limit stress on critical components.

Another scenario deals with the impact of a cyber attack, in which it is presumed that the overlaid security features of the plant IT infrastructure are breached or bypassed. The consequences of such attacks (e.g., malicious or accidental actions of either external or internal origin) could involve unauthorized control maneuvers that damage equipment or put the plant in an unexpected operational state, falsified data that misrepresents the plant status and corrupts the situational awareness of plant operators, or denial of service that inhibits or prevents corrective manual operational actions. The perceptive capability of resilient control involves recognition that signals are false (e.g., signal validation by checking consistency with other measurements) and control actions are not valid (e.g., command validation based on historical knowledge or cross comparison). Model-based prediction can serve as another element of command validation by anticipating future plant states and determining that a control trajectory is harmful. The response of a resilient control system to cyber attack (or operator error) could be to alert the operator and possibly initiate investment protection limitation functions for extreme cases. The resilient control system can also adapt to thwart an attack by substituting validated signals or switching to unaffected control algorithms. In addition to data fusion and validation, it is noted that randomization of communications traffic and other SCADA-specific defensive measures can be employed to minimize vulnerability to attack.

Additional scenarios are described by Stevens et al. to further illustrate the potential benefits of a resilient control approach. These scenarios involve malicious corruption of safeguards/nonproliferation information as part of a cyber intrusion, disruptions of electrical power for operator workstations during a loss of off-site power event combined with failure of backup power, and steam generator leaks resulting from component degradation. In each case, a discussion is provided to highlight capabilities that can be provided through resilient design to address threats and vulnerabilities. In particular, the holistic treatment of plant management functions, including safeguards and cyber security, is cited as a specific benefit of resilient control design. The provision of advanced fault diagnosis and detection capabilities, coupled with adaptive control and state awareness alerts, enable resilience to be embedded in the control system to accommodate failures and resolve potential events. Thus, the comprehensive capabilities supported by resilient design allow the implementation of multiple layers of protection, detection, and response to events and disturbances.

The INL analysis of the application of resilient controls to HTGRs, as illustrated by the notional scenarios, indicates the need for additional research to advance the state-of-the-practice to a level suitable for implementation in an automation strategy for NGNP. In particular, Stevens et al. recommend research in areas of particular interest to HTGR investment protection, including:

- cyber and physical security,
- process stability and efficiency,
- integration of diverse indicators, and
- interlacing of human and automatic responses.

Resilient controls should be seen as an emerging technology and its use for NGNP would, of necessity, be limited to those capabilities that can be demonstrated with an acceptable technology readiness level. The expectation is that the NGNP automation approach would likely involve some resilient features and functions but would not adopt a comprehensive resilient control strategy.

5.4 Integration with Industrial Processes

As specified for the NGNP program, the approach to incorporate industrial applications within the product stream of an HTGR plant is to treat the nuclear facility and industrial facility as separate.⁷² Basically, an interface component is provided in the design to enable the transfer of high temperature fluids from an HTGR to an industrial facility via a dedicated transfer system. The interface component can be a process heat exchanger, a process heat exchange reformer, a process steam generator, or a heat transfer line, depending on the plant design.⁷⁶ In each case, the interface component transfers heat from the secondary heat transport circuit of the HTGR to a tertiary heat transport circuit connected to the industrial process unit(s). In effect, the interface component provides for heat transfer from the secondary coolant circuit of the HTGR to the heat transport medium (e.g., water, helium, liquid salts) of the transfer system. The function of the transfer system is to provide high-temperature steam, liquid, or gas to an offsite industrial facility (i.e., customer) and return the condensate or makeup fluid (or gas) to the HTGR interface component. The conceptual design being developed by General Atomic employs a steam-to-steam heat exchanger to serve as the interface component to the tertiary transfer system.⁷³ For example, the transfer system can consist of pipelines that transfer steam to an industrial facility and return feedwater to the interfacing heat exchanger.

High-level design and interface requirements have been developed for the transfer system that would interconnect the NGNP and industrial facilities.⁷² For the process heat portion (i.e., industrial facility) of an ECS to be excluded from the nuclear facility scope, it must be located outside the HTGR protected area boundary and be operated from a separate control room. In addition, the ECS must be separated from the nuclear facility by a transfer system with interface criteria that serve to ensure that the HTGR is not dependent on, or adversely affected by, events that occur within the separate industrial facility. In effect, failures or transients in the transfer system or the industrial facility must not inhibit safety-related systems and components in the nuclear facility from functioning as required during all operational conditions. Consequently, no portion of the transfer system should be required to perform any safety or safe shutdown function, or be relied upon as a supporting system to a safety-related system. To contribute to operational stability and ensure safety, the transfer system should have monitoring capabilities to detect disturbances and isolate the industrial facility during transients and accidents, if required by the nuclear facility safety analysis.

6. KEY ISSUES FOR HIGHLY AUTOMATED CONTROL ROOM DESIGNS IN VHTRS

7. REFERENCES

1. S. M. Mitchell and M. S., Mannan, "Designing Resilient Engineered Systems," *Chemical Engineering Progress*, **102**(4), pp. 39–45 (April 2006).
2. C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient Control Systems: Next Generation Design Research," *2nd Conference on Human System Interactions*, Catania, Italy, pp. 632–636 (May 2009).
3. J. Eisenhauer, P. Donnelly, M. Ellis, and M. O'Brien, *Roadmap to Secure Control Systems in the Energy Sector*, prepared for the Department of Energy by Energetics, Columbia, MD, January 2006.
4. C. G. Rieger, "Notional Examples and Benchmark Aspects of a Resilient Control System," *3rd International Symposium on Resilient Control Systems*, Idaho National Laboratory, Idaho Falls, ID, pp. 64–71 (August 2010).
5. *Agent Technology Green Paper*, Agent Working Group, OMG Document ec/2000-08-01, Version 1.0, Object Management Group, Needham, MA, August 2000.
6. L. M. Stevens, *Next Generation Nuclear Plant Resilient Control System Functional Analysis*, INL/EXT-10-19359, Idaho National Laboratory, Idaho Falls, ID, July 2010.
7. E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*, Ashgate Publishing, Aldershot Hampshire, UK, 2006.
8. L. M. Stevens, C. G. Rieger, and W. C. Phoenix, *HTGR Resilient Control System Strategy*, INL/EXT-10-19645, Idaho National Laboratory, Idaho Falls, ID, September 2010.
9. McAfee® Foundstone® Professional Services and McAfee Labs™, "Global Energy Cyberattacks: Night Dragon," February 10, 2011, from website <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>.
10. Nicolas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," Version 1.4, February 2011, from website http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
11. D. Kuipers and M. Fabro, "Control Systems Cyber Security: Defense in Depth Strategies," Idaho National Laboratory, May, 2006, from website <http://inl.gov/technicalpublications/Documents/3375141.pdf>.
12. U.S. Department of Homeland Security, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009, from website https://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf.
13. M. L. Fracker, *Measures of Situation Awareness: An Experimental Evaluation*, Report No. AL-TR-1991-0127, Armstrong Laboratories, Wright-Patterson Air Force Base, OH, 1991.
14. P. J. Antsaklis and K. M. Passino, "An Introduction to Intelligent Autonomous Control Systems with High Degrees of Autonomy," *An Introduction to Intelligent and Autonomous Control*, Kluwer Academic Publishers, Boston, pp. 1-26, 1992.
15. P. J. Antsaklis, "Intelligent Learning Control," *IEEE Control System Magazine*, pp. 5–7 (June 1995).
16. P. J. Antsaklis and J. C. Kantor, "Intelligent Control for High Autonomy Process Control Systems," *Proceedings of the First International Conference on Intelligent Systems in Process Engineering*, American Institute of Chemical Engineers, Snowmass, Colorado, pp. 37–46, July 1995.
17. K. J. Astrom, "Toward Intelligent Control," *IEEE Control System Magazine*, pp. 60–64 (April 1989).
18. K. J. Astrom, "Where is the Intelligence in Intelligent Control?" *IEEE Control System Magazine*, pp. 37–39 (June 1991).

19. H. Basher and J. Neal, *Autonomous Control of Nuclear Power Plants*, ORNL/TM-2003/252, Oak Ridge National Laboratory, October 2003.
20. T. R. Chaudhuri, L. G. C. Hamey, and R. D. Bell, "From Conventional to Autonomous Intelligent Methods," *IEEE Control System Magazine*, pp. 78–84 (October 1996).
21. K. M. Passino, "Bridging the Gap Between Conventional and Intelligent Control for Autonomous Systems," *IEEE Control System Magazine*, pp. 12–18 (June 1993).
22. K. M. Passino, "Intelligent Control for Autonomous Systems," *IEEE Spectrum*, pp. 55–62 (June 1995).
23. K. M. Passino and U. Ozguner, "Intelligent Control: From Theory to Application," *IEEE Expert*, **11**(2), pp. 28–30 (1996).
24. B. P. Zeigler and S. Chi, "Model Based Architecture Concepts for Autonomous Control Systems Design and Simulation," *An Introduction to Intelligent and Autonomous Control*, Kluwer Academic Publishers, Boston, pp. 57–78 (1992).
25. R. T. Wood, "Investigation of Autonomous Control for the Jupiter Icy Moons Orbiter," *Space Nuclear Conference '07*, Boston, MA, June 2007.
26. B. R. Upadhyaya et al., *Autonomous Control of Space Reactor Systems*, DE-FG07-04ID14589/UTNE-06, University of Tennessee, 2007.
27. R. J. Doyle, "Spacecraft Autonomy and the Missions of Exploration," *IEEE Intelligent Systems*, pp. 36–44 (September/October 1998).
28. A. G. Mishkin et al., "Experiences with Operation and Autonomy of the Mars Pathfinder Microrover," *Proceedings of the 1998 IEEE Aerospace Conference*, Institute of Electrical and Electronics Engineers, Aspen, CO., pp. 337–351 (March 1998).
29. R. Volpe et al., "The CLARAty Architecture for Robotic Autonomy," *Proceedings of the 2001 IEEE Aerospace Conference*, Vol. 1, Institute of Electrical and Electronics Engineers, Big Sky, MT, pp. 121–131 (March 2001).
30. M. D. Rayman, P. Varghese, D. H. Lehman, and L. L. Livesay, "Results from the Deep Space 1 Technology Validation Mission," *Proceedings of the 50th International Astronautical Congress*, American Institute of Aeronautics and Astronautics, *Acta Astronautica*, **47**, pp. 475–488 (1999).
31. R. Alami et al., "An Architecture for Autonomy," *International Journal of Robotics Research*, **17**(4), pp. 315–337 (1998).
32. E. Gat, "Three-Layer Architectures," *Artificial Intelligence and Mobile Robots: Case Studies of Successful Robot Systems*, D. Kortenkamp et al. (Eds.), MIT Press, Cambridge, MA, pp. 195–210 (1998).
33. N. Muscettola et al., "On-Board Planning for New Millennium Deep Space One Autonomy," *Proceedings of IEEE Aerospace Conference, Vol. 1*, Institute of Electrical and Electronics Engineers, Snowmass, CO, pp. 303–318 (February 1997).
34. R. Volpe, "Rover Functional Autonomy Development for the Mars Mobile Science Laboratory," *Proceedings of the 2003 IEEE Aerospace Conference, Vol. 2*, Institute of Electrical and Electronics Engineers, Big Sky, MT, pp. 643–652 (March 2003).
35. *Testing and Installation of a BWR Digital Feedwater Control System*, EPRI NP-5524, Electric Power Research Institute, December 1987.
36. *Proceedings: Distributed Digital Systems, Plant Process Computers, and Networks*, EPRI TR-104913, Electric Power Research Institute, March 1995.
37. *Proceedings of the 1993 ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, American Nuclear Society, Oak Ridge, TN, April 1993.

38. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 96)*, Vols. 1 and 2, American Nuclear Society, Penn State University, PA, May 1996.
39. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, American Nuclear Society, Washington, DC, November 2000.
40. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2004)*, American Nuclear Society, Columbus, OH, September 2004.
41. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2006)*, American Nuclear Society, Albuquerque, NM, November 2006.
42. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2009)*, American Nuclear Society, Knoxville, TN, April 2009.
43. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2010)*, American Nuclear Society, Las Vegas, Nevada, November 2010.
44. R. W. Winks, T. L., Wilson, and M. Amick, "B&W PWR Advanced Control System Algorithm Development," *Proceedings: Advanced Digital Computers, Controls, and Automation Technologies for Power Plants*, EPRI TR-100804, Electric Power Research Institute, Palo Alto, CA, 1992.
45. D. E. Taylor, "Oconee Nuclear Station Integrated Control System (ICS) Replacement Project," *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, American Nuclear Society, Washington, DC, November 2000.
46. P. J. Otaduy, C. R. Brittain, L. A. Rovere, and N. B. Gove, *Supervisory Control Concepts for a Power Block with Three Reactors and a Common Turbine-Generator*, ORNL-TM-11483, Oak Ridge National Laboratory, Oak Ridge TN, 1990.
47. P. J. Otaduy, C. R. Brittain, L. A. Rovere, and N. B. Gove, "Supervisory Control Conceptual Design and Testing in ORNL's Advanced Controls Research Facility," *AI91: Frontiers in Innovative Computing for the Nuclear Industry, Vol. 1*, Jackson Hole, WY, pp. 170–179 (September 1991).
48. R. T. Wood et al., "Autonomous Control for Generation IV Nuclear Plants," *Proceedings of the 14th Pacific Basin Nuclear Conference*, American Nuclear Society, Honolulu, HI, pp. 517–522 (March 2004).
49. International Atomic Energy Agency, *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook*, Technical Reports Series No. 387, IAEA, Vienna (1999).
50. G. Kaiser et al., *Reaktorinstrumentierung, Prozeßmeßtechnik und Leistungsregelung im Kernkraftwerk (Reactor Instrumentation, Process Measurement Technology, and Output Control in the Nuclear Power Plant)*, VDE-Verlag GmbH, Berlin-Offenbach (1983).
51. R. Fairley and R. Thayer, "The Concept of Operations: The Bridge from Operational Requirements to Technical Specifications," *Annals of Software Engineering* **3**, pp. 417–432 (1977).
52. J. O'Hara, J. Higgins, J. Persensky, P. Lewis, and J. Bongarra, *Human Factors Engineering Program Review Model*, NUREG-0711, Rev. 2, U.S. Nuclear Regulatory Commission, Washington, DC, February 2004.

53. J. O'Hara, J. Higgins, W. Brown, and R. Fink, *Human Performance Issues in New Nuclear Power Plants: Detailed Analyses*, BNL Technical Report No: 79947-2008, Brookhaven National Laboratory, Upton, NY, 2008.
54. T. L. Wilson, Jr. et al., *Task I—Control and Protection Systems in VHTRs for Process Heat Applications*, LTR/NRC/RES/2010-001, Oak Ridge National Laboratory, September 2010.
55. D. L. Moses, *Technical Evaluation Report for the Review of Fort St. Vrain Technical Specification Upgrade Program*, Fort St. Vrain Nuclear Generating Station, Docket 50-267, July 1988.
56. *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, NUREG/CR-6839 (ORNL/TM-2003/223), Oak Ridge National Laboratory, 2003.
57. E. Sauer (Ed.), *AVR-Experimental High-Temperature Reactor—21 Years of Successful Operation for a Future Energy Technology*, Association of German Engineers (VDI), The Society for Energy Technologies, VDI-Verlag GmbH, Düsseldorf.
58. *Design of High Temperature Engineering Test Reactor (HTTR)*, JAERI 1332, 1994, http://httr.jaea.go.jp/research/jaeri_1332.html.
59. Saito et al., "Instrumentation and Control System Design," *Nuclear Engineering and Design*, **233**, pp. 125–133 (2004).
60. Z. Wu, D. Lin, and D. Zhong, "The Design Features of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 25–32 (2002).
61. Z. Shuoping, H. Shouying, Z. Meisheng, and L. Shengquiang, "Thermal Hydraulic Instrumentation System of the HTR-10," *Nuclear Engineering and Design*, **218**, pp. 199–208 (2002).
62. *Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology*, IAEA-TECDOC-1198, International Atomic Energy Agency, February 2001.
63. *Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, December 1995.
64. *Preliminary Safety Information Document for the Standard MHTGR*, HTGR-86-024, Vol. 3, Section 7.3.
65. *Conceptual Design Summary Report Modular HTGR Plant*, DOE-HTGR-87-092.
66. IEEE 603, "Standard Criteria for Safety Systems for Nuclear Power Generating Systems," Institute of Electrical and Electronics Engineers, 1991.
67. IEEE 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Institute of Electrical and Electronics Engineers, 2003.
68. G. G. Preckshot, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, U.S. Nuclear Regulatory Commission, December 1994.
69. J. O'Hara, W. Brown, P. Lewis, and J. Persensky, *Human System Interface Design Review Guidelines*, NUREG-0700, Rev.2, U.S. Nuclear Regulatory Commission, Washington, DC, May 2002.
70. NUREG-0899, "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, Washington, DC, August 1982.
71. *Next Generation Nuclear Plant Project 2009 Status Report*, INL/EXT-09-17505, Idaho National Laboratory, Idaho Falls, ID, May 2010.
72. *NGNP Nuclear-Industrial Facility and Design Certification Boundaries*, INL/EXT-11-21605, Idaho National Laboratory, Idaho Falls, ID, July 2011.
73. *Technology Development Road Mapping Report for NGNP with 750°C Reactor Outlet Helium Temperature*, PC-000586, General Atomics, May 2009.

74. *Next Generation Nuclear Plant High-Level Functions and Requirements*, INEEL/EXT-03-01163, Idaho National Laboratory, Idaho Falls, ID, September 2003.
75. *NGNP System Requirements Manual*, INL/EXT-07-12999, Rev. 3, Idaho National Laboratory, Idaho Falls, ID, September 2009.
76. *Reactor User Interface Technology Development Roadmaps for a High Temperature Gas-cooled Reactor Outlet Temperature of 750°C*, INL/EXT-10-20460, Idaho National Laboratory, Idaho Falls, ID, December 2010.

DRAFT

LTR/NRC/RES/2011-003

Draft Letter Report

**TASK 3. MODELS FOR CONTROL AND
PROTECTION SYSTEM DESIGNS IN VHTRS**

T. L. Wilson, Jr., and S. M. Cetiner
Oak Ridge National Laboratory

Technical Monitor: Y. Yang, NRC RES
Principal Investigator: T. L. Wilson, Jr., ORNL

May 2011

Prepared for the
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

DRAFT

CONTENTS

	Page
LIST OF FIGURES	vii
LIST OF TABLES	ix
1. INTRODUCTION	1
2. TRANSIENT CLASSES	3
2.1 Normal Operating Conditions	3
2.1.1 Load follow	4
2.1.2 Maximum ramp	4
2.1.3 Step change	4
2.2 Abnormal Operating Occurrences	4
2.2.1 Turbine trip	4
2.2.2 Load rejection	5
2.2.3 Loss of heat sink	5
2.2.4 I&C system failures	5
2.3 Design Basis Accidents	6
2.3.1 Pressurized loss of forced circulation (P-LOFC)	6
2.3.2 Depressurized loss of forced circulation (D-LOFC)	6
2.3.3 Anticipated transient without scram (ATWS)	7
3. GENERAL MODELING CHARACTERISTICS OF VHTR STRUCTURES, SYSTEMS, AND COMPONENTS	8
3.1 Plant Design Options	9
3.2 Common Structures, Systems, and Components	11
3.3 Code Phenomena and Component Modeling	11
3.4 Reactor Vessel Cavity and Core Internals	11
3.4.1 Reactor core	12
3.5 Shutdown Cooling System	18
3.5.2 Maintaining water coolant inventory	19
3.5.3 Steam/water ingress into primary loop	20
3.6 Intermediate Heat Exchanger	20
3.7 Turbomachinery	20
3.7.1 Modeling equations	21
3.7.2 Performance maps model for head and efficiency of gas turbines and compressors	21
3.7.3 Conservation equations for the fluid	26
3.7.4 Quasi-steady approximations	30
3.7.5 Conservation of angular momentum equation for shaft speed	32

3.7.6	Electric motor compressor shaft model.....	34
3.7.7	Compressor stall or surge.....	34
3.7.8	Steam turbine models.....	34
3.8	Steam Generator.....	34
3.8.1	Tube heat transfer.....	35
3.8.2	Tube leak model for water ingress from water into gas side.....	36
3.9	Instrumentation System.....	36
3.10	Control System.....	37
3.11	Confinement and Containment.....	39
3.12	Cavity.....	39
3.12.1	Gas composition and temperature.....	40
3.12.2	Gas stratification and mixing.....	40
3.12.3	Air in-leakage.....	40
3.12.4	Structural performance.....	40
3.12.5	Filters.....	40
3.12.6	Dust and aerosol.....	40
3.12.7	Gas species retention.....	41
3.12.8	Holdup.....	41
4.	CHARACTERIZATION OF SELECT CODES FOR VHTR CONTROL SYSTEM ANALYSES.....	41
4.1	RELAP5-3D.....	41
4.1.1	Introduction.....	41
4.2	RELAP5 Transient Overview.....	44
4.3	RELAP5 Modeling Overview.....	46
4.3.1	Hydrodynamic model.....	46
4.3.2	Heat structures model.....	47
4.3.3	Radiation enclosure model.....	47
4.3.4	Reactor kinetics model.....	48
4.3.5	Component models.....	49
4.4	Numerical Solution Scheme.....	61
4.4.1	Numerical solution of radionuclide transport equations.....	62
4.5	Control System Simulation.....	62
4.5.1	Arithmetic control components.....	63
4.5.2	Differentiation control components.....	65
4.5.3	Proportional-integral control component.....	66
4.5.4	Lag control component.....	66
4.5.5	Lead-lag control component.....	66
4.5.6	Shaft component.....	66

4.5.7	Inverse kinetics component	67
4.5.8	Trips and Control Variables	67
4.5.9	Simulating equipment control systems.....	67
4.5.10	Simulating “lumped node” systems	69
4.5.11	Enhancing the RELAP5-3D [®] model boundary conditions.....	69
4.6	Applications of RELAP5-3D/ATHENA for Modeling of the HTGR.....	69
4.6.1	High- and low-pressure conduction cool-down accident analyses of the prismatic NGNP HTGR	69
4.7	Necessary Features for Integrated Systems Simulation of the Reactor and Balance of the Plant for Control Systems Analysis Purposes	77
4.8	MELCOR	78
4.9	STRUCTURE OF MELCOR.....	79
4.9.1	Control Function (CF) package.....	82
4.9.2	Core (COR) package	84
4.9.3	Control volume hydrodynamics (CVH) package	86
4.9.4	Flow Path (FL) package	86
4.9.5	Heat Structure (HS) package.....	88
4.9.6	Material Properties (MP) package.....	89
4.10	MELCOR-H2 Extensions for VHTR Plant Models.....	89
4.11	Modeling the Secondary Loop and the Balance of Plant in MELCOR.....	92
4.11.1	Gas turbine, compressor, and heat transfer models.....	92
4.11.2	Turbine modeling equations.....	96
4.11.3	Compressor model.....	103
4.11.4	Transient model of a general purpose heat exchanger.	109
4.11.5	Hydrogen production modeling.....	118
4.11.6	Fuel temperature model.....	131
4.11.7	Implementation of reactor kinetics in MELCOR-H2	133
4.12	VHTR Core Models in MELCOR-H2	137
4.12.1	Modeling the pebble bed reactor core with MELCOR-H2	137
4.12.2	Modeling the prismatic VHTR core with MELCOR	138
5.	SUMMARY AND CONCLUSIONS	140
5.1	General Observations	140
5.2	Observations on RELAP5	141
5.3	Observations on MELCOR	142
6.	REFERENCES	144
	APPENDIX A: PRESSURE LOSS COEFFICIENT IN TURBINE BLADES.....	A-1
	APPENDIX B: PRESSURE LOSS COEFFICIENT IN COMPRESSOR BLADES	B-1

LIST OF FIGURES

Figure		Page
1	Possible configuration option—direct electrical cycle and a parallel IHX.....	9
2	Alternate configuration option—indirect electrical cycle and a parallel SHX	10
3	Basic layout and some design parameters of the GT-MHR reactor and core internals	12
4	Proposed layout of the SCS in the bottom portion of the reactor vessel underneath the metallic core support floor	18
5	Functional diagram of the SCS—single loop per reactor module	19
6	MGR-GT compressor performance maps	24
7	MGR-GT turbine performance maps.....	25
8	General control volume with shaft work	26
9	Mathematical representation of signals in a sensing element: $f(t)$ is the process variable of interest, $g(t)$ represents the internal dynamics of the sensor, and $h(t)$ is the measured sensor signal, which is the convolution of $f(t)$ and $g(t)$	36
10	Response of a first-order system to a step input signal— τ is called the time constant	37
11	A schematic representation of the control system	37
12	An example implementation of a PID control system simulation	38
13	Top-level block diagram of modules that show the component functional relationship for transient calculations in RELAP5-3D [®]	45
14	Block diagram structure of subroutines for transient and steady state calculations	45
15	Graphical representation of a one-dimensional branch	49
16	Typical separator volume and junctions	50
17	Schematic of mixing junctions	51
18	Four-quadrant curves that represent typical pump characteristics.....	52
19	Graphical representation of a turbine stage group with idealized flow between points 1 and 2.....	53
20	A graphical depiction of an inertial valve.....	55
21	Schematic of a typical relief valve in the partially open position.....	55
22	Typical (a) cylindrical and (b) spherical accumulator modeled in RELAP5-3D [®] . ¹⁸	56
23	Schematic of the ECC mixer component model.....	58
24	A nodalization example of the pressurizer model	59
25	Schematic of a feedwater heater component as modeled in RELAP5-3D [®]	60
26	Nodalization scheme for difference equations.....	61
27	(a) Heat transfer interactions in the RELAP5-3D/ATHENA model for the NGNP VHTR; (b) radiation paths as modeled in RELAP5-3D between the pressure vessel and the RCCS	69
28	(a) Hydraulic nodalization of the VHTR pressure vessel; (b) nodalization of the reactor cavity	70
29	Integrated layout of the primary and secondary heat transport systems and RVACS.....	72
30	Isometric view of the 600-MW(t) power conversion system layout	73
31	Thermodynamic state points of the S-CO ₂ cycle for the 600-MW(t) power conversion system design.....	74

32	RELAP5 nodalization structure of the PCS.....	76
33	Code structure of MELCOR.....	80
34	Flow path definition.....	87
35	Heat structure in a control volume.....	89
36	Schematic of a nuclear reactor that is fully coupled to a thermochemical sulfur-iodine cycle and the power conversion system.....	90
37	Snapshot of the graphical user interface of MELCOR-H2.....	91
38	Schematic of a multistage axial-flow turbine	97
39	Velocity triangles for turbine rotor blades.....	98
40	Schematic of a multistage axial-flow compressor	104
41	Velocity triangles of compressor rotor blades	105
42	Cell and flow path schematic for heat exchanger	111
43	Laminar Nusselt number for constant heat flux boundary condition	113
44	Darcy friction factor for smooth surfaces.....	115
45	Process schematic for sulfur-iodine process.....	119
46	Schematic of reaction chamber showing input and output variables.....	120
47	Schematic for the simplified hybrid sulfur-iodine process.....	128
48	Nodalization scheme for PBMR model in MELCOR	138
49	Nodalization of the simplified NGNP VHTR model in MELCOR-H2.....	139
A-1	Profile loss coefficient for ($\beta_1 = 0$ and $t_{max}/C = 0.2$).....	A-3
A-2	Profile loss coefficient for ($\beta_1 = \phi_2$ and $t_{max}/C = 0.2$).....	A-4
A-3	Inlet Mach number ratio for turbine blades	A-6
A-4	Loss coefficient for trailing edge losses, based on Kacker and Okapuu	A-8
A-5	Off-design incidence correction factor for turbine blades	A-10
A-6	Stalling incidence angle for S/C=0.75	A-11
B-1	Boundary layer momentum thickness at blade outlet, $Re_1=10^6$	B-3
B-2	Correction factor for effect of Mach number on boundary-layer momentum thickness	B-4
B-3	Correction factor for effect of flow area contraction on boundary layer momentum thickness	B-5
B-4	Off-design incidence correction factor for compressor blades	B-7

LIST OF TABLES

Table		Page
1	Summary of RELAP5-3D control variables.....	68
2	Packages contained in MELCOR.....	80
3	Reaction rate parameters.....	127
4	Padé approximation of the exponential function	136

Task 3. Models for Control and Protection System Designs in VHTRs

DRAFT LETTER REPORT

T. L. Wilson, Jr., and S. M. Cetiner
Oak Ridge National Laboratory

May 2011

1. INTRODUCTION

This document discusses High-Temperature Gas Reactor (HTGR) system modeling capabilities that might be needed for various types of analyses and support activities performed by the NRC staff in licensing Very High-Temperature Reactors (VHTRs). Activities may include reviews of licensing applications or development of regulations and guidance for those reviews. The goal is to survey simulation codes and potential I&C applications so that decisions about code development can be made in a timely fashion before the need for an analysis presents itself and then expedience determines the modeling choice. First and foremost, an I&C modeling code for the U.S. Nuclear Regulatory Commission (NRC) would provide the capability to perform independent confirmation of results presented by applicants in licensing submittals. In addition, because the advanced HTGR is a new reactor and heat load concept and will be a first-of-a-kind license review, a modeling tool serves an additional role as a tutorial device to help the staff become familiar with the features, controls, dynamic response, and safety limits of the new type of plant and aid in developing the appropriate regulations for HTGR designs. Gas-cooled reactors have significantly different safety limits and characteristics than a light-water reactor (LWR); thus, it is anticipated that licensing analysts will need to acquaint themselves in the system response and how the system may be protected against safety events. The task of formulating and executing a simulation model has considerable value to the licensing analyst in familiarizing him or her with the details of plant design and operation.

With these goals in mind, this document surveys various types of analyses that may be needed by the NRC reviewing submittals regarding I&C (Chapter 7) and discusses the capabilities of the modeling codes that are currently available.

In the first part of the report, the transients and potential uses of the I&C code by the NRC are discussed. The section describes the important features of transients and the information that might be sought in an I&C analysis. The mental exercise of working through the sequence of events that must be simulated for each transient leads to the modeling features and approximations that are appropriate for an I&C model for that transient. A sufficiently varied ensemble of transients defines a global set of requirements for a general purpose simulation that can be used for a variety of transients, even those beyond the ones identified. The list of transients and potential uses are formulated based on past experience with NRC calculation needs and on known operational and design basis events for HTGRs. The list is representative of appropriate transients. It is not intended to be an exhaustive list or a recommendation to the NRC for a test suite for I&C support calculations for HTGR licensing reviews. The NRC's actual uses of the code or codes may be quite different than what is envisioned in this report but, because the general nature of the ensemble of transients, codes with the capability to simulate these transients would be able to perform a great many other transients that might be relevant to the evaluation of I&C systems of a plant.

The survey of codes has included many of the codes used by vendors and researchers in the gas reactor field. A table summarizing the features of these codes is given. The features and modeling techniques that are included in the models are discussed. The codes may be able to support NRC needs or serve as examples of capabilities that NRC may wish to acquire. A detailed review of the two most likely codes for NRC use, MELTAC and RELAP5/ATHENA, is given.

One of the purposes of this review is to distinguish the capabilities needed for an I&C code as distinct from a code for safety analysis. Simulation codes are not generally categorized as specifically an I&C code or a safety analysis code. In fact, when a code is needed for I&C support, the usual approach is to use what is already available, typically re-using the same codes that are used for safety analysis. This task seeks to identify those unique features of codes and analyses that might be anticipated for I&C support and tailor the discussion to differences and special needs for a code supporting the review of I&C systems by the NRC as opposed to safety analysis. What is found in this review is that the distinction between an I&C and a safety analysis review is less about the types of transients and plant systems than the information that is under review. Not surprisingly, the process models for all the codes are based on a control volume approach with conservation of mass, energy, and momentum within each volume. However, different aspects of the plant and phenomena need to be modeled with accuracy and completeness, and different approximations may be appropriate when performing an I&C analysis.

The main difference between an I&C code and a safety analysis code is that the I&C code, by definition, must represent the operation of sensors, actuators, and control and protection algorithms accurately and completely to determine whether or not the controls perform as required for the safety function. In I&C simulations for use in NRC licensing reviews, the operation of both safety controls and normal operating controls is important. The main reason for performing the analysis is to confirm that no unintended and unanticipated adverse interactions occur and that no failures originating within the safety and control systems leave the reactor unprotected. In contrast, the safety analysis calculation is usually concerned with bounding calculations that are conservative with respect to a huge range of actual responses from the control and protection system. The bounding nature of the safety analysis calculation means that actual control response can be replaced with a limiting value or boundary condition making the safety analysis problem simpler to solve. The evaluation does not depend on the dynamic performance of the sensors or actuators or controls which are assumed to either perform as intended or fail, whichever is limiting in a bounding case. The main output for the safety analysis is whether or not radiation release limits are exceeded. The limiting or worst case performance is necessary to make the safety case that the public is protected under all circumstances.

The lesson learned from the Three Mile Island (TMI) accident is that severe accident analysis by itself is not sufficient. Transients may evolve slowly at first with the response of the normal operating controls before safety systems react. The initial evolution may place the reactor in a worse condition than assumed for the starting point for a safety analysis event. The initial part of the response can mask symptoms and allow conditions to deteriorate before the safety system acts to shut down the plant and achieve safe cooling. The safety analysis cases, which are typically selected on the severity of the initiating event, can fail to identify the modest initiating events that lead ultimately to a catastrophic accident. In the TMI event, a failure originating with a control valve, the power-operated relief valve (PORV) at TMI, led to a small break loss of coolant. In the TMI event, the PORV failure was not addressed specifically in the safety analysis because the PORV leak rate was smaller than a large pipe break which was the bounding case. The recognition of the seriousness of the event was compounded by sensor readings that were affected by the initiating event. The pressurizer level sensors at TMI functioned correctly and measured the conditions local in the pressurizer and registered an increase in level. However, the level in the pressurizer did not reflect the behavior of the coolant level in the reactor vessel which was actually decreasing. The misleading information and incorrect interpretation of plant status contributed significantly to incorrect decision making by operating staff in the control room.

The lesson learned is that operational controls can mask symptoms by feedback compensation and can lead to a worse state than assumed in the safety analysis. In an I&C analysis, the intent is to assess I&C system's performance, not necessarily the protection of fuel and prevention of radioactive release, which is addressed by other analysis. In the I&C analysis, the process model for the plant systems serves to provide feedback to the control system actions to simulate the plant evolutions but not to evaluate the limiting conditions for fuel operation as in safety analysis. Insight is to be gained from evaluating the best estimate response to understand more fully the actual dynamics in normal and near-normal operation so that unintended and unexpected adverse functions in the control and protection system are revealed. This general type of I&C analysis is called *safety implications of control* and was the subject of considerable research by the NRC following the TMI event.¹⁻⁵

Some typical applications of an I&C code in safety implications of controls might be to

- assess properties of a system response, such as total time delay for the process dynamics, instrument, and actuator response;
- assess interaction between safety and nonsafety controls to ensure that nonsafety systems do not compromise the function of the safety systems;
- perform integrated system test of full system response to show that the systems designed separately also work as intended when operating in concert with other systems and do not have unintended competing functions;
- perform transients on presumably nonlimiting cases to ensure that a seemingly benign event does not evolve, through the action of the automatic controls system or possible actions of operators because of misinterpretation of instrumentation indications, into a configuration that has worse consequences than an event with a more severe initiating event; and
- evaluate the effect of a failure originating in the control or protection system quantitatively for use in a failure modes and effects analysis (FMEA).

2. TRANSIENT CLASSES

The transients important to control design are categorized into three major classes: (1) normal operating conditions, (2) abnormal operating occurrences, (3) design basis events. One of the main categories of study for control and protection system is I&C component failure. These events are considered an abnormal operating occurrence. The main categories are divided along the lines of increasing severity but decreasing frequency of occurrence.

The rationale behind this categorization is to identify the necessary processes and phenomena (P&P) to be included in the model for a realistic representation of the transient. As will be discussed in detail, the P&P are obtained from a large pool of physics but have been condensed to fit into the systems engineering analysis scope. The approach to including certain P&P is two-fold: (1) identify the level of connection between a system's dynamics and the P&P and (2) demonstrate that the time scales of the two dynamics support incorporation. One of the main concerns in I&C reviews is to ensure that functions of safety and control systems in combination do not have any unsafe interactions that are not evident when the functions are considered separately.

2.1 Normal Operating Conditions

Normal operating conditions are defined as the envelope that covers the reactor power between some nominal low power range limit (e.g., 20%) to 100% with all reactor and plant systems functioning as designed. Major transients in this class are (1) load follow of ramp demand and (2) load follow of step change in demand.

2.1.1 Load follow

The load follow event is an example case of the ability of the reactor and power conversion systems to respond to disturbance in which the load produced by the reactor and supplied to the power conversion system must change in response to a change in demand. The limiting cases are taken from the contractually rated maneuvering capabilities of the plant. The limiting cases are specified in terms of the ramp rate and size of step changes that can be followed within specified time response.

The main modeling needs for these events are to be able to represent the full plant integrated with its automatic controls. In some instances, special features must be programmed to mimic any actions that are performed manually by operators in the course of the event. Generally speaking, only the reactor and heat removal systems are needed. The reactor building, protection systems, and emergency cooling features are not needed. The plant data are generally selected for a best estimate of the system response; however, a range of values are used for parameters that depend on normal variability in the plant, such as burnup of the core or fouling of a heat transfer surface. These variable parameters should be readily adjustable.

Typically, the modeling does not need to represent the worst case conditions or hot spot conditions in the system. Since the normal operating events are by definition within the trip envelop, the plant's safety analysis can be relied upon to ensure that the design limits are not exceeded.

2.1.2 Maximum ramp

The maximum ramp transient conveys the plant from the lowest automatic level to the highest at the maximum ramp rate permitted. Any plateaus or hold points required by the operation of the plant may be programmed to occur. Any system state transitions related to power change should be simulated as part of the event.

2.1.3 Step change

The step change transient involves a step in the demand. Of course the system cannot respond instantly; the step change transient shows that the system can respond stably and within the time warranted by the vendor. From a control analysis, the step change transient reveals a great deal about the control and plant dynamics. Many control tuning procedures are based on the step change test for overshoot damping time and maximum error. Parametric studies may point to specific combinations of operating conditions that are most limiting in the system's ability to respond within the trip envelop.

2.2 Abnormal Operating Occurrences

Abnormal operating occurrences are defined by the NRC to include events of moderate frequency in which no adverse consequences are expected in normal operation. The safety requirement of the group of transients is to show that no radiological consequences result from abnormal operating occurrences. For an I&C analysis, however, the goal is to investigate the interactions between systems in a full system simulation.

A large class of abnormal operating events is the set of single failure cases. The safety requirement is that the plant be maintained in a safe state for any single failure. The I&C concerns are that control responses do not impair the ability of the safety system to protect the plant nor the ability of the operator to detect and identify the root cause quickly and accurately.

2.2.1 Turbine trip

Turbine trip transients are a relatively common operational event. The initiation can occur because of external grid disturbances or internal events in the secondary plant. When the electrical load is lost, the

turbine can overspeed if the driving flow to the turbine is not terminated rapidly. A turbine trip is a rapid response to protect the turbine from damage. The gas-cooled reactor requires less rapid response to protect the core than the turbine. Unlike an LWR, the HTGR core can sustain the post-event heat up on loss of load. Most Next Generation Nuclear Plant (NGNP) designs have sufficient thermal margin between the operating maximum temperature in the core and the temperature at which fuel damage could occur, such that the temperature rise in the fuel can safely shut down the nuclear reaction following the turbine trip event even if the rods fail to insert (an anticipated transient without scram event). The I&C analysis of such events focus on actions for protecting other components from damage. In many cases, licensees present these actions as investment protection measures but not safety concerns. In some designs, the control rods have lower temperature limits than the fuel and are more susceptible to overheating in a post-turbine trip recovery. Timing and control of the control rods may introduce potential unsafe conditions, such as control rod damage or inability to insert or withdraw the rods.

Protection of heat exchanger surfaces from hot gas is also a concern. The rise in gas temperature following a turbine trip may be sufficiently high that some heat exchange material's temperature limits may be exceeded. The control concern is that primary and secondary flows must be accurately controlled to protect the heat exchanger from damage.

2.2.2 Load rejection

In this transient, the generator breakers to the grid open reducing the load to the house load. The event requires a prompt turbine response to protect the turbine from overspeed. Depending on the turbine control capability, some designs may treat this event as a runback to station load. In this scenario no safety systems actuate; operational controls run reactor power back to a low electrical power equal to the needs of the site.

2.2.3 Loss of heat sink

The loss of normal heat sink means the loss of flow or coolant on the secondary side of the normal heat removal heat exchanger. Loss of flow events are typically the result of loss of pumping or unintended valve closure. Loss of coolant events are caused by breaks in the secondary coolant pressure boundary. Ultimately, this transient results in a heat up of the reactor system and a need to establish an alternate heat removal. However, for events caused by loss of secondary coolant, the initial response may be different depending upon the break location. A break in the secondary coolant pressure boundary downstream of the heat exchanger would result in a temporary increase in flow of the coolant through the cold side until the inventory of secondary coolant begins to be exhausted and the density and pressure drop. The increase in flow results in an overcooling event which is then followed by an undercooling event. A break occurring upstream of the heat exchanger results in an immediate reduction in flow and reduction in heat removal. Thus, in one instance the initial indications of temperature and pressure on the primary indicate the wrong direction that the reactor should respond, whereas, the other is the right direction.

Because of the expected high frequency of events in this category and the requirement for establishing alternate heat removal, this sequence is frequently one of the main contributors to the core damage frequency in probabilistic risk assessments.

2.2.4 I&C system failures

The I&C system failure analysis should be designed to simulate the response of the system and to indicate the ability of the sensors to accurately portray the plant status to the operator so that correct diagnosis of the failure is made and correct actions are taken. The range of transient should simulate the failure of inputs and outputs to high, low, and as-is. Module level failures representing stalled processors or communications should be considered failed power supplies.

It is very likely that the I&C system will be dual or triple redundant. Particular attention is necessary to identify any points of signal selection or redundant power supply failure that are vulnerable to single failure.

2.3 Design Basis Accidents

The design basis accidents are the set of postulated accidents that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to ensure public health and safety. Events are chosen to be the most severe and limiting events so that all other accidents are encompassed by the results of the design basis events. A number of different initiating events may result in the same sequence of plant responses and are grouped together as a single design basis event. The selection of the events which compose this set is the subject of considerable study. Over time and experience, a consensus has emerged among regulators and designers for the set of design basis events for LWRs. The design basis accidents for gas-cooled reactors are still being considered. The following types of transients are certainly part of the list and are generally covered in all gas reactor licensing submittals. The discussions are general and do not address design specific details.

2.3.1 Pressurized loss of forced circulation (P-LOFC)

Events that involve pressurized loss of forced circulation (P-LOFC) are assumed to occur during power operation, where the primary helium flow stops and the primary system remains pressurized. P-LOFCs may result from a variety of initiating events or event sequences. In fact, in typical HTGR designs, the primary helium flow is intentionally stopped by the reactor protection system on shutdown of the reactor to avoid rapid overcooling. The heat up of the core with pumps off is not damaging to the graphite-coated fuel particles. The heat up serves to shut down the nuclear reaction through the negative temperature coefficient even if rods are not inserted (either by accident or by design.) The shutdown cooling system (SCS) is eventually started up to remove the afterheat and maintain the plant at a stable, off-line condition.

Two major initiating sequences can be anticipated that may lead to a P-LOFC: (1) a reactor shutdown with a failure of the SCS to provide forced cooling or (2) a prolonged station blackout.

Two major safety concerns can be considered for P-LOFCs. The first concern is the core heat-up transient and the potential for delayed radioactive release from the fuel. The reactor core will heat up due to the decay heat. However, since the primary system is still under pressure, natural circulation will eventually help equalize the core temperatures with the maximum core temperatures appearing near the top of the core. The maximum fuel temperatures in the P-LOFC events are dependent on the design but typically remain well below prescribed limits.

The second safety concern is the heat-up of metallic structures and other equipment, in particular the primary system pressure boundary and critical components during P-LOFC conditions. Some important metallic structures, such as control rod sleeves, core barrel and reactor pressure vessel, and eventually their support structures, will usually experience elevated temperatures. These temperature excursions and period of time at high temperatures should be taken into account in determining the structural integrity of these components and code limits. An inadvertent restart of helium circulators is an event that can lead to excessive temperature in metallic structures and components.

2.3.2 Depressurized loss of forced circulation (D-LOFC)

A depressurization accident is an event that results in partial or complete loss of helium inventory. D-LOFC conditions may come from primary pressure-containing equipment failures such as leaks or piping ruptures. Another possibility is the opening of primary system safety valves with failure to reclose.

The major consequence of D-LOFC accidents is the core heat-up and potential radioactivity release into the confinement or the containment—depending on the reactor building design. Compared to P-LOFC conditions, helium natural circulation in the core is negligible because of the reduced density and convective cooling is, thus, not effective in removing decay heat. The D-LOFC must rely on radiative cooling to the vessel walls and the vessel cooling systems.

For the long-term D-LOFC, maximum fuel temperatures typically reach peak values in a few days and are located near the middle or beltline of the core. Temperatures then begin a long, slow decrease as decay heat diminishes.

Typically, the design power level of a gas reactor is based on a conservative calculation of maximum fuel temperature in a D-LOFC accident. The heat-up of metallic structures and subsequent impact on material integrity must also be taken into account.

Depending on the location of the depressurization process, the reactor core could experience an initial cooling due to a rapid discharge of helium and increased coolant flow through the core. The cooling would have a positive reactivity effect.

2.3.3 Anticipated transient without scram (ATWS)

Normally the initiating event for an ATWS event sequence is an anticipated operating occurrence followed by a failure to shut down the reactor. In analysis of an ATWS event, all control and safety rod positions are assumed fixed and no rods drop and no secondary shutdown mechanism operates in response to scram signals. Other protective actions, such as core heat removal via the reactor cavity cooling system (RCCS), are assumed successful; however, there may be situations where other assumptions result in adverse consequences. For example, the termination of active cooling is a protective action for accident conditions where failure of such action in an ATWS can represent a serious hazard, and these eventualities should also be considered. The reactor power, primary pressure, and the maximum fuel temperature should be carefully evaluated for the short-term responses. The temperature histories of key components, such as the core barrel, also need to be measured and assessed against acceptance criteria. In a conservative analysis, uncertainties in measurement and modeling should be taken into account; either conservative value or uncertainty analyses should be performed.

2.3.3.1 Air ingress

Air ingress into the primary system is a safety concern because of the damage it could cause by oxidizing graphite structures and components in the vessel and by oxidation damage to the fuel (TRISO particles). At the operating and accident temperatures that would be seen in the core following a D-LOFC, a significant oxidation would be possible. The extent of the air ingress flow rates and the oxygen content of the available air are dependent on a wide variety of possible reactor and reactor cavity design features, initiating event factors, and subsequent accident progression scenarios. These accidents are typically categorized as very low probability events—beyond design basis accidents (BDBA).

An air ingress event caused by a primary system leak or break starting from nominal operating conditions is usually assumed to follow complete depressurization in a long-term D-LOFC accident.

Depressurization to atmospheric pressure is a prerequisite for atmospheric air to enter the primary system. Air ingress during a normal shutdown is not considered since reactor internal temperatures are below the levels where significant graphite degradation would occur.

During D-LOFC, vessel or other primary system breaches would likely result in blowdown of the helium inventory into the reactor or power conversion unit (PCU) cavity, resulting in displacement of air therein. The resulting atmosphere for the duration of the potential ingress event would depend greatly on whether the confinement system is designed to release the initial discharge of the gas to the atmosphere.

Natural convection ingress flow rates are usually limited to relatively low values due to the high core flow resistance and resistances in other parts of the flow paths. There is considerable uncertainty in the mechanisms of ingress. Many calculations assume purely molecular diffusion which is the slowest ingress. Other studies have shown that convection-assisted diffusion occurs in vertical pipe breaks (cold flow in at the bottom of the break, hot flow out at the top of the same opening.)

Since the oxidation rate for graphite is sensitive to temperature, rather fine structure nodalization of the core lower support structure and reflector regions, in addition to the fuel areas, is recommended for determining any potentially significant loss of mass and strength in critical areas. At least a 2-D and preferably a 3-D core thermal fluid model, with oxidation modeling, would be advisable. The model should account for the differences in rate equations for the various types of graphite used in the structure and the fueled regions. Oxidation rate data, particularly for lower- and medium-range temperatures, can also be dependent on test specimen and the rate of oxidant supply.

2.3.3.2 Steam/water ingress

Steam/water ingress into an HTGR core can result from steam generator heat transfer tube leaks or breaks in steam cycle designs, where the pressure of the secondary water/steam is much higher than that of the primary helium. Water ingress events can involve complex interactions of neutronics, thermo-fluids, chemical reactions, and radioactivity releases. Detailed computer codes and models would be needed to calculate the rate and amount of water/steam ingress, the reactivity effects, and any resulting power transients, pressure, and temperature transients; production of oxidization gases; and the added radioactivity source terms. Measurements of any or all of these parameters would be very useful in providing mitigating actions and post-accident analyses. Uncertainty analyses are likely to be necessary as part of understanding the potential range of accident parameters.

3. GENERAL MODELING CHARACTERISTICS OF VHTR STRUCTURES, SYSTEMS, AND COMPONENTS

The discussion of modeling is organized around the major components of the plant. The discussion describes the mathematical modeling and the context and needs specifically of an I&C code. The modeling of the main process components including piping, plenum, and vessels components; prismatic and pebble bed fuel; compressor and turbine models; and heat exchangers (e.g., the helical coil steam generator); actuators; and sensors are discussed.

Since this review focuses on I&C issues, the modeling capabilities and techniques for control devices are especially important. The capability to model typical control components such as PID controllers is surveyed. We also have sought to review the form of the user input for the code. It is desirable that the control modeling input resemble the format in which the control design is specified. In other words, it would be ideal to represent control design in a graphical display resembling a P&ID (process and instrumentation design) schematic. Such tools are common in control design environments, but the codes surveyed for this report do not have a sophisticated user interface of this type. It may also be important to model digital effects such as digital time delays and finite accuracy of the target control hardware. The code literature has been reviewed to see if the capability to model these effects is provided, but it is not discussed. It seems likely that the omission means that the capability is not provided.

In this chapter, structures, systems, and components (SSC) that are common to a HTGR power system are introduced; associated processes and underlying phenomena—if considered necessary—are identified and briefly described.

An alternative configuration used an indirect electrical cycle. The process heat exchanger (PHX) was connected to a secondary heat exchanger (SHX), which is then connected to the IHX, as shown in Fig. 2. This configuration provided the better separation between the nuclear island and the process facility. Because of additional components, this option turned out with the largest mass and the lowest thermodynamic efficiency—within the down-selected options—as expected. However, operational simplicity from isolating the reactor coolant loop from the power conversion processes may favor this option notwithstanding the increased cost and engineering complexity.

The advantage of adding a SHX that connects to the balance of plant is the possibility of using another working fluid for the power cycle. Design studies using supercritical CO₂ (S-CO₂) demonstrate that these systems can deliver electricity with a high thermal efficiency.⁷ If the heat transport loop is connected to a heat source in this configuration, the heat is transferred from the secondary fluid to the liquid salt via the SHX.

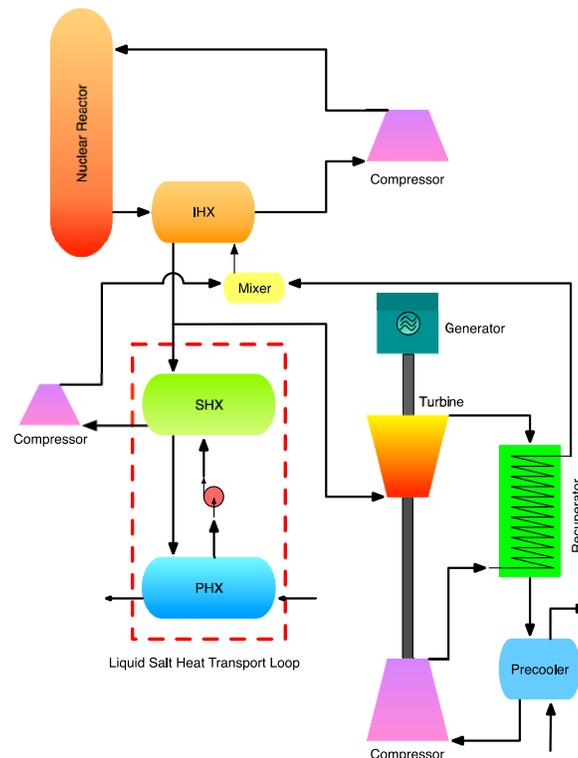


Fig. 2. Alternate configuration option--indirect electrical cycle and a parallel SHX. (Based on Dostal⁷)

The NGNP envisions a multistep development path that will ultimately lead to the VHTR. At each step of the development, the reactor outlet temperature would be increased based on the preceding step. Currently, the NGNP design is considered to start with 750°C core outlet temperature, which will then be raised to 850°C, and finally 950°C for the VHTR. The temperature increments may seem trivial at first, but design implications, particularly in material selection and support system designs such as component cooling, become increasingly significant. The hazards and potential plant damage that must be addressed by control and protection systems increase in severity with the temperature. The fuel design margins are smaller and materials operate closer to temperature limits which may place much higher demands on the control and protection systems. Also, the higher temperatures of operation may require more indirect means for sensing because sensors cannot operate at the elevated level. The dynamics of the indirect sensing system may need to be taken into account in the model.

3.2 Common Structures, Systems, and Components

The following SSCs are included in this report:

1. reactor vessel cavity and core internals,
2. pipes and ducts,
3. SCS,
4. IHX,
5. secondary heat exchanger (SHX),
6. steam generator,
7. helium circulators,
8. gas turbine,
9. instrumentation system,
10. control system, and
11. confinement/containment systems.

3.3 Code Phenomena and Component Modeling

The term “code phenomena” is used to identify the physical processes that are represented in the modeling code. The code phenomena for the VHTR included in this report were extracted primarily from NUREG/CR-6944—*Next Generation Phenomena Identification and Ranking Tables (PIRTs)* study⁸. The list was compiled by a large panel of experts in the field and should be regarded as the most complete and up-to-date processes and phenomena for VHTRs. Not all the phenomena in the PIRT are considered pertinent to systems analysis from a controls engineering point of view. The PIRT code phenomena tables were edited based on engineering judgment and expert solicitation. An instrumentation and controls analysis is more detailed in some areas and less detailed in others. The processes and phenomena list was expanded to include typical control system engineering considerations. Modeling related attributes to determining local conditions which might cause fuel failure are condensed.

The processes and phenomena list was categorized into major systems and subsystems to help conceptualize interaction with other systems.

3.4 Reactor Vessel Cavity and Core Internals

Reactor vessel cavity and core internals include the following subsystems or components:

1. reactor core,
2. inlet plenum,
3. outlet plenum,
4. reactor vessel cavity, and
5. RCCS.

A typical gas reactor pressure vessel and core internals layout is shown in Fig. 3.

The following sections introduce and briefly describe the major phenomena associated with each subsystem or component. The modeling of the core includes the thermal transport processes of conduction in the fuel and solid structures, radiation, and convection.

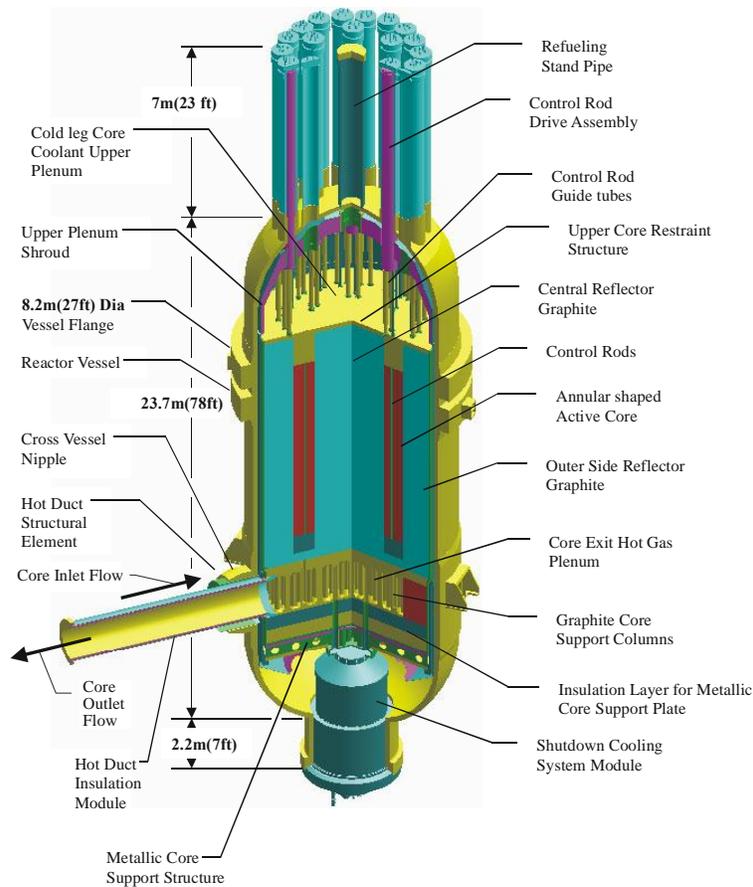


Fig. 3. Basic layout and some design parameters of the GT-MHR reactor and core internals.⁹

3.4.1 Reactor core

3.4.1.1 Fuel geometry

Phenomena associated with the reactor core should be considered independently for the prismatic and pebble-bed design types. The same phenomenon may apply categorically, but the geometries of pebble bed and prismatic fuel are significantly different in details that the modeling of the two designs should be discussed separately.

Mechanically, geometry determines the effective hydraulic diameter of the core, which in turn affects how much pressure loss the coolant experiences. Pressure losses, in effect, create a flow distribution map inside the core, determine active core cooling and fuel operating temperatures, and affect $T_{\text{fuel,max}}$. Changes in geometric configuration, even minor, may have significant ramifications on the heating of the coolant fluid—and cooling of the fuel assemblies of fuel pebbles, and on how the temperature is distributed in the core volume.

Pebble-bed design has uncertainties due to variation in packing fraction, which creates difficulty in predicting local hot spots. Lack of instrumentation in the active core further exacerbates the understanding of dynamics and puts more emphasis on prediction of core condition by modeling.

The fuel geometry in the core is affected by three types of phenomena:

1. changes due to temperature gradients,
2. changes due to graphite irradiation, and
3. changes due to core barrel geometry.

3.4.1.1.1 Changes due to temperature gradients

Changes in core geometry as a result of temperature gradients primarily affect fuel operating temperatures. The underlying reason in large gradients in HTGRs is the large ΔT from core inlet to core outlet. During normal operation, axially driven local velocity variations affect temperature gradients. Furthermore, the relationship between gas temperature and viscosity requires understanding of localized effects. From the modeling standpoint, computational fluid dynamic (CFD) capabilities can be incorporated into the codes to model the localized interrelated effects of temperature gradient and flow. In many instances, I&C analysis cannot support computational load of a CFD model of the core. Instead, either one-dimensional flow or coarse mesh two- or three-dimensional model is used. It is understood that the simplified I&C models cannot predict the local effects for safety evaluation. The goal is to couple the temperature gradient effects with the flow and neutronics solutions.

3.4.1.1.2 Changes due to graphite irradiation

Irradiation of graphite changes the structure of the material and, as a result, material thermophysical properties tend to shift from their unirradiated conditions. A key property that changes as the material is irradiated is the thermal conductivity, which determines the rate at which the internally generated energy is transferred to the coolant. As the thermal conductivity changes, fuel operating temperatures also shift. Because of fuel temperature changes, flow patterns may as well change. The main rationale for this phenomenon is the fuel time at temperature, which is the determining parameter for fuel failure fraction. In I&C analysis, the issues are less about fuel failure. The material properties need to be appropriate for the particular analysis conditions or a range of parameters should be considered. The model inputs should be developed covering the appropriate range.

3.4.1.1.3 Changes due to core barrel geometry

Changes in core barrel geometry have some effect on fuel operating temperatures. Fuel block warping, which applies specifically to prismatic design, can be a serious problem.

In the prismatic design, core block stability causes disturbances in core flow distribution, as observed at Fort St. Vrain, where the opening of gaps between blocks was tied to irregular increases in bypass leakage flow. Though experience exists for this phenomenon, it is anticipated to be strongly dependent on the design. Onset of oscillation is hard to predict because the NGNP designs employ a tall vessel.

For the pebble-bed design, another important phenomenon is the core bridging in which some pebbles became lodged in a fixed position while others continue to circulate through the core. Bridging was observed at bottom of core at the beginning of life at AVR. Some solutions were developed and established for AVR; however, their applicability remains to be seen once the design is finalized.

Another phenomenon in the pebble-bed design is the wall interface effect, which may cause diversion of some coolant flow. The number of pebbles across the core diameter is known to impact these effects.

The I&C concern is to determine what measurable effects would be seen in plant sensors in the case of changes to the core barrel geometry.

3.4.1.2 Core coolant flow and properties

Coolant heat transfer correlations are used to calculate core temperatures. Models are generally based on equations that yield core-average values, but local values of heat transfer vary significantly from average

heat transfer. Moreover, heat transfer calculations in high-temperature regions tend to be more difficult. For the pebble-bed design, flow laminarization is known to take place close to vessel wall, which further complicates the modeling of fluid flow and heat transfer.

Core inlet flow distribution is important for core cooling calculations. Inlet flow distribution is mainly imposed by the inlet pressure distribution, which is a strong function of complicated geometry of the inlet plenum. For systems with multiple loops, thermal mixing takes place in the plenum. For cases where proper mixing is not achieved, nonuniform inlet temperature distributions might occur. If the nonuniformities are sufficiently large, they result in thermal stress problems. Some degree of uncertainty exists in the data and correlations.

Understanding of flow distribution in the outlet plenum is complicated by multiple phenomena including turbulent mixing with incoming jets over large temperature spans. This issue may contribute to localized hot spots leading to excessive thermal stresses. Thermal streaking may lead to problems with downstream components such as a turbine or the IHX.

3.4.1.3 Core properties

Material property changes over the life of the components primarily as the result of irradiation affect the results of certain critical calculations, including $(T_{fuel})_{max}$ (low values) and $(T_{vessel})_{max}$ (high values).

Because graphite mass constitutes a large portion of the reactor core, core effective conductivity is a complex function of graphite temperature history and cumulative radiation dose. Of particular safety importance is the calculation of peak fuel temperature, which is highly sensitive to irradiation and annealing—two competing processes. Significant deviations in peak fuel temperatures were demonstrated (approximately 75 to 100°C) based on realistic sensitivities in fuel element annealing. Local predictions of level of annealing can be problematic. Because of the level of uncertainty involved, most safety analysis calculations cannot take advantage of annealing effects because the uncertainty in data is too large to separate out these effects.

Graphite heat capacity also varies as a function of temperature. Understanding of heat capacity is particularly important in determining fuel failure fraction in accident analyses. A large heat capacity provides a wider margin to failure due to slower accident response and gives time for taking protective actions during an event. It also allows more time for fission products with shorter half-lives, hence reduces the source term in severe accident analyses. Heat capacity data for graphite are quite good.

Another critical core material property is the vessel emissivity, which may deviate drastically depending on the history of elevated temperatures and time-at-temperatures. Understanding of vessel emissivity is important in accident analyses to predict the amount and rate of heat exchange between the reactor vessel outer surface and the RCCS walls. This property was designated to be of high importance by the *Accident and Thermal Fluids Analysis PIRT* group¹⁰. All of this discussion also applies to RCCS panel emissivity. However, these considerations have more relevance in accident analysis calculations; most control systems design and analysis tools will neglect this process.

Stored (Wigner) energy is the energy from carbon atom dislocations in the graphite lattice structure of the moderator and reflector graphite due to irradiation. The sudden release of Wigner energy was a significant contributor to the Windscale accident in 1957 and is important for due consideration of a significant reactor accident involving a graphite moderated core. The susceptibility of NGNP to sudden release of Wigner energy is much less than Windscale because the temperature of operation is much higher. The graphite lattice anneals at normal operating temperature expected for the NGNP; however, the Wigner energy should be given consideration at low-temperature operation where the amount of dissipative energy from the thermal vibration modes is not sufficient to restore the lattice structure. This phenomenon is most notable—for graphite—at temperatures between 200 and 250°C where large energy releases are observed. Understanding or incorporation of this phenomenon is necessary in fuel failure fraction

calculations. This process is fairly well understood, and it is not expected to occur for irradiation of graphite at high temperatures where annealing effects dominate. Since the focus of control systems design and analysis mostly deals with higher temperature normal operations and anticipated operational occurrences, Wigner stored energy in most cases may be neglected. It should be included in low temperature criticality events.

3.4.1.4 Factors affecting reactivity, power transients, and power distribution

There are a number of postulated scenarios that can affect overall reactivity of the core. Different scenarios can be considered for the prismatic design and the pebble-bed design.

A common scenario for designs that use a direct cycle with a steam generator is reactivity insertion due to steam or water ingress into the primary system. The primary concern is the potential for large water ingress from steam generators for steam cycle plants because of the large inventory of water at pressure higher than the helium pressure in the steam cycle plants. Other water sources, such as the SCS or PCU coolers, may also leak and lead to steam coming in contact with the primary system. The potential for these sources to be introduced to the primary is less because their pressure is normally less than the helium pressure. In-leakage would only occur for low pressure events. Water presence—even at small volume fractions—increases neutron moderation and potentially resulting in positive reactivity insertion. Presence of water at sufficiently high concentrations decreases the control rod effectiveness for prolonged exposure periods, resulting in reduction of the shutdown margin. However, HTGRs have notably high negative reactivity feedback mechanisms that should effectively compensate these effects and safely reduce the power level. However, the level of passive safety is design dependent and is also a function of amount water leaked into the primary system. Past experience with the Fort St. Vrain and AVR reactor indicates that, if water is present at all in the cooling system, water leakage into the primary gas is difficult to prevent. Moreover, moisture sensing is difficult and is expected to involve a gas sampling and cooling process with flow and sensing dynamics. Simulating ingress, moisture propagation, and sensing phenomena should be supported in the control and protection system design and analysis tools to demonstrate that the control system will reduce the potentially adverse effects of reactivity insertion to protect the investment, and that the protection system activates according to design requirements to bring the reactor and the plant to a safe state. Major steam or water ingress scenarios will probably not be covered within the control system design but most likely be addressed under safety analyses or severe accident analyses. Protection system design might be required to meet certain functional requirements to mitigate potential consequences during the progression of the accident. Modeling the moisture sensing system and its reliability to sample the coolant at the appropriate location and detect the presence of small leaks is the main I&C analysis concern.

Negative reactivity feedback coefficients for fuel, moderator, and reflectors provide passive safety shutdown characteristics. These mechanisms provide inherent defense, by very nature of the physics, against—almost—any reactivity insertions. Hence, their understanding is critically important to deliver a safe system. The understanding of these feedback mechanisms is hindered by lack of knowledge of resonance capture phenomena at high temperatures. Experiments performed at high-burnup graphite piles at high temperatures suggest miscalculation of power coefficients. Resonance capture is parasitic absorption of neutron during the slowing down process. Shifts in neutron spectrum due to water ingress may change the fraction of resonance capture. The moderator or reflector reactivity feedback coefficient will essentially depend on whether the capture fraction increases or decreases—for negative feedback, fraction of resonance capture should increase as the neutron spectrum softens. Reactivity coefficients are typically inputs to I&C models. The safety and control system analysis requires that suitable coefficients that reflect the range of uncertainty be calculated for the specific conditions under simulation.

3.4.1.5 Inlet plenum

In most proposed reactor designs, the coolant gas enters an annular region around the core near the bottom of the vessel. It flows upward keeping the pressure vessel at the cooler conditions of the reactor inlet gas. At the top of the core barrel, the coolant turns and enters a volume above core and reflector that distributes the coolant for downward flow through the core, reflector, and control components.

3.4.1.6 Core inlet flow distribution

Knowledge of core inlet flow distribution is important for core cooling calculations. It constitutes a boundary condition for coupled thermal hydraulic and neutronic dynamics. The inlet plenum employs a sophisticated geometry to control flow into the reactor core, which provides a regulated introduction of coolant into the flow channels. Presence of core support structures and other essential components also causes flow disturbances which further complicate the computational model. For the prismatic design, flow channels will have varying heat generation rates due to three-dimensional flux shape in the core. Hence, the core inlet flow should be determined based on the anticipated power map during normal operation. For the pebble-bed design, coolant follows a more stochastic path due to random motions of pebbles in the core barrel. Moreover, the flow channels in the pebble-bed design are more interconnected than those of the prismatic design potentially resulting in faster-developing cross flows due to discrepancies in local heat generation rates in neighboring cells. As a result of this, flow in pebble-bed cores would tend to reach equilibrium before it reaches the hot portion of the core.

In the prismatic design, on the other hand, channels are convectively independent along graphite columns; therefore, cross flows can only develop in the space between stacks.

3.4.1.7 Thermal fluid mixing from separate loops

Multiple loops with different types of heat loads are likely to result in unbalanced return temperatures, particularly in transient conditions. Hot and cold streaks can persist for great distances in pipe flow. Lack of sufficient degree of mixing leads to nonuniform core inlet temperature distribution, which ultimately induces undue thermal stresses in components, particularly in the core support structure. Also, the temperature sensors read a local temperature rather than the average temperature which could result in incorrect control or protection system response.

A good understanding of mixing is also necessary for fuel time-at-temperature calculations for safety analysis. It is not expected that a system code would incorporate three-dimension flow models; however, a range of mixing behaviors should be considered when evaluating I&C response.

3.4.1.8 Outlet plenum

The outlet plenum is the chamber at the exit of the reactor vessel in which flows from the core and bypass channels mix together and flow to the concentric duct. It is particularly significant because of the distribution of temperatures at the core exit can lead to hot streaks that can potential damage components downstream.

Flow distribution from the core into the outlet plenum is a complex function of pressure drops in the channels upstream as well as the irrecoverable losses in the outlet plenum. The latter is primarily affected by sudden change in coolant flow direction due to geometry of the outlet plenum subject to coolant velocity profile at the core outlet.

Flow distribution affects how the fluid mixes in the plenum. Proper mixing of the hot stream is intended to reduce local hot spots downstream that may introduce excessive stress on the support structure and other critical components, such as the IHX and the turbine.

The complication arises from the complex nature of turbulent mixing with incoming jets over large temperature spans. This condition is further exacerbated in pebble-bed reactors.

Similar approaches to provide approximate models of partial mixing in a system code may be needed for cases investigating detectability of hot jet behavior in the outlet plenum.

3.4.1.9 Reactor Vessel Cavity and RCCS

Reactor vessel cavity is the chamber in which the reactor pressure vessel is contained. The RCCS is a safety-grade passive decay heat removal system that serves as an alternative to active heat removal systems. The primary modes of heat transfer are (1) radiation from vessel to RCCS panels, (2) natural convection in RCCS tubes—either air or water, and (3) convective air-cooling with natural draft. The primary purpose of RCCS is ensuring the integrity of reactor cavity concrete as well as reducing the pressure vessel temperatures to increase the lifetime of the component. The latter purpose is not considered a safety issue but is implemented for investment protection purposes.

In analyzing depressurization events, one of the unknowns is the location of the break which might significantly affect axial heating profile of the RCCS. The axial heat flux profile determines the radiant heat input from the core to the reactor vessel creating another level of complexity in determining the temperature profile of the vessel. Furthermore, since the RCCS is always active and removing heat, the radiant heat transferred by the RCCS is the integral part of total heat balance; hence, validation data is needed.

A key parameter in this process is the emissivity of surfaces that are involved in the radiative heat transfer. As the components age, its surface properties undergo significant changes, which in turn results in major shifts in emissive and absorptive characteristics. Therefore, data compilation is an essential part of understanding how the components will behave under anticipated accident conditions. View factors can be easily calculated with commercially available engineering software tools. Prior to obtaining operational data for emissivity, the I&C code would require a range of appropriate values of emissivity to cover the limiting cases which may exist.

The conductive heat transfer in the solids involved can contribute a significant fraction of the overall heat exchange; therefore, conjugate heat transfer models should be considered even in I&C codes.

There have been known issues with water-cooled designs in the past for similar systems. For instance, fouling on the coolant side is a known in heat-exchange systems with insufficient chemistry control. Fouling is referred to as the accumulation of material on solid surfaces. This gradual buildup of scale over time impedes the effectiveness of the heat transport system resulting in lower heat removal. Again, the I&C code depends on external calculations for appropriate range of fouling factors.

3.4.1.10 Piping and ducts

The interconnections between components may be conventional piping and ducts but also a mathematical or organizational distinction such as the annular regions of the vessel that serve to direct flow of gas. The general approach to modeling piping is to simplify to one-dimensional flow and account for the convective energy transport and flow and pressure drop characteristics of the pipe in the hydrodynamic solution using standard control volume approach. Wall temperature is typically included in VHTR model. Unlike conventional LWRs, temperatures in the pipes and vessels can be the limiting concern even in normal operating transients.

One unique component in the VHTR design is the concentric duct. The reactor vessel in most of the gas designs is connected to the heat removal system by a concentric duct in which the hot coolant leaving the reactor flows in the inner region of the duct, and the cooler returning flow is in the outer annular region. The purpose of this configuration is to reduce the pressure that the wall of the hot duct must be able to bear. The high temperature of the exit gas requires materials that will not creep under load. By placing the duct inside the pressure boundary of the return flow the pressure across the duct wall is only the difference in pressure between the hot leg and the cold flow rather than the full pressure drop to ambient. However, the concentric duct introduces certain accident scenarios which must be detected in the plant

and controlled. Failure of the hot duct into the cold duct leads to a sudden increase in the outer wall temperature. Failure of both walls leads to the potential for air ingress. The I&C analysis of these events involves both the ability to simulate instrumentation for detection of failures and safety system responses.

3.5 Shutdown Cooling System

Shutdown cooling system (SCS) is an active system intended to remove the decay heat after reactor shutdown as a redundant means to the secondary heat transport system. Typically, the SCS is designed to come online following detection of (1) heat exchanger leaks, (2) circulator overspeed, (3) low cooling water flow, (4) loss of net positive suction head, and (5) high heat exchanger temperatures. A conceptual rendering of the SCS along with some the primary heat transport system components is shown in Fig. 4.

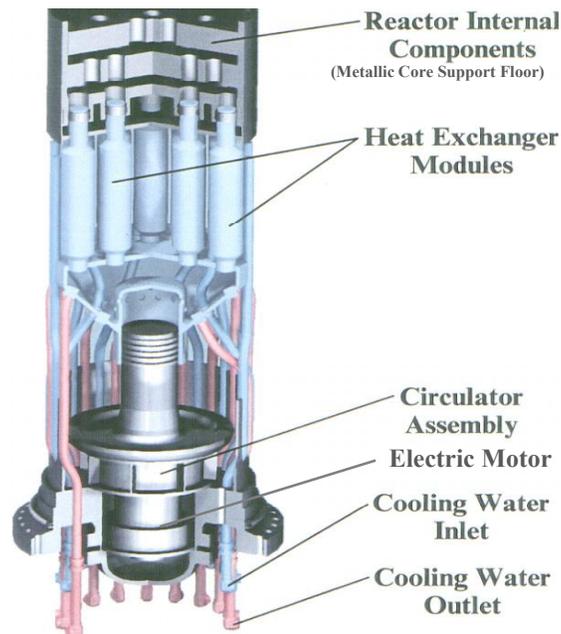


Fig. 4. Proposed layout of the SCS in the bottom portion of the reactor vessel underneath the metallic core support floor.¹¹

Upon activation, the SCS closes the shutoff valve and shuts down the primary helium circulator. As illustrated in Fig. 5, the SCS consists of a helium circulator, a helium shutoff valve, a gas-to-liquid heat exchanger, and a control system, and it interfaces with the Shutdown Water Cooling System and service equipment.

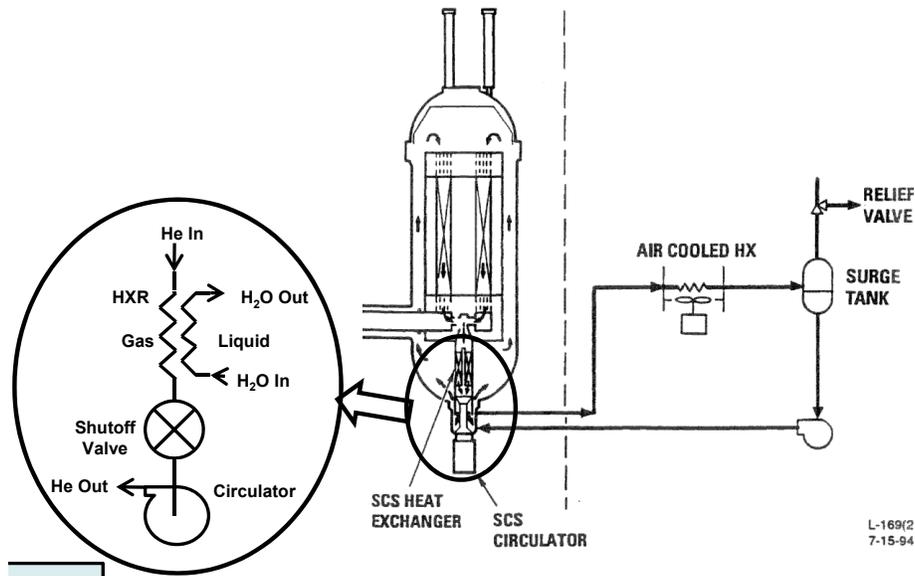


Fig. 5. Functional diagram of the SCS—single loop per reactor module.¹¹

The SCS is classified as a nonsafety-related system in the modular high temperature reactor (MHTGR) and was considered to be one of the two systems available for decay heat removal in case the secondary heat transport system became unavailable.⁹

3.5.1.1 Flow and temperature transients during startup

The SCS is not operational under normal reactor conditions, primarily because any heat removed by the SCS is nonrecoverable and contributes to the parasitic heat loss. Upon initiation of flow in the SCS loop, the SCS can undergo flow and temperature transients until it finally reaches equilibrium. A low-order model of the SCS can be developed and implemented into the integrated plant dynamics simulation. This capability will determine the operating envelope of the design and help investigate if safety-critical functions are challenged.

The startup transients in the SCS can potentially cause excess thermal stress in adjacent components. These transients must be well understood because they challenge the integrity of the primary system boundary.

3.5.2 Maintaining water coolant inventory

The usual working fluid in the SCS is water, as illustrated in Fig. 5. The water inventory in the system must be maintained at all times to meet the functional requirements of the design. Furthermore, in addition to the mass inventory, the chemistry of the coolant should also be regulated to avoid or mitigate fouling in the water-to-air heat exchanger and other mechanical units. Some level of fouling is unavoidable and can be tolerated, but excessive build-up can drastically change the thermal resistance in tubes and may result in departure from the nominal operating envelope.

A simple parametric fouling model can be incorporated into the thermal model to determine its effect on overall performance of the system.

3.5.3 Steam/water ingress into primary loop

The SCS provides an additional redundancy for removing heat from the reactor in a post-shutdown condition. However, it introduces an additional risk by bringing a water source in close proximity to the primary system. The SCS pressure should nominally be kept below the pressure of the primary coolant to reduce the risk of water or steam ingress. However, if a leak path from the SCS into the primary system develops coincidentally with a depressurization event, the pressures will eventually equalize and allow ingress of water or steam into the primary system. The I&C code must evaluate the instrumentation detects and respond to limit the water ingress by isolating the SCS. A transition to alternative cooling must be demonstrated.

3.6 Intermediate Heat Exchanger

The IHX is a gas-to-gas or gas-to-liquid salt heat exchanger that couples the primary heat transport system to the secondary loop of the plant. The IHX is a critical component for safe operation of the reactor and the rest of the systems in the balance-of-plant side. It is anticipated that the IHX will experience the most severe operational conditions because it is connected to the outlet plenum where very hot gas streaks of gas exiting the core are possible due to hot channels and imperfect mixing in the outlet plenum and hot duct. Protecting the IHX from excessive temperature is one of the limiting cases for control and safety analysis.

Control of flow and temperature in the IHX is a concern in both normal and abnormal operating conditions. Unlike LWRs, VHTRs have greater risk from undercooling the IHX than from undercooling the core. Control and safety responses have to be sufficient to protect the pressure boundary between the primary and secondary coolant and prevent a normal operating event such as loss of heat sink from progressing to a pressure boundary failure.

One interesting anticipated transient of high importance is the potential failure in the intermediate heat transport loop that moves heat from the primary heat transport system. For gas-phase intermediate heat transport systems, the total gas inventory in the intermediate loop may be significantly larger than the total inventory of gas in the primary system. A failure in the intermediate heat exchanger may first result in overcooling the primary helium due to enhanced heat transfer followed by a loss of heat sink (i.e., undercooling).

Failure of the IHX can potentially lead to damage to safety-related SSCs due to blow-down effects from large mass transfer and over-pressurization of either the primary or secondary loop. The degree of damage depends on the heat transfer fluid in the secondary heat transport system—helium in the secondary loop might significantly increase pressurized gas inventory and result in prolonged depressurization events.

The eventual effect of loss of pressurized coolant inventory from the intermediate heat transport system is the loss of heat sink to the primary loop.

3.7 Turbomachinery

The helium circulator and turbine are axial flow turbomachines. In a gas turbine plant such as the gas-turbine high-temperature reactor (GT-HTR), the turbine, compressor, and electrical generator are combined on a single shaft usually in the primary loop of the plant. The turbine turns the shaft supplying power to both the circulation of primary coolant and electrical generator. This configuration is described as a closed Brayton cycle design (closed in the sense that the working fluid is cycled through the core, turbine, and compressor in a closed loop. In contrast, an aircraft jet engine is an open Brayton cycle.)

In designs utilizing a steam generator and conventional steam turbine for electrical generation, the helium circulator is powered by an electric motor. Typically the electric motor for the circulator is variable speed.

The dynamics of flow in conjunction with the dynamics of the shaft mean that the turbomachinery is an important dynamic element of both control and safety analysis. In most safety scenarios, the circulators in the primary loop are tripped at the start of any event involving reactor shutdown. This has the effect of protecting the heat removal equipment from the transient and allows the reactor heatup to assist in shutting the reaction down through negative temperature feedback.

3.7.1 Modeling equations

The complicated flow through moving and fixed rows of blades in a turbine or compressor precludes a complete first-principles model, at least for the purpose of I&C transient calculations. A lumped-parameter, one-dimensional flow model is usually used in a system modeling code, wherein one or more stages of a turbine are treated as a single volume called a stage group. The flow volume may be staggered with respect to the mass and energy volume. The stage group is then represented using energy, continuity, and momentum equations which are modified to account for the mechanical work done on or by the blades. In general the fluid volume within the turbine is small compared to other volumes. Consequently, the time constants associated with the dynamic conservations are very small and may limit the time steps size for the numerical integration of the hydrodynamic equations. In many models, one or more of the conservation equations is approximated as a quasi-steady balance equation with no storage of the conserved quantity in the fluid. This is equivalent to approximating the small actual volume as a zero volume element.

3.7.2 Performance maps model for head and efficiency of gas turbines and compressors

The mechanical performance of gas turbomachines can be represented by relationships that relate pressure change and efficiency to variable conditions of the device such as flow, speed, inlet pressure, and inlet temperature. These relationships are called performance maps or characteristic maps. The performance maps can be used to determine the actual work done on or by the fluid and the net power available to the shaft. The maps may be calculated using detailed multidimensional flow models in a separate calculation of the turbine components or determined from experimental data. Dimensional analysis suggests that devices that are geometrically similar have similar performance maps when the variables are reduced to their dimensionless groups so that a class of similar devices can be represented by a single set of performance maps.

In compressible flow devices, the performance map relationships are defined in terms of dimensionless groups in the following general form.¹²

$$\frac{\hat{p}_{02}}{p_{01}}, \eta, \frac{\hat{P}}{\rho_{01} N^3 D^5} = f \left\{ \frac{\dot{m} \sqrt{RT_{01}}}{D^2 p_{01}}, \frac{ND}{\sqrt{RT_{01}}}, Re, \gamma \right\}. \quad (3.7-1)$$

The three performance coefficients on the left-hand side are the pressure coefficient, efficiency, and the power coefficient. The pressure coefficient is the ratio of stagnation pressures. Stagnation pressure is defined as $p_0 = p + \frac{1}{2} \rho c^2$ and accounts for the recoverable pressure from the kinetic energy in the flow.

The definition of stagnation temperature similarly accounts for kinetic energy in the flow, $T_0 = T + \frac{c^2}{2C_p}$.

(Note that specific heat for a perfect gas is given by $C_p = \frac{\gamma R}{\gamma - 1}$.) The additional subscript of 1 or 2 on the variable indicates inlet and outlet respectively.

The efficiency coefficient (sometimes called the hydraulic efficiency) for a turbine is defined as

$$\eta_t = \frac{\text{Actual work done by the fluid}}{\text{Maximum possible work in an isentropic expansion from the entering to leaving pressure}}. \quad (3.7-2)$$

The corresponding definition of an efficiency of a compressor is the minimum work done on the fluid actual work by an isentropic compression from entering to leaving.

$$\eta_c = \frac{\text{Minimum possible work in an isentropic compression from the entering to leaving pressure}}{\text{Actual work done on the fluid}}.$$

The formulae are defined differently so that the efficiency is between zero and 1 for both compressors and turbines.

The four dimensionless groups in the argument of the performance map are respectively dimensionless flow, dimensionless speed, Reynold's number, and ratio of specific heats. The variables appearing in the dimensionless groups are \dot{m} mass flow rate, T_{01} stagnation temperature at inlet in absolute units, N angular speed, D diameter of rotor, R gas constant ($R = R_0 / MW$ where R_0 is the universal gas constant $R_0 = 8.314 \text{ kJ} / \text{kg mol} / \text{K}$ and MW is the molecular weight of the gas).

For a specific device handling a specific gas, it is customary in vendor literature to omit the constants of the design (D , R , and γ) and write the performance maps in terms of dimensioned input quantities. The Reynold's number, Re , is usually dropped as an input because the performance maps do not depend strongly on it. For a turbine operating on an ideal gas (not a steam turbine), the power coefficient is directly related to the change in temperature. Since temperature can be measured directly in the device, the power coefficient is usually written in terms of temperature.

With these changes in formulation, the performance maps are then formulated in terms of the general parameters

$$\frac{\hat{p}_{02}}{p_{01}}, \eta, \frac{\Delta \hat{T}_0}{T_{01}} = f \left\{ \frac{\dot{m} \sqrt{T_{01}}}{p_{01}}, \frac{N}{\sqrt{RT_{01}}} \right\}. \quad (3.7-3)$$

The performance relationships for $\Delta \hat{T} / T_{01}$ can be obtained theoretically for a turbomachine operating on an ideal gas. The ideal gas law ($p / \rho = RT$), the perfect gas law for isentropic expansion, ($p / \rho^\gamma = \text{constant}$), definition of efficiency, and the steady state conservation of energy in the gas can be used to derive the following algebraic expressions. By convention, the two equations are needed because the efficiency is defined differently for compressors and turbines so that the ratio is positive.

Turbine

$$\frac{\Delta\hat{T}_{0,t}}{T_{01}} = \eta_t \left[1 - \left(\frac{p_{02}}{p_{01}} \right)_t^{\frac{\gamma-1}{\gamma}} \right] \quad (3.7-4)$$

Compressor

$$\frac{\Delta\hat{T}_{0,c}}{T_{01}} = \frac{1}{\eta_c} \left[\left(\frac{p_{02}}{p_{01}} \right)_c^{\frac{\gamma-1}{\gamma}} - 1 \right], \quad (3.7-5)$$

where the subscripts, t and c , have been added to distinguish the turbine and compressor relationships respectively.

The enthalpy of an ideal gas is given by $\Delta h = C_p \Delta T$. That the shaft work done on or by the fluid can be computed as:

Turbine

$$W_{shaft,t} = -\dot{m} C_p \Delta\hat{T}_{0,t} \quad (3.7-6)$$

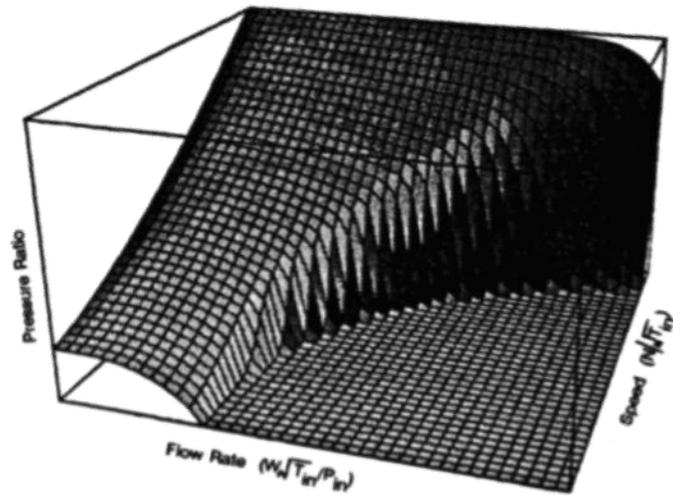
Compressor

$$W_{shaft,c} = \dot{m} C_p \Delta\hat{T}_{0,c} \quad (3.7-7)$$

By convention, the equations are defined differently so that the temperature difference is positive. The equations are defined such that $W_{shaft,t}$ is negative and $W_{shaft,c}$ is positive.

The efficiency and pressure ratio performance maps are usually obtained by detailed calculation or experiment. Figures 6 and 7 illustrate typical performance maps for a gas turbine and a compressor. The figures were generated analytically by Yan¹³ using data obtained from General Atomics and United Technology for the GT-HTR.

cf-3D



ce-3D

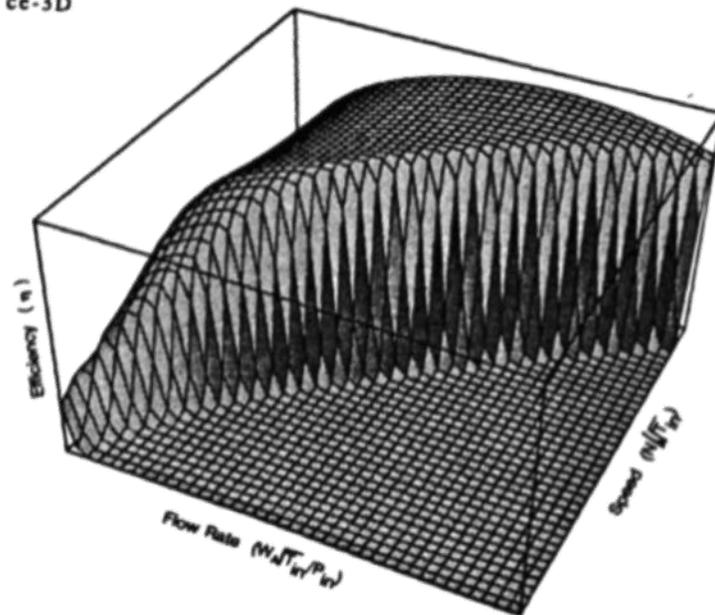


Fig. 6. MGR-GT compressor performance maps.¹³

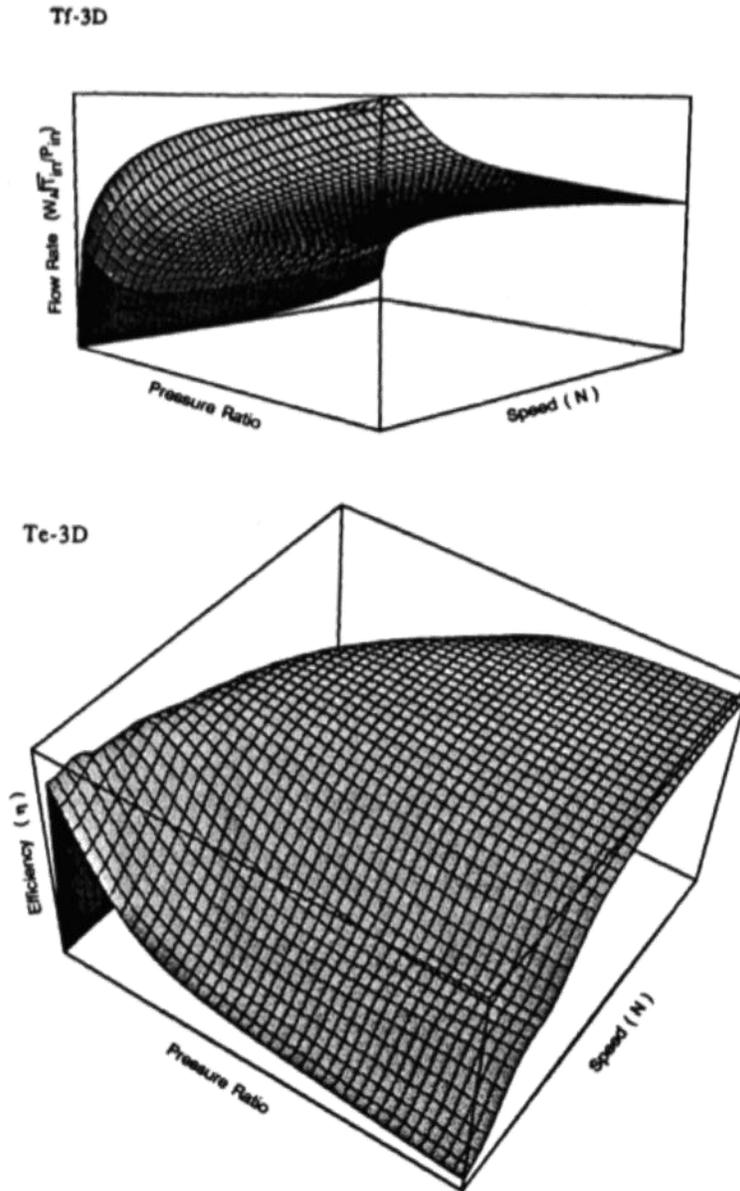


Fig. 7. MGR-GT turbine performance maps.¹³

Since the pressure coefficient and efficiency which appear in (3.7-4) and (3.7-5) are available from Figs. 6 or 7, the power from the shaft work can be evaluated using the inlet conditions. These quantities represent the energy added or removed from the fluid in the stage group control volume by the blades.

$$W_{shaft,c} = \dot{m} C_p T_{01} \left(\frac{\Delta \hat{T}_t}{T_{01}} \right); \quad W_{shaft,t} = -\dot{m} C_p T_{01} \left(\frac{\Delta \hat{T}_c}{T_{01}} \right). \quad (3.7-8)$$

Similarly, the change in stagnation pressure across the blade region is obtained from the pressure coefficient map.

$$\Delta \hat{p}_0 = p_{01} \left(1 - \frac{\hat{p}_{02}}{p_{01}} \right). \quad (3.7-9)$$

3.7.3 Conservation equations for the fluid

Figure 8 represents a general control volume in which shaft work is included

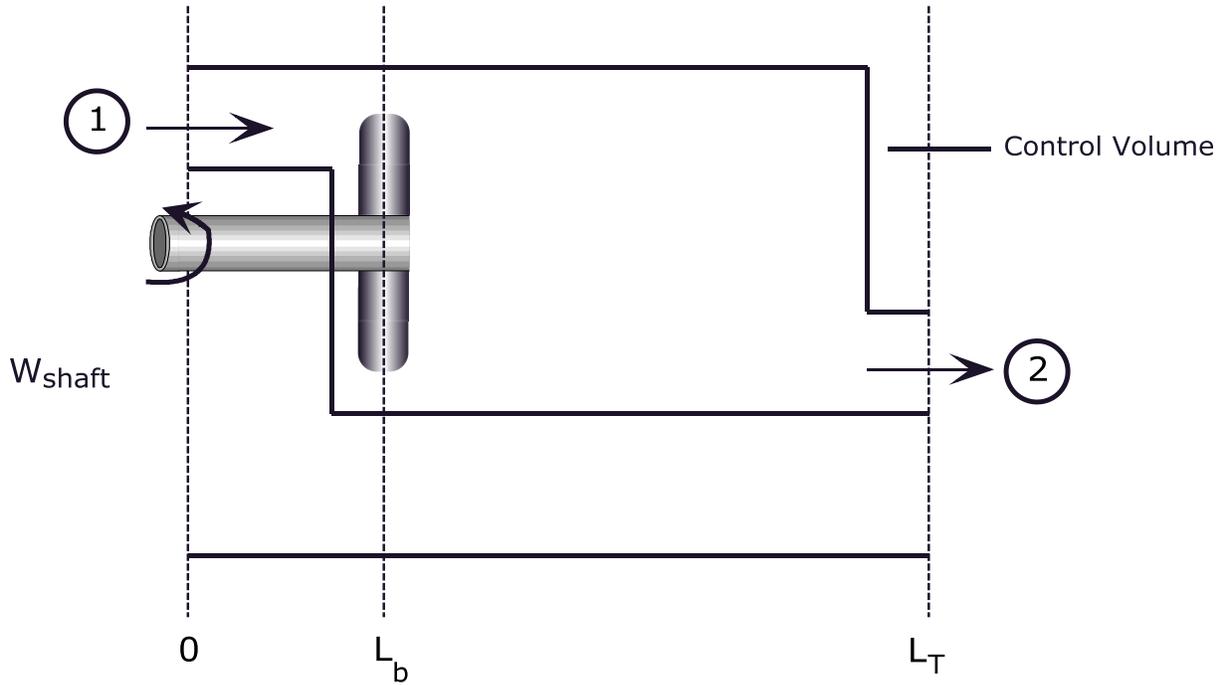


Fig. 8. General control volume with shaft work.

To distinguish between the work done on or by the blades and other energy terms, the stage group can be considered as two parts in a series: first, a volumeless blade region, then an associated fluid control volume. A circumflex is used to distinguish the outlet of the blade region from the outlet of the control volume. Hence, the stagnation pressure of the outlet of the blade region, which is the inlet of the control volume) is \hat{p}_{02} . The outlet of the control volume is p_{02} .

The general time-dependent conservation equations for energy, mass, and momentum for a control volume are modified to account for the mechanical work done on or by the blades. The conventional form of the control volume equations for energy and mass are obtained by integrating the differential

conservation equations over the volume. Terms associated with the shaft work appear in the energy and momentum equations.

Mass

$$V \underbrace{\frac{d\bar{\rho}}{dt}}_{\text{Mass storage}} = \underbrace{\dot{m}_1 - \dot{m}_2}_{\text{Convected mass}} . \quad (3.7-10)$$

The overbar on $\bar{\rho}$ indicates an appropriately defined integral average along the path of the fluid through the stage. The mass flow rates into the control volume at the inlet and outlet are \dot{m}_1 and \dot{m}_2 . Note that mass flow and the fluid velocity are related by $\dot{m} = c\rho A$ where c is fluid velocity, and A is flow area.

Energy

$$\underbrace{V \frac{d\bar{\rho}e}{dt}}_{\text{Energy Storage}} = \underbrace{\dot{m}_1 \left(h_1 + \frac{c_1^2}{2} + gz_1 \right) - \dot{m}_2 \left(h_2 + \frac{c_2^2}{2} + gz_2 \right)}_{\text{Convected energy}} + \underbrace{Q}_{\text{Conducted Energy}} + \underbrace{W_{shaft}}_{\text{Shaft Work}} . \quad (3.7-11)$$

In the energy equation, e represents the total energy of the fluid including thermodynamic energy, kinetic energy, and potential energy from elevation, $e = u + pv + \frac{c^2}{2} + gz = h + \frac{c^2}{2} + gz$. The overbar \bar{e} indicates an integral average over the volume.

The momentum equation may take various forms in the turbine and compressor models. The equations may appear to be different but are actually equivalent. It is worthwhile to address the main different versions to show the equivalence. The following differential form of the momentum equation in three dimensions is derived by applying Newton's second law to an element of fluid.¹⁴

$$\underbrace{\frac{\partial(\rho\mathbf{c})}{\partial t}}_{\text{Temporal acceleration}} + \underbrace{\nabla \cdot (\rho\mathbf{c}\mathbf{c})}_{\text{Spatial acceleration}} = \underbrace{-\nabla p + \rho\mathbf{g} + \nabla \cdot \boldsymbol{\tau}}_{\text{Applied forces}} , \quad (3.7-12)$$

where \mathbf{c} is the velocity vector, $\mathbf{c}\mathbf{c}$ is a vector multiplication that yields a 3×3 matrix, \mathbf{g} is the gravitational field vector, and $\boldsymbol{\tau}$ is the viscous stress tensor. Expanding the derivatives on the left yields

$$\rho \frac{\partial \mathbf{c}}{\partial t} + \mathbf{c} \frac{\partial \rho}{\partial t} + \mathbf{c} \nabla \cdot (\rho \mathbf{c}) + \rho \mathbf{c} \nabla \cdot \mathbf{c} = -\nabla p + \rho \mathbf{g} + \nabla \cdot \boldsymbol{\tau} . \quad (3.7-13)$$

Regrouping terms yields an expression in which the continuity equation emerges as a factor in the second term. This term is exactly zero.

$$\rho \frac{\partial \mathbf{c}}{\partial t} + \mathbf{c} \left[\frac{\partial \rho}{\partial t} + \nabla \cdot (\rho \mathbf{c}) \right] + (\rho \mathbf{c} \cdot \nabla) \mathbf{c} = -\nabla p + \rho \mathbf{g} + \nabla \cdot \boldsymbol{\tau} . \quad (3.7-14)$$

Applying that simplification yields the following equation:

$$\rho \frac{\partial \mathbf{c}}{\partial t} + \rho \mathbf{c} \nabla \cdot \mathbf{c} = -\nabla p + \mathbf{g} + \nabla \cdot \boldsymbol{\tau} . \quad (3.7-15)$$

The second term may be put into a form that is directly integrable along a streamline by using the following identity:

$$\mathbf{c} \nabla \cdot \mathbf{c} = \frac{1}{2} \nabla (|\mathbf{c}|^2) - \mathbf{c} \times (\nabla \times \mathbf{c}) . \quad (3.7-16)$$

The last term in (3.7-16) is identically zero so that the momentum equation may be written as

$$\rho \frac{\partial \mathbf{c}}{\partial t} + \frac{1}{2} \rho \nabla (|\mathbf{c}|^2) = -\nabla p + \mathbf{g} + \nabla \cdot \boldsymbol{\tau} . \quad (3.7-17)$$

Equations (3.7-12) and (3.7-17) are two forms of the same equation. Both are used for modeling turbomachines. The difference in the storage rate term accounts for the factor of one-half in the spatial acceleration. If a quasi-steady equation is formed by dropping the storage rate and simplifying to one dimension, then the momentum balance is different by the factor of one-half. The difference in the term

which is set to zero, $\frac{\partial(\rho \mathbf{c})}{\partial t}$ in the one case and $\frac{\partial \mathbf{c}}{\partial t}$ in the other that accounts for the difference in the equations. We will proceed from Eq. (3.7-17).

Before forming the control volume equations by integrating over the volume, the vector velocity needs to be converted into a scalar. Flow distribution and pressure distribution are fairly uniform across a cross-sectional area perpendicular to the direction of flow. Flow components in the cross-sectional area (i.e., normal to the direction of flow) are associated with turbulence and viscous dissipation. The usual approximation for dynamic models is to assume one-dimensional flow along a streamline to reduce the momentum equation to a scalar equation. Let s be the position variable along the streamline and c_s be the velocity in the streamline direction.

$$\rho \frac{\partial c_s}{\partial t} + \frac{1}{2} \rho \frac{\partial}{\partial s} (c_s^2) = -\frac{\partial}{\partial s} p + g \sin \theta + (\nabla \cdot \boldsymbol{\tau})_s , \quad (3.7-18)$$

where θ is the angle s makes with the horizontal. This form of the momentum equation can be integrated along a stream line. The effect on the fluid momentum of shaft work and viscous loss are incorporated through the $(\nabla \cdot \boldsymbol{\tau})_s$ term. Integration of the spatial acceleration term requires an approximation to bring the density inside the differentiation.

$$\int_{s_1}^{s_2} \rho \frac{\partial}{\partial s} (c_s^2) ds \approx \int_{s_1}^{s_2} \frac{\partial}{\partial s} (\rho c_s^2) ds = \rho_2 c_{s,2}^2 - \rho_1 c_{s,1}^2 . \quad (3.7-19)$$

This approximation is not very good for gas flow but is commonly made. The resulting integral equation is the following:

$$\bar{\rho} \frac{dc_s}{dt} + \frac{1}{2} (\rho_2 c_{s,2}^2 - \rho_1 c_{s,1}^2) = -(p_2 - p_1) + g(z_2 - z_1) + \int_{s_1}^{s_2} (\nabla \cdot \boldsymbol{\tau})_s ds . \quad (3.7-20)$$

The integral averages of velocity and density are obtained by the definitions:

$$\bar{c}_s = \frac{\int_{s_1}^{s_2} \rho c_s ds}{\int_{s_1}^{s_2} \rho ds} , \quad \bar{\rho} = \frac{\int_{s_1}^{s_2} \rho ds}{L_T} . \quad (3.7-21)$$

The term, $g(z_2 - z_1)$, is obtained from $\int_{s_1}^{s_2} \cos \theta ds = z_2 - z_1$. The variable, z , represents the elevation along the streamline.

The stress term, $(\nabla \cdot \boldsymbol{\tau})_s$, accounts for the interaction between the fluid and the solid surfaces in the control volume that result in both useful momentum gained or lost by the moving blades acting in the direction of flow (shaft work) or momentum lost through viscous dissipation. A rigorous assessment of the term is beyond the scope of this review. We can simplify the term into pressure change components due shaft work and viscous dissipation:

$$\int_{s_1}^{s_2} (\nabla \cdot \boldsymbol{\tau})_s ds = -\Delta p_{shaft} - \Delta p_{loss} . \quad (3.7-22)$$

In dynamic models using performance maps as in Eq. (3.7-9), the Δp_{shaft} comes from the performance map:

$$\Delta p_{shaft} = \Delta \hat{p}_0 = p_{01} \left(1 - \frac{\hat{p}_{02}}{p_{01}} \right). \quad (3.7-23)$$

The loss term is usually small. If it is accounted for in the model, it is usually approximated as a form loss of the following type:

$$\Delta p_{loss} = \frac{1}{2} K_{visc} \bar{\rho} \bar{c}^2. \quad (3.7-24)$$

Substituting the shaft and viscous terms into the momentum equation gives the following general form:

$$L_r \bar{\rho} \frac{d\bar{c}_s}{dt} + \frac{1}{2} (\rho_2 c_{s,2}^2 - \rho_1 c_{s,1}^2) = -(p_2 - p_1) + g(z_2 - z_1) - p_{01} \left(1 - \frac{\hat{p}_{02}}{p_{01}} \right) - \frac{1}{2} K_{visc} \bar{\rho} \bar{c}^2. \quad (3.7-25)$$

3.7.4 Quasi-steady approximations

The three conservation equations in integral form, Eqs. (3.7-10), (3.7-11), and (3.7-25), the performance map relationships Eqs. (3.7-8) and (3.7-9), and the ideal and perfect gas expressions form a system of algebraic and differential equations that is at least formally solvable. However, this fully dynamic form poses some numerical difficulties for the typical I&C application. In general, the path length through a stage group is small compared to the fluid velocity so that the time constants associated with the turbine or compressor are much smaller than those of the rest of a typical system model. Time constants associated with mass, energy, and momentum are on the order of path length over gas velocity and path length over sound velocity. Solving the conservation equations dynamically would make the system very stiff. If the differential equations are solved by explicit integration methods, a smaller time step would be required for the turbine and compressor components than for other parts of the model while capturing very little in the way of important system dynamics. Under these circumstances, it is generally appropriate to approximate one or more of the conservation equations as a quasi-steady process to improve efficiency of the numerical solution. Mathematically, the quasi-steady implies that the dynamic equation continuously and instantly returns to equilibrium, and the right hand side of the differential equation is perfectly a balanced algebraic expression. It is exactly the same as approximating the small actual volume of the stage group as a zero volume. For example, the quasi-steady approximation for mass equation is obtained by setting V in Eq. (3.7-10) to zero and yields a relation that states that the outlet flow is equal to the inlet flow. In general the same approximation is made throughout all stages so that a single uniform flow is used in a device as in the following:

$$\dot{m}_1 = \dot{m}_2 = \dot{m}. \quad (3.7-26)$$

The energy equation can be simplified in the same way as the mass equation by setting the volume to zero. Also, the potential energy and conducted energy terms are small and may be neglected. With these two approximations, the resulting energy equation is given by:

$$0 = \dot{m}_1 \left(h_1 + \frac{c_1^2}{2} \right) - \dot{m}_2 \left(h_2 + \frac{c_2^2}{2} \right) + W_{shaft} . \quad (3.7-27)$$

To simplify Eq. (3.7-27), the convected energy can be written in terms of the stagnation temperature and W_{shaft} may be replaced with the formula from Eq. (3.7-8). Assuming the quasi-steady continuity equation is also being applied, the energy equation may be solved for the stagnation temperature at the outlet of turbine and compressor, respectively.

$$\dot{m}_1 \left(h_1 + \frac{c_1^2}{2} \right) - \dot{m}_2 \left(h_2 + \frac{c_2^2}{2} \right) = \dot{m} C_p \left(T_1 + \frac{c_1^2}{2C_p} - T_2 - \frac{c_2^2}{2C_p} \right) = \dot{m} C_p (T_{01} - T_{02}) . \quad (3.7-28)$$

Substituting this result into Eq. (3.7-27) gives

$$\dot{m} C_p (T_{02} - T_{01}) = W_{shaft} . \quad (3.7-29)$$

Using the shaft work equations in Eqs. (3.7-6) or (3.7-7) and the performance map calculations of the power ratio from Eqs (3.7-4) or (3.7-5), the following result is obtained:

$$\begin{aligned} T_{02} = \hat{T}_{02} = T_{01} \left(1 + \frac{\Delta \hat{T}_c}{T_{01}} \right), \\ T_{02} = \hat{T}_{02} = T_{01} \left(1 - \frac{\Delta \hat{T}_t}{T_{01}} \right); \end{aligned} \quad (3.7-30)$$

Thus, for the quasi-steady approximation, the outlet temperature is computed directly from the performance map.

The quasi-steady momentum equation is obtained by the same approach.

$$0 + \frac{1}{2} (\rho_2 c_{s,2}^2 - \rho_1 c_{s,1}^2) = -(p_2 - p_1) + g(z_2 - z_1) + p_{01} \left(1 - \frac{\hat{p}_{02}}{p_{01}} \right) - \frac{1}{2} K_{visc} \bar{\rho} \bar{c}^2 . \quad (3.7-31)$$

The elevation term and the wall friction term are small for turbomachines and may be neglected. After applying these approximations and rearranging, the quasi-steady approximation gives

$$\left(p_2 + \frac{\rho_2 c_{s,2}^2}{2} - p_1 - \frac{\rho_1 c_{s,1}^2}{2} \right) = -p_{01} \left(1 - \frac{\hat{p}_{02}}{p_{01}} \right). \quad (3.7-32)$$

Using the definition of stagnation pressure gives the final result

$$\frac{p_{02}}{p_{01}} = \frac{\hat{p}_{02}}{p_{01}}. \quad (3.7-33)$$

In use, the turbine model would have a pipe or plenum upstream and downstream which gives the entering and leaving stagnation pressures. The performance map for pressure ratio gives the flow that matches the given pressure ratio and shaft angular speed.

When the turbine model is divided into many stage groups, a fully quasi-static model (all conservation equations are quasi-steady), the numerical problem is that the model is a system of nonlinear algebraic equations which cannot be solved analytically for the flows, pressures, and temperatures. Numerical solutions of the systems, with a finite accuracy, must be employed to find a solution. The error in the numerical solution of the system may interact adversely with the solution of the pressure and flow equations in the remainder of the plant model.

In models reviewed for this paper, MELCOR's approach is fully quasi-static. A numerical approach for iteratively solving the system of equations is described. For RELAP, the energy equation is quasi-steady, and the mass and momentum equations are solved dynamically as part of semi-implicit scheme for the full hydrodynamic network of the model. The user is advised to artificially increase the control volume length of inlet and outlet plena to make the system less stiff and alleviate numerical problems with the solution.

3.7.5 Conservation of angular momentum equation for shaft speed

The shaft momentum equation can be written in a number of ways depending on the phenomena of interest. If the shaft dynamics and flex oscillations are important, each component on the shaft could be represented with its own momentum equation and coupled to other components by a stiffness model of the shaft. More commonly, however, the I&C modeler is primarily interested in the heat transport and fluid systems, and the flexibility of the shaft is neglected. A typical shaft momentum equation representing the shaft as a rigid member is the following:

$$\underbrace{\left(I_t + I_c + I_{gen} \right) \frac{dN_{shaft}}{dt}}_{\text{Rate of change of angular momentum}} = \underbrace{\frac{\dot{W}_t}{N_{shaft}} - \frac{\dot{W}_c}{N_{shaft}} - \frac{\dot{W}_{gen}}{N_{shaft}} - \frac{\dot{W}_{losses}}{N_{shaft}}}_{\text{Torques applied to the shaft}}, \quad (3.7-34)$$

where I represents moment of inertia, N_{shaft} is the shaft angular speed, and \dot{W} is the work rate. The subscripts, t , c , gen , and $losses$ represent turbine, compressor, generator, and mechanical losses, respectively. The ratio of work rate to speed gives torque.

The model for shaft speed depends on the mode of operation. At least four should be considered:

1. generator synchronized to the grid,
2. generator operated as a motor by variable frequency generator,
3. generator tripped, and
4. broken shaft.

When the generator is connected to the grid, the shaft speed is fixed by the grid frequency. Small fluctuations about the grid frequency are present but are only important for voltage and frequency control for the grid. The effect on the fluid equations is small and generally neglected for fluid system models. The shaft equation is reduced using a quasi-steady approximation. The generator accepts the net power produced by the shaft perfectly and instantly. The shaft equation stays perfectly in equilibrium.

$$\dot{W}_{gen} = \dot{W}_t - \dot{W}_c - \dot{W}_{losses} . \quad (3.7-35)$$

The resulting shaft speed is simply the grid frequency:

$$N_{shaft} = N_{grid} , \quad (3.7-36)$$

where N_{grid} is the grid frequency with appropriate conversion factor for the number of poles in the generator.

Brayton cycle turbine generators are not self-starting; therefore, the shaft must be accelerated to speed by using the generator (or some auxiliary motor) as a motor to drive the shaft to starting speed. The expected configuration would have a variable frequency generator to gradually accelerate the shaft. In this case, the generator work can be renamed motor torque and is the result of the dynamic model of the variable frequency generator.

When the generator trips, the electrical load and synchronization are lost. The transient that follows is a concern because of the potential overspeed and the potential overheating of structural metal following the loss of heat removal. To protect the turbine and compressor, the turbine is bypassed and controls are activated to reduce the speed and coolant circulation. The shaft equation reduces to

$$\frac{dN_{shaft}}{dt} = \frac{\dot{W}_t - \dot{W}_c - \dot{W}_{losses} + \dot{W}_{motor}}{(I_t + I_c + I_{gen})N_{shaft}} , \quad (3.7-37)$$

where \dot{W}_{motor} represents the special case of the variable frequency generator connected to the generator operating as a motor.

3.7.6 Electric motor compressor shaft model

In plants that utilize a steam generator instead of a gas turbine for power removal from the primary loop, the compressor is powered by a variable speed electrical motor.

$$\frac{dN_{shaft}}{dt} = \frac{\dot{W}_{motor} - \dot{W}_c - \dot{W}_{losses}}{(I_t + I_c + I_{gen})N_{shaft}} \quad (3.7-38)$$

The model of the motor and motor controls are contained the \dot{W}_{motor} term. This term represents the dynamics of the voltage of the DC generator that ultimately control the shaft speed.

3.7.7 Compressor stall or surge

Compressor stall is the condition in which the blade flow separates from the blade airfoil resulting in a sudden change in performance. The basic phenomenon is the same as the stall of a fixed wing aircraft. The stall condition occurs when the airfoil angle of attack increases beyond the point of maximum lift and flow begins to separate at the trailing edge of the wing. In an axial compressor, the angle of attack of the blades varies with the flow and shaft rotational. Just as in aircraft wings under abnormal operating conditions, the angle can exceed limiting angle of attack. The condition can occur in a variety of modes and varying severity. Rotating stall involves localized stall cells of relatively stagnant flow that rotate around the circumference of the compressor. If the stall is due to a temporary external cause in the gas flow, the stall may be not significant. Under other circumstances, the compressor may stabilize at a steady although reduced compression than unstalled modeling would predict.

As the flow separation becomes limiting, the flow can reverse in the compressor resulting in a situation called axisymmetric stall or surge. This is a particularly dangerous condition. Frequently, the flow reversal reduces the pressure ratio across the stage so that positive flow resumes. Positive flow continues until the surge condition returns leading to a repeated cycle that can lead to high levels of vibration and potential destruction of the compressor.

The modeling of surge and stall is a difficult three-dimensional flow problem. In controls, the main objective is to maintain the compressor in safe, unstalled operating conditions. Models of compressor should provide stall limit curves to indicate the regions of safe and unsafe operation. If modeling of the stall or surge condition is necessary, then the points of discontinuity in the flow and temperature coefficients at the inception of stall and inception of surge must be accounted for in the numerical solution.

3.7.8 Steam turbine models

Steam turbine models are similar to gas turbines except that the steam cannot be approximated as an ideal or perfect gas. Steam properties replace the ideal gas relationships in the derivation. In steam cycles, it is usually necessary to perform steam extraction and moisture separation. In dynamic models, these flow terms for stage are provided by performance maps obtained from detailed engineering models of the turbine.

3.8 Steam Generator

Steam generator is a heat exchanger with gas as heat transfer fluid on the heating side and water boiling to steam on the cooling side. Generally, the steam generators are configured with water/steam on the tube

side and gas on the shell side. The steam side is typically higher pressure than the gas side. Because of the low heat transfer properties of helium gas, the steam generators are designed with a variety of tube configurations and extended surfaces to improve boiling stability.

To model the boiling process on the steam-water side, the heat transfer must represent the changes in the heat transfer regime as the fluid is heated from liquid to vapor. The heat transfer correlations generally divide the process into the following regimes:

- subcooled,
- nucleate boiling,
- film boiling, and
- superheat single phase.

Some designs of steam generators use separate bundles of tubes for each regime. Boiling can be isolated to a drum boiler designed to improve boiling stability. In this case each set of tubes is modeled as a separate heat exchanger.

Another approach to enhance heat transfer is the helical coil steam generator. In this design, the water/steam side is a bundle of helically curved tubes. The arrangement of flow in the steam generator has the primary (helium) coolant flowing downward in the shell and the secondary (water/steam) flowing upward in tubes which are coiled in helices. The curved tubes enhance the heat transfer on both the primary and secondary side. The primary coolant flow must flow almost perpendicular to the tube causing enhanced turbulence at the surface and a thinner boundary layer.^{15, p. 269} This effect improves the heat transfer roughly a factor of 3 compared to straight tubes. On the secondary side, the coolant must follow the curved path of the helix. The radial acceleration along the curved path produces different forces on the vapor and liquid due to their different speeds and densities. The liquid is driven toward the wall reducing the tendency of a vapor film to form between the water mixture and the wall. The heat transfer tends to keep a thin film of water on the tube surface which rapidly evaporates in a very efficient form of heat transfer. The secondary side heat transfer is two to five times more efficient than comparable boiling in straight tubes. Empirical correlations specifically for the helical tubes for pressure drop and heat transfer must be used to account for the enhanced fluid contact of the liquid and tube wall.

3.8.1 Tube heat transfer

The heat transfer rate at any point along a steam generator tube is proportional to the local temperature differences from primary to tube and tube to secondary. Since the primary and secondary fluid temperatures are only known at a finite number of points, some approximation of the temperature distribution between points must be made. The obvious and easy choice, such as the arithmetic average, leads to a very poor estimate of the heat transfer rate. Another common alternative is the log mean temperature difference. This scheme is based on the steady state temperature distribution and, thus, gives accurate results for slow transients. There are two problems with the log mean temperature difference. First, the scheme does not readily allow the tube metal thermal dynamics to be modeled, and, second, under transient condition, the argument of the logarithm can be negative which is not a valid mathematical operation. The argument of the logarithm is a ratio of temperature differences. At steady state, the ratio of temperature differences is always a positive number but can very easily be negative during a transient. Various approaches to deal with crossed temperatures are purely ad hoc and contribute an aphysical dynamic response.

A better alternative is to use a formula based on the heat exchanger effectiveness formulation by London and Kays¹⁶. The usual effectiveness formula consists of the maximum heat transfer rate times and effectiveness factor, ε . The maximum heat transfer rate is the rate that would occur if the heat transfer area were infinitely long or if the heat transfer coefficient were infinitely large.

3.8.2 Tube leak model for water ingress from water into gas side

One of the significant design basis transients for the NGNP designs is the steam generator tube leak. The pressure on the steam side of the steam generator is significantly higher than the gas side leading to water ingress events when tube leaks occur. The chemical reaction of water with the graphite in the core is one of the design basis events leading to core damage and radiation release. The safety model of the event is concerned with the consequences of the worst case events and conservative approximations are used. An I&C analysis is concerned with detectability and successful system response to limit the effects of the event. Simulation of the leak rate, accurate modeling of the propagation of the mixture of helium and steam to the location of detection, and a physical simulation of the detection mechanism is needed for I&C analysis. One of the more complex systems for protection against water ingress is the steam generator dump systems which rapidly drains the water from steam generator upon detection of moisture in the primary. The dump system is a protective response whose interactions with other protection and control systems must be simulated.

3.9 Instrumentation System

Instrumentation system includes components that are responsible for measuring a process variable. The sensing element of the measurement system is usually referred to as the sensor, transducer, or transduction element. Sensor is basically a device that converts (i.e., transduces) the physical quantity of interest into a useful signal—usually an electric signal. The measured process (pressure, temperature, flow, etc.) causes known variations in the transduction element, whose electrical response is correlated with the process. This correlation, $g(t)$ as shown in Fig. 9, is usually referred to as the response function—or the transfer function—of the transducer.

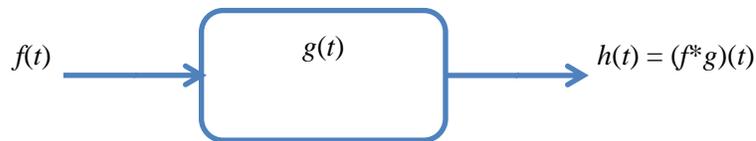


Fig. 9. Mathematical representation of signals in a sensing element: $f(t)$ is the process variable of interest, $g(t)$ represents the internal dynamics of the sensor, and $h(t)$ is the measured sensor signal, which is the convolution of $f(t)$ and $g(t)$.

Mathematically, the transfer function of the transduction element acts as a filter to the input signal and converts it into the output signal—usually electrical signal. The filtering process might involve large delays, which is usually the case for slowly acting processes, such as the temperature response of an RTD. These delays, as shown in Fig. 10, should be taken into account in determining the response of the instrumentation system as a whole. The delay parameters are particularly important in designing the control and protection systems.

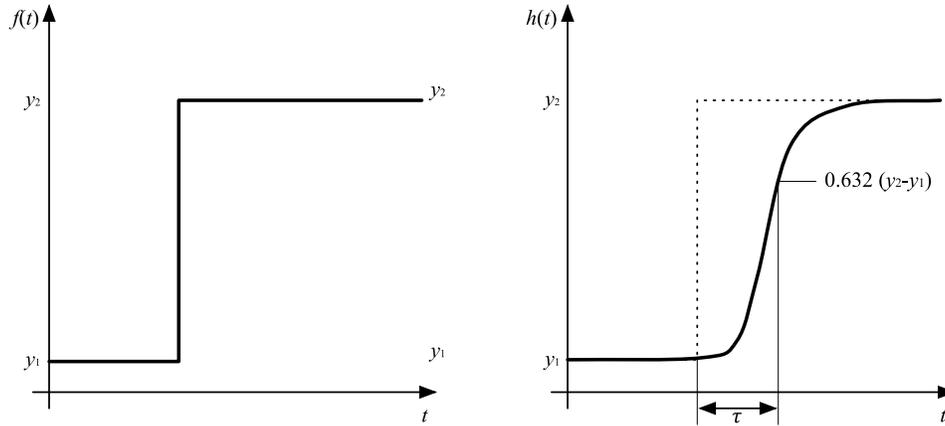


Fig. 10. Response of a first-order system to a step input signal— τ is called the time constant.

Once the sensor output is generated, the signal is processed through various analog, digital, or a combination of analog and digital components (e.g., preamplifier, amplifier, analog-to-digital, A/D converters and digital-to-analog, D/A converters, cables, etc.). Each component introduces its internal dynamics into the final signal generated in the process.

For control and protection system design purposes, sensor dynamics can be incorporated—in a simplistic way like a first- or second-order model—into integrated plant models to determine the overall response of the system. Models can be derived by simple analytical correlations or through experimental measurements. Usually, within the operating range of the sensor, there is a linear correlation between the measured quantity and the sensor response, which eliminates complex mathematical operations to convert the measured signal into a meaningful engineering quantity (calibration). Derivation of physical models of sensors can be found in the literature.¹⁷

3.10 Control System

A control system is defined as a device—or a series of devices—that regulate the behavior of other devices or systems. A schematic representation of a sensor, controller, and the controlled system is shown in Fig. 11. In this representation, the controller block includes the control unit as well as the requisite actuators to translate the controller output to the physical process. An actuator converts the output of the control unit into a mechanical response to introduce the appropriate change in the controlled system. An example might be controlling the opening of a throttle valve to regulate flow in a control volume.

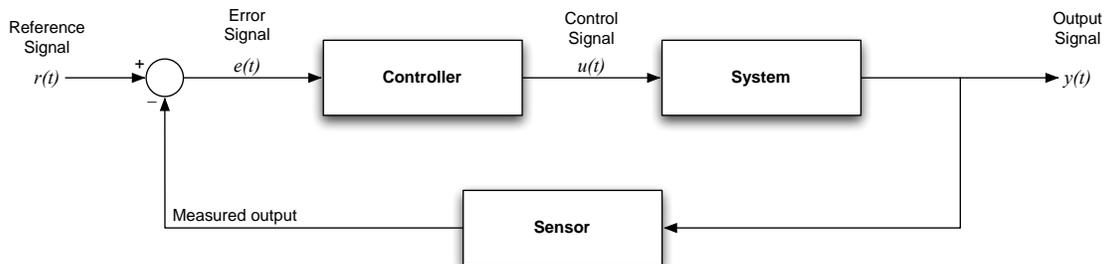


Fig. 11. A schematic representation of the control system.

The primary objective of a control system is to minimize the error signal, $e(t)$, which is defined as

$$e(t) = y(t) - r(t) , \quad (3.10-1)$$

where $y(t)$ is the output signal, and $r(t)$ is the reference signal. The design philosophy of a control system is that the overall system is stable—even if the controlled system or the process is inherently unstable.

The most common controller type is proportional-integral-derivative (PID) control, which is mathematically represented as

$$u(t) = K_p e(t) + K_i \int_0^t e(\tau) d\tau + K_d \frac{d}{dt} e(t) , \quad (3.10-2)$$

where K_p is the proportional gain, K_i is the integral gain, and K_d is the derivative gain. A proper controller design is achieved by tuning the gain parameters of each linear operator such that the overall system is demonstrated to be stable within a prescribed domain of input signals. PID controllers can be implemented directly by analog components.

Conventionally, the controller block includes analog passive and active components to generate the control output. For certain systems, the control block may contain only mechanical components (e.g., a relief valve to keep the pressure in a volume restricted within a threshold).

Other controller design strategies include, but not limited to, optimal control, robust control, fuzzy logic control, etc. These control strategies come at the cost of sophisticated mathematical operations that require high computational power and a lack of transparency in the response. Because the gas reactor is a slow responding system with large energy storage, PID control is expected to be sufficient to deliver desired performance. However, it is not optimal, and, for most cases, it is not a robust control design. Robustness might be desirable for certain processes or systems to ensure that the system dynamics is kept within certain bounds even though the input domain is allowed to deviate from the nominal ensemble of inputs.

Control system components are commonly represented graphically using a schematic of analog wiring diagrams as the model. The devices, such as summer, differencer, amplifier (gain), differentiator, and integrator, are represented individually as graphical blocks. An example implementation of a control system simulation is shown in Fig. 12.

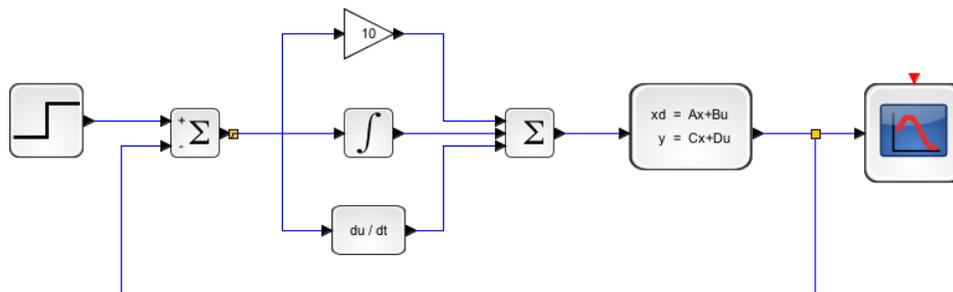


Fig. 12. An example implementation of a PID control system simulation.

The main concern of the models is to be able to interface the control design to the process in a simulation. Important issues include accuracy of representing digital time delay and discretization of measured values in analog to digital conversion.

3.11 Confinement and Containment

Modeling of confinement and containment are primarily a concern for depressurization events, although certain events such as station blackout could result in substantial cavity heat up events. Phenomena related to confinement and containment modeling include pressure, temperature, and gas composition transients in the reactor cavity confinement space during depressurization accidents. An example event is air ingress into the core through breaks in the reactor pressure vessel. This is a complex event involving multiple phenomena. Safety analysis of the confinement and containment is responsible for analyzing limiting cases to determine that the reactor fuel and structural components remain within design limits. Instrumentation and control analysis is concerned with the active control of any systems required to operate in the confinement and containment to detect and mitigate the event. In some designs, the confinement or containment involves more active control of venting and filtering than a corresponding LWR. Thus, some greater emphasis may be placed on the review of this part of the system. The I&C concerns are control and protection system interactions during the event, detectability of events at sensor locations, and survivability of I&C equipment under accident conditions.

The analysis requires that the geometry represented with a reasonably sized computation model which properly accounts for the transfer of heat and mass without making the simulation large and slow. Gas compositions in each node accounts for air, helium, reaction products due to oxidation, or water-graphite reaction. Considerations are needed for air in-leakage to confinement space and for any special injections of inert gas by the operators during recovery from a long-term accident.

3.12 Cavity

Rapid depressurization could possibly create large pressure waves, which could potentially damage safety systems, including the RCCS. Damage in the RCCS may result in loss of cooling functionality of the system—either partially or completely—hence, should be investigated for a consequential effect on essential instrumentation and controls which might be used to provide backup decay heat removal. Depressurization might also open up a release path for air and water ingress into the reactor cavity as well as for possible fission product transport out to the environment. The I&C requirement is to consider the event (depressurization) together with any potential consequential damage to the plant. The I&C role is to evaluate vulnerabilities to I&C equipment damage and then to evaluate consequence. The calculational model is usually limited to evaluation of the consequences.

The phenomena of interest for confinement and containment are significantly different than the phenomena involved in the containment of a light-water-cooled reactor. First, the lack of phase-change mechanism with helium may put the emphasis on gas cooling due to contact with the cavity structure. Helium, unlike steam, will not condense to reduce pressure in the reactor containment. As a result, a depressurization accident could retain the high pressure for a long time in the case of an airtight containment. Confinement strategies are based on a controlled release with suitable holdup and/or filtering for scenarios that may produce fuel damage and contamination products with the coolant release. Active control and monitoring play a larger role in the confinement strategy as the final barrier to radiation release.

Cavity cooling through the modeling of passive reactor cavity cooling system involves conductive, convective, and radiative cooling of the vessel walls. The reactor cavity cooling system loop involves a natural circulation connecting the heat exchangers in the cavity and outside the cavity. Operation of the

cavity cooling system is important for accident mitigation in the event of a station blackout. The operation of the system affects operability of equipment needed for long-term cooling.

3.12.1 Gas composition and temperature

The gas composition in the reactor cavity affects the reaction rates in material properties for heat transport. Temperature and pressure are the measureable variables which must be simulated. Combustible gases including CO from air ingress events and hydrogen from water ingress events must be considered in the simulation of the cavity and the operation of hydrogen and oxygen monitors based on location.

3.12.2 Gas stratification and mixing

Depressurization events will proceed with a distribution of temperature and composition. The mixing processes are driven by a combination of density differences due to varying concentrations or temperature and species diffusion. Three dimensional modeling of the containment is necessary to represent the distribution and their effect on sensors and other instrumentation and controls located in the containment/confinement cavity.

3.12.3 Air in-leakage

Air in-leakage into containment involves the concentration and distribution of oxygen. A major rupture of the reactor vessel and containment leads to a worst case air ingress event in which the oxygen supply is unlimited. The leakage models need to account for counter flow in a single break in which cold outside air enters at the bottom of a break while hot gases escape at the top.

3.12.4 Structural performance

Generally, while structural performance is a major issue for depressurization events, it is not a major issue in the I&C assessment. The issue in I&C is that sensors are provided in locations needed for monitoring structural performance.

3.12.5 Filters

For confinement strategies, depressurization events are expected to result in release of coolant from the confinement through filters. Filters are designed to remove radioactive particulate and reactive gases such as iodine. However, filter beds may be damaged by the high temperature of released reactor coolant gas. Certain filter bypass schemes may be utilized to allow hot uncontaminated gas to escape early in a depressurization transient to protect the filter beds from damage so that they are available if the event proceeds to core damage. The I&C issue is the ability of the control system to detect and respond correctly to conditions necessary for bypassing the filters. The performance of the beds for effectiveness of contamination removal and simulating conditions that might lead to failure due to high temperature are issues primarily for safety analysis but could also be part of the filters of the I&C analysis.

3.12.6 Dust and aerosol

Graphite dust from mechanical agitation particularly of pebble bed fuel is a concern. Metal fission products such as cesium and silver condense on the dust and the particulate may be carried with the escaping coolant in a depressurization event. The dispersion of the dust from a depressurization event is a concern. Safety analysis codes are used for estimating the radioactive release. The I&C issue is the modeling of radiation monitors. The simulation codes may be used to assess the location and effectiveness of monitors of dust and aerosol contamination.

3.12.7 Gas species retention

The objective of various reactive beds is to capture and retain gases through entrapment of particulate in the filter medium or the chemical reaction of gaseous radioactive species. The models of the beds are used to estimate the effectiveness of the filtration under a range of depressurization events and the effectiveness of control schemes to protect the beds from high-temperature uncontaminated gas.

3.12.8 Holdup

Holdup is the process of retaining gases that contain radioactive fission products long enough for the activity to decay to safe levels. The holdup takes place in the confinement cavity itself or gas may be compressed for retention in holdup tanks.

4. CHARACTERIZATION OF SELECT CODES FOR VHTR CONTROL SYSTEM ANALYSES

This chapter characterizes MELCOR-H2 and RELAP5 modeling codes for transient analysis of full gas-cooled reactor system and its associated instrumentation and controls for the NGNP.

4.1 RELAP5-3D

4.1.1 Introduction

RELAP5-3D is a transient analysis code for thermal-hydraulic systems. The main resource for this summary of capabilities is the RELAP5-3D[®] Code Manual¹⁸. The code was originally developed for modeling light water reactors. Historically, its main emphasis has been on modeling the two-phase flow phenomena in LWRs. The RELAP mathematical formulation of equations and reliable numerical scheme for modeling two-phase flow is generally viewed as one of the significant achievements in reactor safety. In the present, well-developed model, the hydrodynamic model is a transient, two-fluid model for flow of a vapor/gas and liquid mixture that can contain noncondensable components in the vapor/gas phase (e.g., hydrogen released from metal-water reactions) and/or a soluble component in the liquid phase (e.g., boric acid). The addition of coolants such as helium and liquid salts as well as gases representative of graphite-air and graphite-water reactions are described by Davis and Oh.¹⁹ A one-dimensional as well as a multidimensional hydrodynamic model is included. The term “two-fluid model” means that the liquid and vapor phases are modeled by separate energy, mass, and momentum conservation equations. The equations are coupled together with empirical relations that represent the energy, mass, and momentum exchange between the phases. Despite the emphasis on two-phase flow, the RELAP formulation reduces gracefully to a single-phase model that is suitable for other liquids and gases as coolants. The code also has the material properties of fluids such as helium, liquid metals, and liquid salts for coolants other than water. Additional noncondensable gases that would occur in air and water ingress events in high-temperature gas reactors have recently been added. The two-phase modeling emphasis means that RELAP has a very strong capability for water ingress events in NGNPs.

The RELAP code is a mature modeling tool. It is considered by many to be the standard reference for safety analysis of LWRs. The code is backed by both verification activities and a long history of usage in safety analysis for licensing. The scrutiny of results over time means that the likelihood of coding blunders is relatively small. The code has been qualified both theoretically and by comparisons to other codes and to experimental results. The verification efforts to date have been almost entirely for light-water conditions and events. The comparisons of simulation results against experiments and plant data have shown that with proper usage the results are accurate. The validation of gas reactor model benefits

from the formulation of equations, routines for material properties, heat transfer coefficients, pressure loss coefficients, and numerical schemes as well as the software engineering and procedures. The modeling of gas reactors by RELAP with their specific geometry or materials cannot be viewed as proven with quite the same confidence as results for LWRs; however, it should be recognized that the modeling of a single phase gas is a much simpler hydrodynamic problem than modeling two-phase water. Special geometries such as the pebble bed core, new heat exchanger configurations, and gas turbine and compressor models require additional experimental verification to give the same confidence in results as LWR components. However, the development program for the coding modifications and features for gas reactor benefits from residing within the same software engineering environment and utilizing the same code maintenance procedures that have been developed for the RELAP over the years.

The LWR applications for which the code was originally intended include small break loss-of-coolant accidents, operational transients such as anticipated transients without scram (ATWS), loss of feedwater flow, loss-of-offsite power (LOOP), and loss of force flow (LOFF) transients. The reactor coolant system (RCS) behavior can be simulated up to and slightly beyond the point of fuel damage. The applications for gas-cooled reactors are similar: pressurized and depressurized loss of forced circulation, reactivity insertions, turbine trip, loss of offsite power, and similar events can be simulated for HTGRs. The code has the ability to simulate a limited level of chemical reaction in gas and water ingress events up to the point the structural changes affect the flow.

The basic building block for a RELAP modeling system is a control volume. A control volume may be hydrodynamic control volumes, which represent the fluid or heat structures which represent solid materials. The fluid and energy flow paths in fluid control volumes are approximated by either one-dimensional stream tube or multidimensional models. The energy flow paths in solid heat conductors are approximated by either one-dimensional or two-dimensional heat conduction models. The philosophy of modeling is that system models are constructed from the control volumes; however, the code contains special system component models where needed. In particular, pumps, turbines, generator, valves, steam-water separator, and controls are included. Gas compressor and turbine models have been developed for gas reactor systems. The gas compressor and turbines are based on the pump and steam turbine models. Both a point kinetics model and a multidimensional nodal neutron kinetics model are included to simulate the neutron reaction.

RELAP5-3D[®] couples the neutron kinetics, thermal hydraulics, and mechanic (shaft work) interactions in reactor systems. It is designed to analyze how the components of a full system interact dynamically with one another. RELAP is constructed with the approximations and formulations that make a full-system model both possible from the standpoint of numerical stability and practical from the standpoint of computational time. RELAP offers both simplified one-dimensional flow solutions and multidimensional simulations of fluid flow and heat conduction within components as needed for the phenomena being simulated. One-dimensional flow is a very satisfactory approximation for most flow conditions in a reactor system. However, in situations such as cross flow mixing in a core, a multidimensional model can be used to model the spatial distribution effects of flow and temperature. The multidimensional model has been used only for a coarse nodal model. It is not clear if multidimensional modeling is capable or practical at a dimensional scale to represent flow in a pebble bed or to model the hot jets in the lower plenum of a prismatic core.

RELAP5-3D has been used in an integrated code system configuration that consists of CFD codes such as FLUENT and CFX, and the containment dynamics simulation code CONTAIN^{*}.²⁰ In one application, a framework for message-passing interface was created by Weaver et al in which the parallel virtual machine (PVM) allowed the coordination of execution of the coupled codes.²¹ This framework was used

*CONTAIN is a containment modeling and dynamics simulation tool developed by SNL.

to couple RELAP5-3D to CFDS-FLOW3D—now called CFX and owned by ANSYS—for demonstration of a proof-of-principle calculation.²² A similar framework was used to analyze the temperature and flow characteristics of the hot-gas streams in the outlet plenum of a VHTR.²³

The RELAP5 code package includes the capability to model a control system. The control system model provides basic mathematical operations, such as addition, multiplication, integration, and control components such as proportional-integral, lag, and lead-lag controllers, for use with the basic fluid, thermal, and component variables calculated by the remainder of the code. This capability can be used to construct models of system controls or can be used to create special purpose physical models of phenomena that can be described by algebraic and differential equations. The control system or component models may also be entered as user-defined FORTRAN subroutines that are linked to the main RELAP model. The control system package is limited to the algebraic operations without accounting for digital hardware effects, such as discrete-time sampling, latency, and communications.

The code's numerical solution includes the evaluation and numerical time advancement of the control system coupled to the fluid and thermal system. The control system is advanced explicitly with the energy equations. The scheme is described as a semi-implicit scheme, which means that the pressure and flow equations are solved implicitly while the energy equation is solved explicitly at each time step.

The point reactor kinetics model is advanced in a serial and implicit manner. Its calculation is performed after the heat conduction-transfer and hydrodynamic advancements but before the control system advancement. The kinetics model consists of a system of ordinary differential equations integrated using a modified Runge-Kutta technique. The integration time step is regulated by a truncation error control and may be less than the hydrodynamic time step; however, the thermal and fluid boundary conditions are held fixed over each hydrodynamic time interval. The reactivity feedback effects of fuel temperature, moderator temperature, moderator density, and boron concentration in the moderator are evaluated using averages over the hydrodynamic control volumes and associated heat structures that represent the core. The averages are weighted averages established a priori such that they represent the effect on total core power.

Certain nonlinear or multidimensional effects caused by spatial variations of the feedback parameters cannot be accounted for with such a model. Thus, the user must judge whether or not the model is a reasonable approximation of the physical situation being modeled. A multidimensional nodal neutron kinetics model is also available.

The control system model provides a way for simulating any lumped process, such as controls or instrumentation, in which the process can be defined in terms of system variables through logical, algebraic, differentiation, or integration operations. These models do not have a spatial variable and are integrated with respect to time. The control system is coupled to the thermal and hydrodynamic components serially and implicitly. The control system advancement occurs after the heat conduction transfer, hydrodynamic, and reactor kinetics advancements and uses the same time step as the hydrodynamics so that new time thermal and hydrodynamic information is used in the control model advancement. However, the control variables are fed back to the thermal and hydrodynamic model in the succeeding time step (i.e., they are explicitly coupled).

RELAP5-3D was recently modified to include all the Advanced THERmal Energy Network Analysis (ATHENA) code features and models that were previously only available in the ATHENA configuration. ATHENA includes a number of coolants that can be used as the working fluid, including helium, nitrogen, sodium, potassium, lithium, hydrogen, carbon dioxide, ammonia, glycerin, lead-bismuth, lithium-lead, and sodium-potassium.²⁰

The basic properties for helium are calculated from thermodynamic tables that tabulate saturation properties as a function of temperature, saturation properties as a function of pressure, and single-phase properties as a function of pressure and temperature. The properties and derivatives in the tables are

saturation pressure, saturation temperature, specific volume, specific internal energy, isobaric thermal expansion coefficient, isothermal compressibility, and specific heat at constant pressure. The transport properties, such as viscosity, thermal conductivity, and surface tension, are calculated from formulations based on least square fits to the available data. Other noncondensable gases, such as oxygen and carbon monoxide, were also incorporated to support analysis of HTGRs.¹⁹ This capability is critical to simulate the effects of air ingress on graphite oxidation following a depressurization accident.

Helium and nitrogen were used in the scoping transient analysis of the VHTR concept, which simulated the low- and high-pressure loss of forced convection cooling transients.^{24,25} Another study used RELAP5-3D[®] to analyze the potential of flow laminarization in a gas-cooled fast reactor (GFR) concept.²⁶ Dostal et al. designed a power conversion system with supercritical carbon dioxide as the working fluid using RELAP5-3D for a GFR concept.⁷ A new compressor model was developed to support gas-cycle applications derived from first principles and implemented into RELAP5-3D.²⁷

A system code such as RELAP5-3D[®] contains numerous approximations to the behavior of a real, continuous system. These approximations are necessitated by the finite storage capability of computers, by the need to obtain a calculated result in a reasonable amount of computer time, and in many cases because of limited knowledge about the physical behavior of the components and processes modeled. For example, knowledge is limited for components such as pumps and separators, processes such as two-phase flow, and heat transfer. Examples of approximations required because of limited computer resources are limited spatial nodalization for hydrodynamics, heat transfer, and kinetics; and density from thermodynamic property tables. In general, the accuracy effect of each of these factors is of the same order; thus, improving one approximation without a corresponding increase in the others will not necessarily lead to a corresponding increase in physical accuracy. At the present time, very little quantitative information is available regarding the relative accuracies and their interactions. What is known has been established through applications and comparison of simulation results to experimental data. Progress is being made in this area as the code is used, but there is, and will be for some time, a need to continue the effort to quantify the system simulation capabilities.

4.2 RELAP5 Transient Overview

The top-level functional structure of RELAP5-3D[®] that carries out the transient calculations is shown in Fig. 13. An executive code, call *driver*, handles calls to the relevant modules according to their respective input descriptions. Modules of interest for control system simulations are briefly discussed in the subsequent sections.

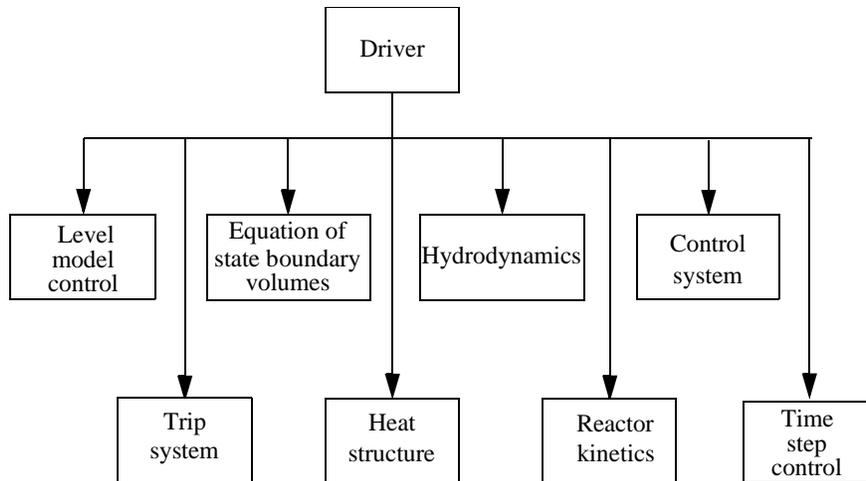


Fig. 13. Top-level block diagram of modules that show the component functional relationship for transient calculations in RELAP5-3D[®].

A block diagram structure of the subroutines for steady state and transient calculations is shown in Fig. 14. The subroutine TRNCTL consists only of the logic to call the next lower level routines. Subroutine TRNSET performs final cross-linking of information between data blocks, sets up arrays to control the sparse matrix solution, establishes scratch workspace, and returns unneeded computer memory. Subroutine TRAN, the driver, controls the transient advancement of the solution.

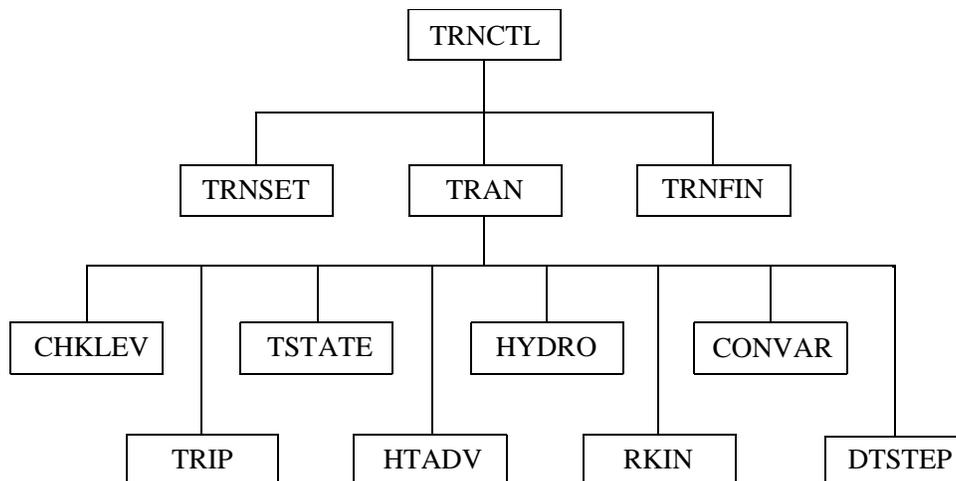


Fig. 14. Block diagram structure of subroutines for transient and steady state calculations.

The level module (CHKLEV) controls the movement of two-phase levels between volumes.

The trip system module (TRIP) evaluates logical statements. Each trip statement is a simple logical statement that has a true or false result. The decision of what action is needed resides within the components in other modules. For example, valve components are provided that open or close the valve based on trip values; pump components test trip status to determine whether a pump electrical breaker has tripped.

The equation of state boundary volume module (TSTATE) calculates the thermodynamic state of the fluid in each hydrodynamic boundary volume (time-dependent volume). This subroutine also computes velocities for the time-dependent junctions.

The heat structure module (HTADV) advances heat conduction/transfer solutions. It calculates heat transferred across solid boundaries of hydrodynamic volumes.

The hydrodynamics module (HYDRO) advances the hydrodynamic solution.

The reactor kinetics module (RKIN) advances the reactor kinetics of the code. It computes the power behavior in a nuclear reactor using the space-independent or point kinetics approximation, which assumes that power can be separated into space and time functions. It also optionally computes the power using a multidimensional nodal kinetics model.

The control system module (CONVAR) provides the capability of simulating control systems typically used in hydrodynamic systems. It consists of several types of control components. Each component defines a control variable as a specific function of time-advanced quantities. The time-advanced quantities include quantities from hydrodynamic volumes, junctions, pumps, valves, heat structures, reactor kinetics, trip quantities, and the control variables themselves. This permits control variables to be developed from components that perform simple, basic operations.

The time step control module (DTSTEP) determines the time step size, controls output editing, and determines whether the transient advancements should be terminated.

In the next sections of this volume of the manual, the various transient modules will be discussed. These are in the following order: hydrodynamics, heat structures, trips, control system, reactor kinetics, and special techniques (includes time step control).

4.3 RELAP5 Modeling Overview

RELAP5-3D[®] is designed for use in analyzing nuclear power plant system component interactions of the reactor and heat transport systems; it offers both one-dimensional and multidimensional simulations of fluid flow within components. Multidimensional effects for fluid flow, heat transfer, or reactor kinetics may be modeled. The multidimensional flow model allows the modeling of crossflow effects in a pressurized-water reactor (PWR) core. The reflood modeling uses a two-dimensional conduction solution in the vicinity of a quench front. To further enhance the overall system modeling capability, a control system model is included.

4.3.1 Hydrodynamic model

The hydrodynamic model is based on fluid control volumes and junctions to represent the spatial arrangement of the flow. For the one-dimensional flow model, the control volumes can be viewed as stream tubes having inlet and outlet junctions. Each control volume has a defined positive direction of flow from the inlet to the outlet ports of the control volume. Control volumes are connected in series, using junctions between control volumes to represent a flow path. Fluid velocities are computed only at the junctions and are associated with mass and energy flow between control volumes. All internal flow paths, such as recirculation flows, must be explicitly modeled since only single liquid and vapor/gas velocities are represented at a junction. (In other words, a countercurrent liquid-liquid or gas-gas (as in air ingress events) flow cannot be represented by a single-junction.) For flows in pipes, there is little confusion with respect to nodalization. However, in a steam generator having a separator and recirculation flow paths, some experience is needed to select a nodalization that will give correct results under all conditions of interest. Nodalization of branches or tees also requires an understanding of the RELAP junction model. For the multidimensional model, use of control volumes and junctions are also used based on Cartesian or cylindrical coordinates. The three-dimensional model is intended as a coarse-

mesh, average flow representation. The three-dimensional model is not suitable for small-scale geometric features such as individual fuel pins and grid plates. It is unclear if the three-dimensional model is accurate or practical for the simulation of hot jets in the lower plenum of prismatic cores.

4.3.2 Heat structures model

The heat structure is a solid control volume used to represent walls and other structural material, which contributes dynamically to thermal storage in system. Heat conduction flow paths are usually modeled in a one-dimensional sense, using a finite difference mesh to calculate temperatures and heat flux vectors. The heat conductors can be connected to hydrodynamic volumes to simulate a heat flow path normal to the fluid flow path. The heat conductor or heat structure is thermally connected to the hydrodynamic volume through a heat flux that is calculated using heat transfer correlations. Electrical or nuclear heating of the heat structure can also be modeled as either a surface heat flux or as a volumetric heat source. The heat structures are used to simulate pipe walls, heater elements, nuclear fuel pins, and heat exchanger surfaces.

A special two-dimensional, heat conduction solution method with an automatic fine mesh rezoning in the vicinity of the liquid level is used for low-pressure reflood (for LWR safety cases). Both axial and radial conduction are modeled, and the axial mesh spacing is refined as needed to resolve the sharp axial thermal gradient at the liquid-vapor interface. The hydrodynamic volume associated with the heat structure is not rezoned, and a spatial boiling curve is constructed and used to establish the convection heat transfer boundary condition. At present, this capability is specialized to the LWR core reflood process, but the plan is to generalize this model to higher pressure situations so that it can be used to track a quench front anywhere in the system. This feature is not needed for the single-phase gas reactor systems. It is not clear if the low-pressure reflood modeling would be usable or adaptable for large-scale water ingress into the reactor.

4.3.3 Radiation enclosure model

RELAP5-3D[®] models the radiative heat exchange between heat structures using a lumped-system approximation for gray diffuse surfaces contained in an enclosure. The surfaces that have a line of sight or a reflection path through which they can communicate with each other are considered to be in the same enclosure. This method has the following assumptions:

1. the fluid in the enclosure neither emits nor absorbs radiant thermal energy;
2. reflectance from a surface is neither a function of incident, nor reflected direction, nor of radiation frequency; and
3. temperature, reflectance, and radiosity* are constant over each surface.

The energy balance for the i -th surface can be written as

$$R_i A_i = \varepsilon \sigma T_i^4 A_i + \rho_i \sum_{j=1}^n R_j F_{ji} A_j , \quad (4.3-1)$$

*Radiosity of a surface is defined as the radiant energy flux leaving the surface (i.e., the emitted and reflected energy fluxes combined).

where R is the radiosity (energy flux) in W/m^2 , ε is emissivity (dimensionless), σ is the Stephan-Boltzmann constant in W/m^2K^4 , T is the surface temperature in K, $\rho = 1 - \varepsilon$ is reflectivity (dimensionless), F_{ij} is the view factor from surface j to surface i , and A_i is the area of surface i . The view factors from each surface to all other surfaces in an enclosure must sum to unity.

4.3.4 Reactor kinetics model

RELAP5-3D supports two levels of reactor kinetics modeling: point reactor and multidimensional kinetics models. Point reactor model is the simplest way of modeling the dynamics of a reactor system. However, point reactor model is not useful if spatial information is necessary, for instance, for simulating xenon dynamics or implementing control rod effects. For these cases, multidimensional kinetics support built into RELAP5 can be used.

4.3.4.1 Point reactor kinetics model

The point reactor kinetics model is advanced in a serial and implicit manner after the heat conduction-transfer and hydrodynamic advancements but before the control system advancement. The kinetics model consists of a system of ordinary differential equations integrated using a modified Runge-Kutta technique. The integration time step is regulated by a truncation error control. These models do not have a spatial variable and are integrated with respect to time.

4.3.4.2 Multidimensional neutron kinetics

The multidimensional neutron kinetics model in the RELAP5-3D[®] code was developed to allow the user to model reactor transients where the spatial distribution of the neutron flux changes with time. The model is based on the NESTLE code developed at North Carolina State University.²⁰ The model solves the few-group neutron diffusion equation utilizing the nodal expansion method (NEM). It can solve the steady state eigenvalue (criticality) and/or eigenvalue-initiated transient problems.

The neutron kinetics model in NESTLE and RELAP5-3D[®] uses the few-group neutron diffusion equations. Two or four energy groups can be utilized, with all groups being thermal groups—if desired. Core geometries include Cartesian and hexagonal. Three-, two-, and one-dimensional models can be utilized. Various core symmetry options are available, including quarter, half, and full core for Cartesian geometry and one-sixth, one-third, and full core for hexagonal geometry. Zero flux, nonreentrant current, reflective, and cyclic boundary conditions are treated.

The few-group neutron diffusion equations are spatially discretized utilizing the NEM. Quartic or quadratic polynomial expansions for the transverse integrated fluxes are employed for Cartesian or hexagonal geometries, respectively. Transverse leakage terms are represented by a quadratic polynomial or constant for Cartesian or hexagonal geometry, respectively. Discontinuity factors (DFs) are utilized to correct for homogenization errors. Transient problems utilize a user-specified number of delayed neutron precursor groups. Time discretization is done in a fully implicit manner utilizing a first-order difference operator for the diffusion equation. The precursor equations are analytically solved assuming the fission rate behaves linearly over a time-step.

Independent of problem type, an outer-inner iterative strategy is employed to solve the resulting matrix system. Outer iterations can employ Chebyshev acceleration and the Fixed Source Scaling Technique to accelerate convergence. Inner iterations employ either color line or point successive over-relaxation (SOR) iteration schemes, dependent upon problem geometry. Values of the energy group dependent optimum relaxation parameter and the number of inner iterations per outer iteration to achieve a specified L_2 relative error reduction are determined a priori. The nonlinear iterative strategy associated with the NEM method is utilized. This has advantages in regard to reducing FLOP count and memory size requirements compared to the more conventional linear iterative strategy utilized in the surface response

formulation. In addition, by electing not to update the coupling coefficients in the nonlinear iterative strategy, the finite difference method (FDM) representation, utilizing the box scheme, of the few-group neutron diffusion equation results. The implication is that the model can be utilized to solve either the nodal or FDM representation of the few-group neutron diffusion equation.

The neutron kinetics subroutines require as input the neutron cross sections in the computational nodes of the kinetics mesh. A neutron cross-section model has been implemented that allows the neutron cross sections to be parameterized as functions of RELAP5-3D[®] heat structure temperatures, fluid void fraction or fluid density, poison concentration, and fluid temperatures. A flexible coupling scheme between the neutron kinetics mesh and the thermal hydraulics mesh has been developed to minimize the input data needed to specify the neutron cross sections in terms of RELAP5-3D[®] thermal hydraulic variables. A control rod model has been implemented so that the effect of the initial position and subsequent movement of the control rods during transients may be taken into account in the computation of the neutron cross sections. The control system has been modified to allow the movement of control rods by control variables.

This model has not yet been applied to gas reactor cores.

4.3.5 Component models

RELAP5-3D[®] consists of a variety of generic models that are used to build system models. Generally speaking, system component models—such as the core, steam generator, etc.—are not provided as standard components due to the sheer variability of their design. However, certain models for subsystem components—such as a branch, separator, jet mixer, pump, turbine, valve, accumulator, emergency core cooling (ECC) mixer, annulus, pressurizer, and feedwater heater—are included as built-in models in RELAP5-3D[®]. Brief descriptions of the models from the RELAP5 code manual¹⁸ are provided below.

4.3.5.1 Branch

The branch component is a model designed for convenient interconnection of hydrodynamic components. The identical result can be obtained by using a single-volume component and several single-junction components.

The *one-dimensional branch* model is consistent with the one-dimensional approximation for a piping network and assumes that multidimensional effects at branches are small compared to system interaction effects. In the case of branched flows that occur in headers or plena, this model gives an accurate physical description of the flow division or merging process. Examples of such situations in LWR systems are flow divisions at the core inlet if parallel flow paths through the core are modeled; steam generator inlet and outlet plena when several parallel tube groups are modeled for the effect of tube height and length. A graphical representation of the one-dimensional branch is shown in Fig. 15.

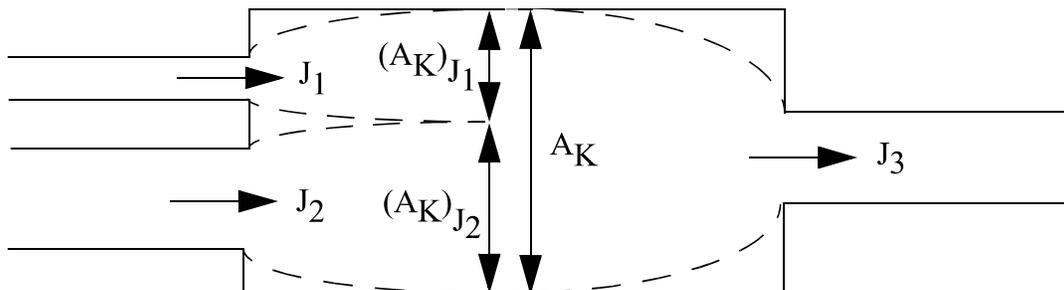


Fig. 15. Graphical representation of a one-dimensional branch.¹⁸

RELAP5-3D[®] comes with additional branch models, including the *tee branch* and the *crossflow branch*. The tee branch is, in fact, modeled as a crossflow branch. Examples of crossflow branches include the cold or hot leg connections in PWR systems.

4.3.5.2 Separator

PWR and boiling-water reactor (BWR) systems use a steam separator to increase the quality of steam before the fluid enters turbine. In addition, steam dryers are used to further increase the quality of the steam to at least 99.9%. The physics being modeled is the removal of water from the two-phase fluid, which is exiting either the core in a BWR or the steam generator in a PWR. The separator model consists of three regions: a standpipe, the separator barrel, and the discharge passage.

The separator component as modeled in RELAP5-3D has two different implementations—the *simple separator model*, and a *mechanistic separator model*, which was intended to model the centrifugal separators and chevron dryers in BWRs. The *simple separator model* is a nonmechanistic model that consists of a special volume with junction flows as depicted in Fig. 16.

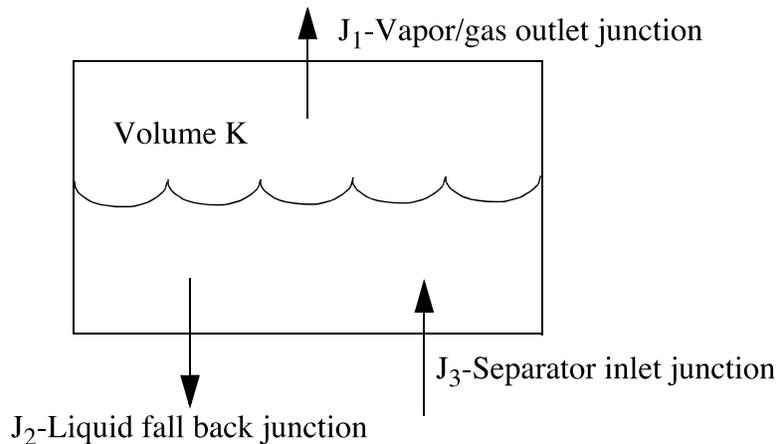


Fig. 16. Typical separator volume and junctions.¹⁸

The *mechanistic separator* component model consists of a special volume with three junction flows as shown in Fig. 16. A vapor/gas-liquid inflowing mixture is separated by defining the quality of the outflow streams using mechanistic models of the separating process in the separator and dryer components. The separator model may also be incorporated in multi-tube bundle steam generators where separators are employed.

4.3.5.3 Jet mixer

The *jet mixer* component is used for cases where the momentum effects due to the mixing of two parallel streams of fluid at different velocities may be important. An example of this is the jet pump in a BWR, where the suction force is generated by the momentum transfer between the two fluid streams.

The basic approach in modeling the *jet mixing* is by superimposing a quasi-steady model for the mixing process on the normal volume-junction flow path representation used in RELAP5-3D[®]. A graphical representation of this modeling approach is shown in Fig. 17.

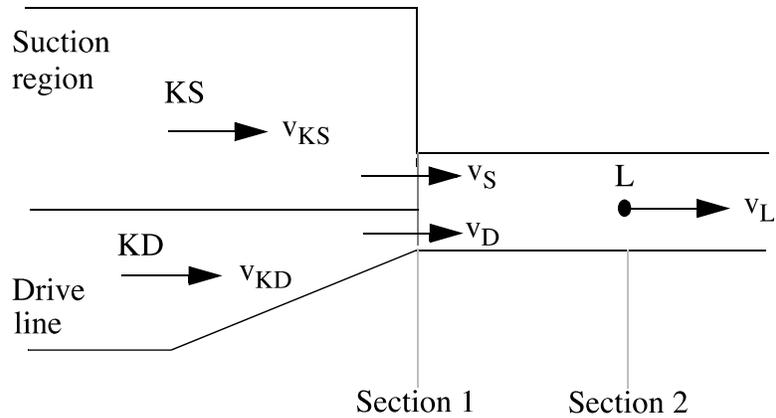


Fig. 17. Schematic of mixing junctions.¹⁸

4.3.5.4 Pump

The basic approach to pump modeling is to superimpose a quasi-static model for pump performance on the RELAP5-3D[®] volume-junction flow path representation. The pump is a volume-oriented component, and the head developed by the pump is apportioned equally between the suction and discharge junctions that connect the pump volume to the system. The pump model is interfaced with the two-fluid hydrodynamic model by assuming the head developed by the pump is similar to a body force. Thus, the head term appears in the mixture momentum equation; but, like the gravity body force, it does not appear in the difference momentum equation. The term that is added to the mixture momentum equation is $\frac{1}{2} \rho_m g H$, where H is the total head rise of the pump (m), ρ_m is the volume fluid density (kg/m^3), and g is the gravitational acceleration (m^2/s).

The *centrifugal pump performance model* depends on pump performance data, which must be generated experimentally. Analytic models exist that rely on first-principle calculations and are reasonably successful in predicting near-design pump performance for single fluids. However, for off-design operation or for operation with a two-phase fluid, these predictions fail to represent the actual values.

The basic parameters that characterize the pump performance are the rotational speed, ω , the volumetric flow, Q , the head rise, H , and the shaft torque, τ . The relationship between these four parameters can be uniquely displayed by a four-quadrant representation as shown in Fig. 18.¹⁸

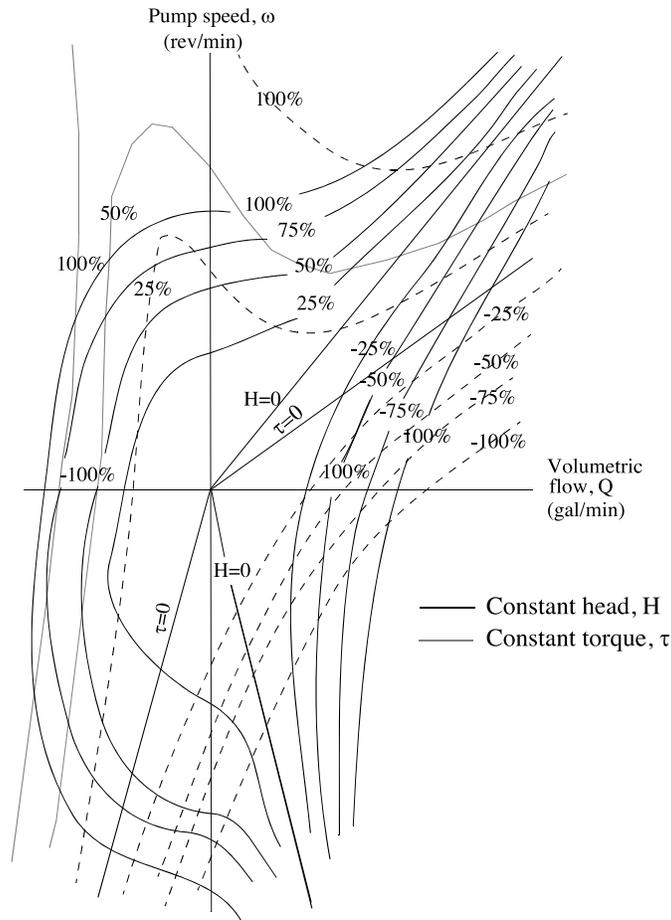


Fig. 18. Four-quadrant curves that represent typical pump characteristics.¹⁸

The *centrifugal pump drive model* uses the pump torque to calculate the pump speed, ω , after the pump is shut off by the input trip signal. The speed is calculated by the deceleration equation

$$I \frac{d\omega}{dt} = \tau . \quad (4.3-2)$$

The total pump torque is calculated by considering the hydraulic torque from the homologous curves and the pump frictional torque.

The capability to simulate a locked-rotor condition of the pump is included in RELAP5-3D[®], which provides capability for simulating the pump rotor lockup as a function of input elapsed time, maximum forward speed, or maximum reverse speed. At the time the rotor locks, the pump speed is set to zero.

4.3.5.5 Turbine

RELAP5-3D[®] uses a lumped-parameter turbine model, where a sequence of turbine stages—referred to as a stage group—is treated as a single junction and a single volume, as depicted in Fig. 19. The stage group is then represented using modified energy continuity and momentum equations. An efficiency factor based on simple momentum and energy considerations is used to take into account nonideal internal processes.

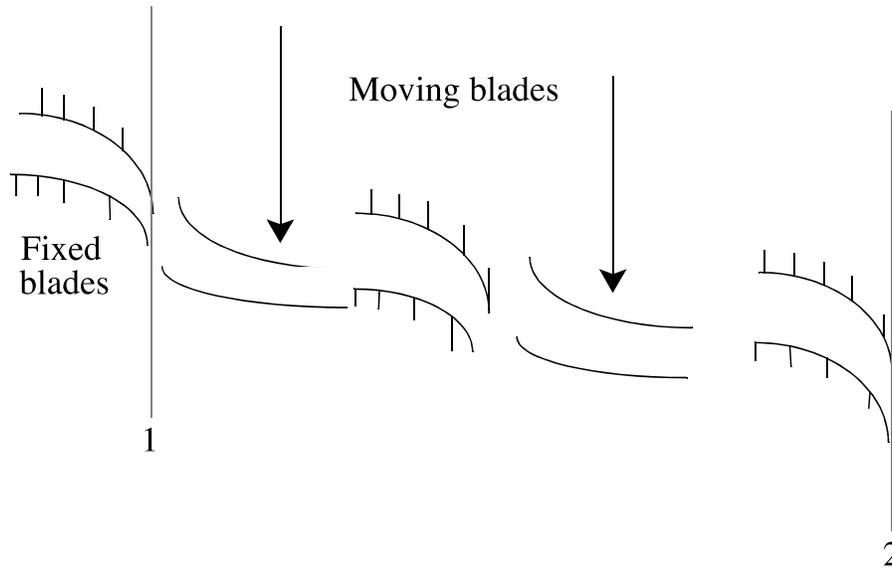


Fig. 19. Graphical representation of a turbine stage group with idealized flow between points 1 and 2.¹⁸

The *single-stage turbine model* represents the most general turbine model—also called a Type 1 turbine—included in RELAP5-3D[®]. This model considers a single-row fixed-blade system followed by a single-row rotating blade system.

The *two-stage impulse turbine* is the second turbine design that comes as a built-in component model. This model implements a two-row impulse stage—also called a Type 0 turbine (i.e., a nozzle), a moving constant-area blade passage, a fixed constant-area stationary passage, and a final constant-area moving-blade passage, which is modeled as a single-stage group.

Power/torque output of turbine

The relationship between power and torque for a rotating shaft is

$$\dot{W} = \tau\omega , \quad (4.3-3)$$

where \dot{W} is the power, τ is the torque, and ω is the shaft rotational velocity.

4.3.5.6 Valves

Valves are quasi-steady models that are used either to specify an option in a system model or to simulate control mechanisms in a hydrodynamic system. The valve models can be classified into two categories: (1) valves that open or close instantly and (2) valves that open or close gradually. Either type can be operated by control systems or by flow dynamics.

Valves in the first category are trip valves and check valves. The model for these valves does not include valve inertia or momentum effects. Valves in the second category are inertial swing check valve, the motor valve, the servo valve, and the relief valve. The inertial valve and relief valve behavior is modeled using force equations. The motor and servo valves use differential equations to control valve movement.

The operation of a *trip valve* depends solely on the trip signal selected. An abrupt opening or closing is imposed based on the trip condition. A latch option is also included.

The operation of a *check valve* is specified to open or close by a static differential pressure, to open by static differential pressure and close by flow reversal, or to open by static differential pressure and close by dynamic differential pressure. All check valves may be initialized as open or closed. Leakage is also allowed if the valve is closed, and the abrupt area change model is used to calculate the valve form losses.

The *inertial valve* models the motion of the valve flapper assembly in an inertial-type check valve. The abrupt area change model is used to calculate kinetic form losses. A graphical representation of the model is shown in Fig. 20. The valve flapper disc resides in a pipe and swings about the hinge. These valves are generally used to prevent a backflow from occurring.

The *motor valve* has the capability to control the junction flow area between two control volumes as a function of time. The operation of the valve is controlled by two trips: one for opening the valve and a second for closing the valve. A constant rate parameter controls the speed at which the normalized valve area changes. The first option for the motor valve is to use the abrupt area change model to calculate kinetic form losses with respect to the valve area. A second option is provided for the motor valve that allows for the specification of valve flow coefficients, C_v , using the smooth area change model. These coefficients can be specified using a general table of C_v verses normalized stem position. The energy loss coefficient is calculated using the valve flow coefficient by the following formula:

$$K = 2C \frac{A_{valve}^2}{C_v^2 \rho_0}, \quad (4.3-4)$$

where ρ_0 is the density of liquid water at 15°C and 0.1 MPa.

4.3.5.7 Accumulator

The accumulator model features the mechanistic relationships for hydrodynamics, heat transfer from the tank wall and liquid surface, condensation in the vapor/gas dome, and vaporization from the liquid surface to the vapor/gas dome. The geometry of the tank can be selected either cylindrical or spherical. The accumulator model also includes a surge line and an outlet check valve junction.

RELAP5-3D[®] models the accumulator as lumped-parameter component, which is based on the assumptions that (1) the spatial gradients in the accumulator tank are expected to be small and (2) a simple gas ideal gas equation of state can be used.

The geometric elements used in the hydrodynamic model of the accumulator are shown in Fig. 22 (a) and (b) for the cylindrical and spherical designs, respectively.

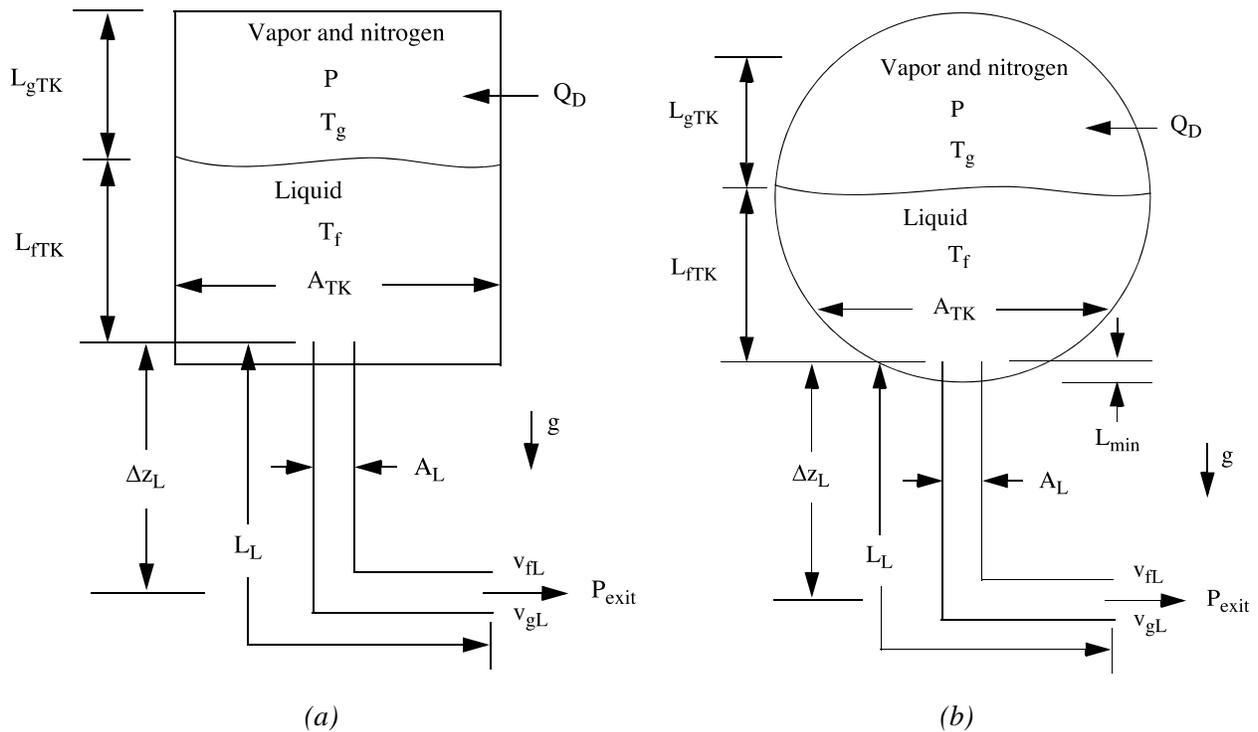


Fig. 22. Typical (a) cylindrical and (b) spherical accumulator modeled in RELAP5-3D[®].¹⁸

Other model assumptions are as follows:

1. Heat transfer from the accumulator walls and mass transfer from the liquid are modeled using natural convection correlations, assuming similarity between heat and mass transfer from the liquid surface.
2. The vapor/gas in the dome is modeled as a closed expanding system composed of an ideal gas with constant specific heat. The vapor in the dome exists at a very low partial pressure; hence, its effect on the nitrogen state is neglected. However, energy transport to the vapor/gas dome as a result of vaporization/condensation is included.

3. Because of the high heat capacity and large mass of liquid below the interface, the liquid is modeled as an isothermal system.
4. The model for liquid flow includes inertia, wall friction, form loss, and gravity effects.

Convective heat transfer to the vapor/gas dome from the walls and the fluid surface is modeled by the cooling law:

$$Q_i = \bar{h}_i A_i (T_i - T_g) , \quad (4.3-5)$$

where i is the thermal transport surface, \bar{h}_i is the average convective heat transfer coefficient associated with that surface element, A_i is the surface area, and $(T_i - T_g)$ is the temperature difference between the surface and the vapor/gas mixture in the dome. For the heat transfer coefficient, two kinds of turbulent natural convection heat transfer models are used and combined by superposition: (1) heat transfer with the cylindrical walls of the tank using a turbulent natural convection correlation and (2) heat transfer from the disk-shaped ends of the cylinder, again using a turbulent natural convection correlation. For the spherical geometry, the equivalent definitions are used for model parameters.

When the accumulator is engaged, the vapor/gas dome temperature decreases due to expansion, while the liquid remains essentially isothermal. As a result, there is simultaneous vaporization at the liquid-vapor/gas interface and condensation in the dome. This mechanism transports a large amount of energy to the vapor/gas dome as a result of the heat of vaporization of the liquid. This process is approximated by a quasi-steady formulation. The rate of condensation is approximated by assuming that the vapor/gas dome remains at 100% humidity and by considering simple humidity relationships.

The accumulator component model uses a semi-implicit numerical scheme to render the solution independent of the time step employed by the main code. The differential equations are solved using the finite-difference algorithms.

4.3.5.8 ECC mixer

ECC mixer component is introduced into RELAP5-3D[®] to model the ECC injection in a PWR. This component is a specialized branch that requires three junctions. The physical extent of the ECC mixer component is the length of the cold leg pipe centered around the position of the ECC injection location, which should be about three times the inside diameter of the cold leg pipe. Junction number one is the ECC connection, junction number two is the cold leg cross section through which flow enters, and junction number three is the one that leads to the reactor vessel. A schematic cross sectional drawing of the component model is shown in Fig. 23.

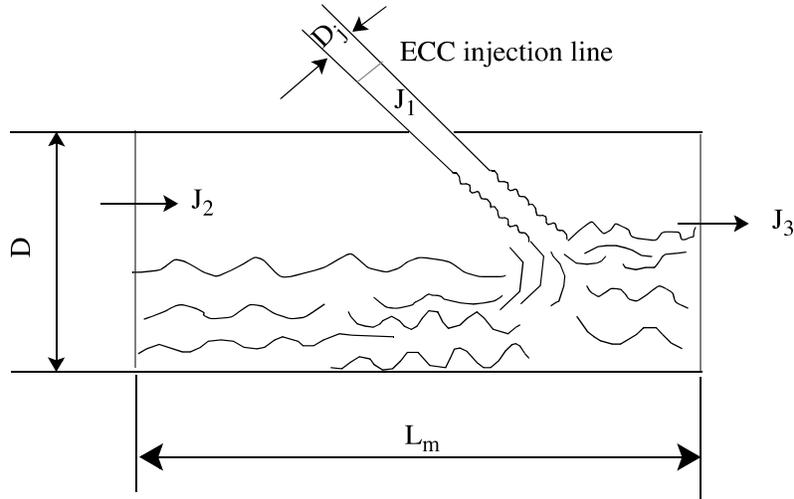


Fig. 23. Schematic of the ECC mixer component model.¹⁸

The computational model for the ECC mixer employs a particular flow regime map for condensation and uses a different correlation for interfacial heat transfer for each flow pattern to calculate the interfacial heat transfer coefficient, h_{if} . The interfacial heat transfer rate is calculated as follows:

$$Q_{ik} = h_{ik} A_i (T^s - T_k) , \quad (4.3-6)$$

where k is used to designate either the liquid or vapor/gas phase, Q_{ik} is the heat transfer rate, h_{ik} is the interfacial heat transfer coefficient, A_i is the interfacial area per unit volume, T^s is the saturation temperature, and T_k is the bulk temperature of phase k . Six basic modes of heat transfer are considered to represent the flow patterns:

1. wavy flow,
2. plug flow,
3. slug flow,
4. bubbly flow,
5. annular/annular-mist flow, and
6. dispersed droplet flow.

The effect of noncondensables on the rate of condensation is incorporated into the model by using a reduction factor, f , reported by an experimental study by DeVuono and Christensen.²⁸

Annulus

The annulus component in the annular-mist regime, the code assumes that all the liquid is in the film and that there are no drops for both the junction and volume flow regimes. This assumption was based on the work by Schneider, who showed that this was necessary in order to get downcomer penetration following a cold leg break.²⁹

4.3.5.9 Pressurizer

The pressurizer component models the dynamics of a pressurizer in PWR systems. A nodalization example for a pressurizer is shown in in Fig. 24.

This example models the pressurizer upper head with a branch node and the cylindrical shell and the lower head with a pipe discretized in seven cells. The shell and the lower and upper heads are modeled using heat structures. The spray valves are triggered by overpressurization of the primary coolant. The spray system is modeled with single volumes, as depicted in Fig. 24, by the nodes 335, 337, and 339 and the associated valves by the nodes 336 and 338.

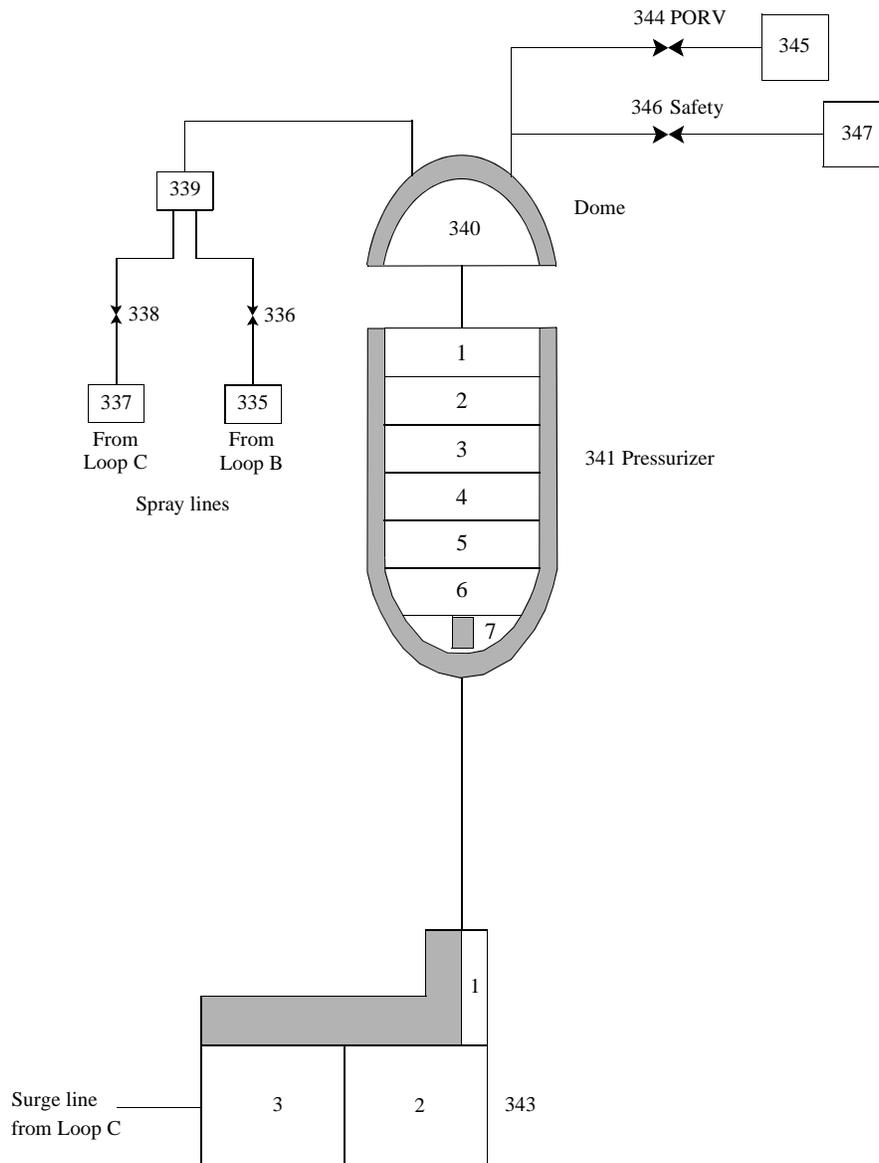


Fig. 24. A nodalization example of the pressurizer model.

4.3.5.10 Feedwater heater

The feedwater heater component is a variation of the branch component. The branch component was modified to include the shell and one or more tubes to represent the shell-and-tube heat exchanger. Feedwater heaters transfer heat from the shell to the tubes by condensing steam on the outside of the tubes. A cross sectional drawing of the component is shown in Fig. 25. RELAP5-3D requires that the feedwater heater components be defined as horizontal. It further requires that the number of junctions connected to the shell be two or three—one for vapor inlet, one for a condensate output, and one optional third junction for condensate inlet.

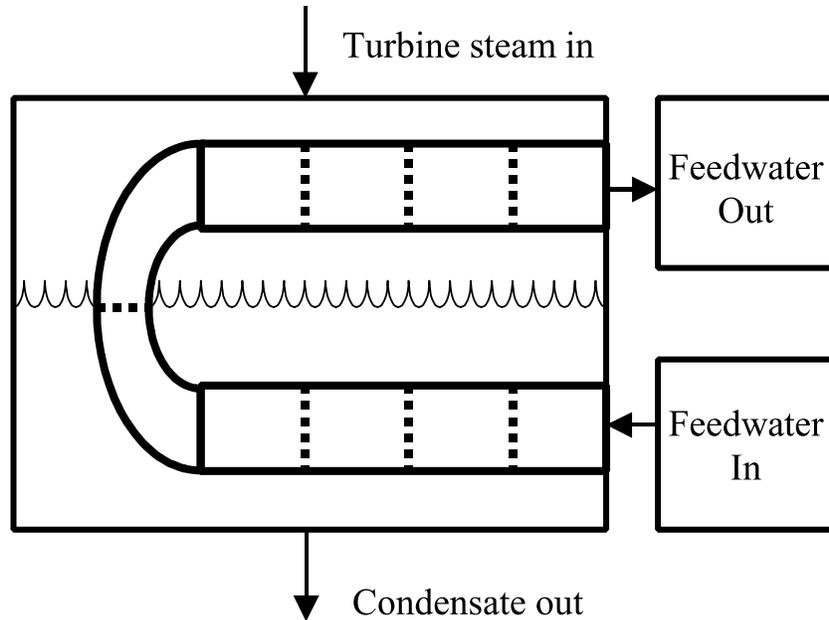


Fig. 25. Schematic of a feedwater heater component as modeled in RELAP5-3D³⁰.

When the flow regime in a feedwater heater component is horizontally stratified, heat transfer from the shell side to the tubes is computed using a condensation heat transfer correlation for the portion of the tubes exposed to steam and a convection correlation for the portion of the tubes exposed to liquid.

4.3.5.11 Compressor

In RELAP5-3D, the compressor model is similar to the pump model as it performs the same function on a gas as the pump performs on single-phase and two-phase fluids. The compressor model consists of an inlet junction, a control volume, and, optionally, an outlet junction, which can also be defined as an ordinary junction or another compressor component.

In a compressor, a change in angular momentum of the working fluid is caused by forces acting in the tangential direction only—radial and axial forces are constrained by the physical design. In principle, the isentropic torque can be calculated by considering an isentropic compression of the fluid and then applying an efficiency factor to get the total torque.

There are minor differences with the pump model. For instance, compressor head curve is specified differently for compressors than that of the pump homologous curves. Furthermore, the compressor torque is calculated based on the characteristic curves and the stage efficiency.

4.4 Numerical Solution Scheme

RELAP5-3D[®] transients evolve by advancing the semi-implicit numerical scheme that is based on replacing the system of differential equations with a system of finite difference equations partially implicit in time. The implicit terms are formulated to be linear in the dependent variables at new time, which results in a linear time-advancement matrix that is solved by direct inversion using a border-profile lower-upper (BPLU) solver. A sparse matrix solver is also available and can be selected by the user in the input deck.

Several stabilizing techniques are used to render the numerical algorithms stable. These include (1) the selective implicit evaluation of spatial gradient terms at the new time, (2) donor formulations for the mass and energy flux terms, and (3) use of a donor-like formulation for the momentum flux terms. The well-posedness and the accuracy of the final numerical scheme have been demonstrated for practical cell sizes by extensive numerical testing.

The difference equations are based on the concept of a control volume—also called a mesh cell—in which mass and energy are conserved by equating accumulation to the rate of mass and energy in through cell boundaries minus the rate of mass and energy out through the cell boundaries plus the source terms. This model results in defining mass and energy volume-average properties and requires knowledge of velocities at the volume boundaries.

The difference equations for each cell are obtained by integrating the mass and energy equations with respect to the spatial variable, x , from the junction at x_j to x_{j+1} . The momentum equations are integrated with respect to the spatial variable from cell center to adjoining cell center—i.e., x_K to x_L . These modeling variables in a representative geometry can be seen in Fig. 26. Integration of mass and energy equations from junction j to junction $j+1$ yields differential equations in terms of cell-average properties and cell boundary fluxes.

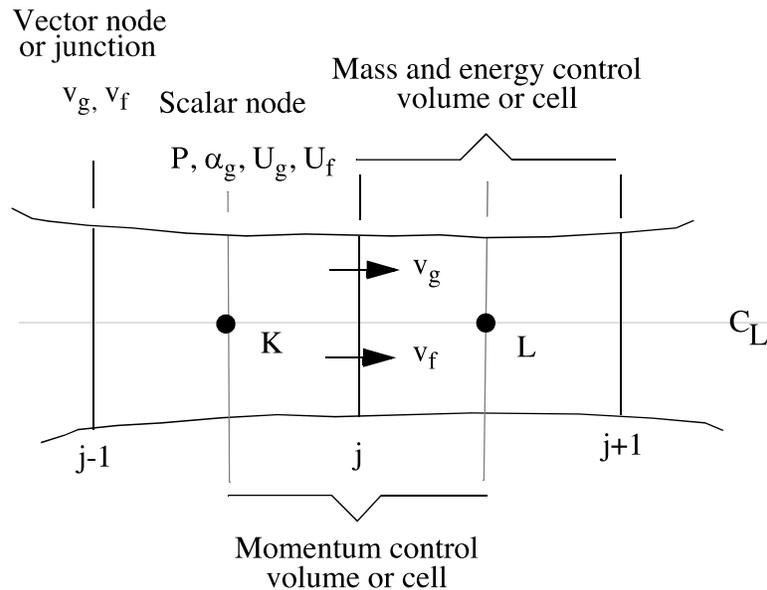


Fig. 26. Nodalization scheme for difference equations.¹⁸

The general guidelines followed in developing the numerical approximations are as follows:

- Mass and energy inventories are very important quantities in safety analysis; therefore, more emphasis is given to these quantities. A greater degree of approximation for momentum effects is considered acceptable, since nuclear reactor flows are dominated by large momentum sources and sinks (i.e., pump, abrupt area change, etc.).
- To achieve fast execution speed, implicit evaluation is used only for those terms responsible for the sonic wave propagation time step limit and those phenomena known to have small time constants. Thus, implicit evaluation is only used for the velocity in the mass and energy transport terms, the pressure gradient in the momentum equations, and the interface mass and momentum exchange terms.
- To further increase computing speed, time-level evaluations are selected so the resulting implicit terms are linear in the new time variables. Where it is necessary to retain nonlinearities, Taylor series expansions about old time values are used to obtain a formulation linear in the new time variables—higher-order terms are neglected.
- To allow easy degeneration to homogeneous, or single-phase, formulations, the momentum equations are used as a sum and a difference equation. The particular difference equation used is obtained by first dividing each of the phasic momentum equations by $\alpha_g \rho_g$ and $\alpha_f \rho_f$ for the vapor/gas and liquid phase equations, respectively, and then subtracting.

4.4.1 Numerical solution of radionuclide transport equations

RELAP5-3D[®] uses a Eulerian radionuclide tracking model that simulates the transport of radioactive or fertile nuclides in the reactor coolant systems. The model can be used in connection with the nuclear detector model to describe the response of the control and safety systems to the presence of radioactive species in the coolant. The concentration of radionuclide species are assumed to be sufficiently dilute that the following assumptions are valid:

1. the fluid properties are not altered by the presence of radionuclide species;
2. energy absorbed by the coolant from the decay of radionuclide species is negligible; and
3. the radionuclide species are well-mixed with the transporting phase, such that they are transported at the coolant velocity.

Based on these assumptions, the equation for the conservation of mass for radionuclide species is solved, i.e.,

$$\frac{\partial C}{\partial t} + \frac{1}{A} \frac{\partial}{\partial x} (CvA) = S \quad (4.4-1)$$

where C is the number density of the radionuclide species in atoms per unit volume, v is the average coolant velocity, A is the cross sectional area of the flow channel, and S is the source of the radionuclide species in units of atoms per unit volume per second.

4.5 Control System Simulation

RELAP5 allows implementing an integrated control system into the simulation. The control system input provides the capability to evaluate simultaneous algebraic and ordinary differential equations. The control system consists of several types of control components. This control system simulation model provides a way for simulating any lumped process, such as controls or instrumentation, in which the process can be

defined in terms of system variables through logical, algebraic, differentiating, or integrating operations on variables from the fluid, heat structure, and neutronic components. The control system simulation returns calculated values as inputs to those components. These models do not have a spatial variable and are integrated with respect to time. The control system is coupled to the thermal and hydrodynamic components serially and implicitly. This capability can be used to construct models of system controls or to model other components—not incorporated in the RELAP modeling system—that can be described in terms of algebraic and differential equations. The code numerical solution includes the evaluation and numerical time advancement of the control system coupled to the fluid and thermal system.

The control system advancement occurs after the heat conduction transfer, hydrodynamic, and reactor kinetics advancements and uses the same time step as the hydrodynamics so that new time thermal and hydrodynamic information is used in the control model advancement. However, the control variables are fed back to the thermal and hydrodynamic model in the succeeding time step.

Each control system component defines a control variable as a specific function of time-advanced quantities. The time-advanced quantities include hydrodynamic volume, junction, pump, valve, heat structure, reactor kinetics, trip quantities, and the control variables

Control components included in RELAP5 are as follows:

1. arithmetic (+, −, *, /),
2. integration,
3. differentiation,
4. proportional-integral,
5. lag,
6. lead-lag,
7. shaft component, and
8. inverse kinetics component.

Following sections will briefly discuss the functions performed by these control components.

4.5.1 Arithmetic control components

The control components introduced under this section share the following variable definitions:

- y_i : control variable defined by the i th control component,
- A_j , R , and S : real constants input by the user,
- I : integer constant input by the user,
- v_j : quantity advanced in time by RELAP5-3D—can include y_i ,
- t : time, and
- s : Laplace transform variable.

Superscripts involving the n denote time steps.

4.5.1.1 Constant

$$y_i = S \quad [\text{CONSTANT}] . \quad (4.5-1)$$

4.5.1.2 Addition and subtraction

$$y_i = S(A_0 + A_1 v_1 + A_2 v_2 + \dots) \quad [\text{SUM}] . \quad (4.5-2)$$

4.5.1.3 Multiplication

$$y_i = S v_1 v_2 \quad [\text{MULT}] . \quad (4.5-3)$$

4.5.1.4 Division

$$y_i = S \frac{1}{v_1}, \quad \text{or} \quad y_i = S \frac{v_2}{v_1} \quad [\text{DIV}] . \quad (4.5-4)$$

4.5.1.5 Exponentiation

$$y_i = S v_1^I \quad [\text{POWERI}] , \quad (4.5-5)$$

$$y_i = S v_1^R \quad [\text{POWERR}] , \quad (4.5-6)$$

$$y_i = S v_1^{v_2} \quad [\text{POWERX}] . \quad (4.5-7)$$

4.5.1.6 Table lookup function

$$y_i = S F(v_1) \quad [\text{FUNCTION}] , \quad (4.5-8)$$

where F is a function defined by table lookup and interpolation.

4.5.1.7 Standard functions

$$y = S F(v_1, v_2, \dots) \quad [\text{STDFNCTN}] , \quad (4.5-9)$$

where F can be chosen from a number of supported operations.

4.5.1.8 Delay

$$y_i = S v_1(t - t_d) \quad [\text{DELAY}] , \quad (4.5-10)$$

where t_d is the delay time. A user input parameter, h , determines the number of pairs of data used to store past values of v_1 . The maximum number of time-function pairs is $h + 2$, and the delay table time increment is t_d/h . The delayed function is obtained by linear interpolation using the stored past history. As time is advanced, new time values are added to the table. Once the table fills, new values replace values that are older than the delay time.

4.5.1.9 Unit trip

$$y_i = S U(\pm t_r) \quad [\text{TRIPUNIT}] . \quad (4.5-11)$$

4.5.1.10 Trip delay

$$y_i = S T_r(t_r) \quad [\text{TRIPDLAY}] , \quad (4.5-12)$$

where t_r is the trip number.

Control system components are treated as the last item in processing the operations in a given time sequence. Therefore, at the end of a time step $(n + 1)$, values for trip variables t_r and all v_1 variables—

except control variables y_i —are available. The control components are evaluated in component number order.

4.5.1.11 Integration control component

This component evaluates the following mathematical expression:

$$y_i = S \int_{t_1}^t v_1 dt \quad [\text{INTEGRAL}] , \quad (4.5-13)$$

where t_1 is the simulation time when the component is added to the system. The computation of integral is carried out by trapezoidal approximation:

$$y_i^{n+1} = y_i^n + S \left[v_i^n + v_i^{n+1} \right] \frac{\Delta t}{2} , \quad (4.5-14)$$

where Δt is the integration time step.

4.5.2 Differentiation control components

Time differentiation of a variable is defined as

$$y_i = \frac{dv_1}{dt} \quad (4.5-15)$$

The differentiation operation can be performed by two operands. The first operand, DIFFERNI, evaluates the derivative by the inverse of the integration technique, i.e.,

$$y_i^{n+1} = S \frac{2}{\Delta t} (v_1^{n+1} - v_1^n) - y_i^n \quad [\text{DIFFERNI}] \quad (4.5-16)$$

This component operation is known to become unstable under certain circumstances.

An alternative derivation component, DIFFERND, is defined as follows:

$$y_i^{n+1} = \frac{S}{\Delta t} (v_1^{n+1} - v_1^n) \quad [\text{DIFFERND}] \quad (4.5-17)$$

Unless necessary, differentiation of control variables should not be considered since the derivative operation is inherently unstable. The differentiation output can be fed to a filter for proper signal treatment.

4.5.3 Proportional-integral control component

This component evaluates the following mathematical expression:

$$y_i = S \left[A_1 v_1 + A_2 \int_{t_1}^t v_1 dt \right] \quad [\text{PROP} - \text{INT}] \quad (4.5-18)$$

4.5.4 Lag control component

The lag component is defined in Laplace transform notation as

$$Y_i(s) = S \left(\frac{1}{1 + A_1 s} \right) V_1(s) \quad [\text{LAG}] . \quad (4.5-19)$$

4.5.5 Lead-lag control component

The lead-lag component is defined in the Laplace transform notations as

$$Y_i(s) = S \left(\frac{1 + A_1 s}{1 + A_2 s} \right) V_1(s) \quad [\text{LEAD} - \text{LAG}] . \quad (4.5-20)$$

4.5.6 Shaft component

The shaft component is a special control component that advances the rotational velocity. The shaft component is mathematically represented as follows:

$$\sum_i I_i \frac{d\omega}{dt} = \sum_i \tau_i - \sum_i f_i \omega + \tau_c \quad [\text{SHAFT}] ,$$

where I_i is the moment of inertia from component i , τ_i is the torque from component i , f_i is the friction from component i , and τ_c is an optional torque from a control component. The summations are over the pump, compressor, motor, or turbine components that are connected to the shaft and the shaft itself. The shaft and each associated component contain its own models, data, and storage for inertia, friction, and torque has storage for its rotational velocity. Each component can be assigned a disconnect trip number; the component is connected when false and disconnected when true. Any disconnected component is advanced separately and, thus, can have a different rotational velocity than the shaft. All connected components have the same rotational velocity.

4.5.7 Inverse kinetics component

The inverse kinetic component solves the point reactor kinetics equations for the reactivity. The mathematical expression of the operations is as follows:

$$y = S \left[\frac{\frac{\Lambda}{\beta} \left(\frac{dv_1}{dt} \right) + \sum_{i=1}^{N_d} D_i(t_0 + \Delta t)}{v_1} \right] \quad (4.5-21)$$

where D_i is defined as

$$D_i(t_0 + \Delta t) = e^{-\lambda_i \Delta t} D_i(t_0) + \frac{\beta_i}{\beta \lambda_i} (1 - e^{-\lambda_i \Delta t}) \frac{dV_1}{dt} \quad (4.5-22)$$

The input to the inverse kinetics control block should be the total fission power computed by the point kinetics model, the total fission power computed by the nodal neutron kinetics model, the fission power in one of the nodal neutron kinetics zones, or the response of a neutron detector that senses the neutron flux computed by either of the two neutron kinetics models.

4.5.8 Trips and Control Variables

The trip capability available in the RELAP5-3D[®] code enables the user to specify actions during a simulated system transient. When coupled with the code's control variables, the user has a versatile tool that greatly expands the capabilities of the RELAP5-3D[®] code. The trip logic can be used with the time-dependent volume component, the pump component, the valve components, the time-dependent junction component, some options of the branch component, the accumulator component, and with tables used to describe reactor kinetics characteristics and heat structure characteristics. In general, the trip's condition is either true or false. The trip's condition is determined at each time step by checking the status of the trip-defined test. The test consists of comparing the specified variable to either another variable or a parameter using specified conditions such as equal to, greater than, less than, greater than or equal, less than or equal, or not equal. In combination with the "logical trips," very complex logical sequences can be simulated since the "logical trips" allow comparison between two or more trips such that one or more trips may be required to be true to create a true "logical trip" condition.

RELAP5-3D[®] consists of 21 control capabilities as summarized in Table 1. The control variables can be used for three primary functions: (a) to simulate equipment control systems, (b) to create "lumped node" parameters, and (c) to add further dimensions to the boundary conditions imposed on the thermal-hydraulic and heat structure group components.

4.5.9 Simulating equipment control systems

Every piece of equipment that is a component of a physical system has a control system. The control system may be no more sophisticated than a simple on/off switch that is controlled by the equipment operator. Sometimes, however, equipment control systems can be highly complex and sophisticated. Consequently, the code has control variable components designed to allow the user to model virtually any

physical component of the equipment system. Specifically, the lag, lead-lag, proportional-integral, and differential components are designed to simulate common controller functions. When used in combination with the other control variable components, even the complex and sophisticated Babcock & Wilcox's (B&W) PWR Integrated Control System has been successfully modeled using RELAP5-3D®.

Table 1. Summary of RELAP5-3D control variables

Component	RELAP5-3D® Primitive	Function
Sum/Difference	SUM	Allows addition or subtraction of variables
Multiplier	MULT	Allows multiplication of two variables
Divide	DIV	Allows division of two variables
Differentiating	DIFFRENI and DIFFREND	Performs differentiation of a variable as a function of time
Integrating	INTEGRAL	Performs integration of a variable as a function of time
Functional	FUNCTION	Defines a look-up functional relationship to a variable
Standard function	STDFNCTN	Performs absolute value, square root, exponential, natural algorithm, sine, cosine, tangent, arc-tangent, minimum value, or maximum operation on a variable
Delay	DELAY	Acts as a time-delay factor operating on a variable
Unit trip	TRIPUNIT	Becomes true at a defined time; can also be defined as a complementary function
Trip delay	TRIPDLAY	Becomes true at a defined time
Integer power	POWERI	Gives variable raised to integer constant power I quantity times constant
Real power	POWERR	Gives variable raised to real constant power R quantity times constant
Variable power	POWERX	Gives variable raised to real variable power V quantity times constant
Proportional-Integral	PROP-INT	Defines a proportional-integral controller
Lag	LAG	Defines a lag controller function
Lead lag	LEAD-LAG	Defines a lead-lag controller function
Constant	CONSTANT	Defines a constant value to be used with other control variables
Shaft	SHAFT	Defines shaft characteristics that may be used in conjunction with a generator
Pump control	PUMPCTL	Defines a pump controller (used principally for steady state analysis)
Steam control	STEAMCTL	Defines a steam flow controller (used principally for steady state analysis)
Feed control	FEEDCTL	Defines a feedwater flow controller (used principally for steady state analysis)
Inverse kinetics	INVKIN	Defines inverse kinetics (used to solve point reactor kinetics for reactivity rather than for neutron density)

4.5.10 Simulating “lumped node” systems

Equipment components such as containments, tanks, flow systems, and balance-of-plant components can be simulated using the control variables by creating difference equation sets that represent the specific component’s behavior. The equation sets can then be coupled to the RELAP5-3D[®] model of primary interest using tables and simple functional relationships to simulate the interactions between the primary thermal-hydraulic and the “lumped node” models.

4.5.11 Enhancing the RELAP5-3D[®] model boundary conditions

The control variables can be used to simulate the presence of instrumentation that provides key input to system trip or equipment functions. For example, a piece of instrumentation affected by the total pressure rather than the static pressure can be modeled by creating a control variable that monitors the fluid static pressure and the fluid velocity head to calculate the total pressure head (in the absence of a gravitational change), and then provides a value to be compared to a trip test value. Similarly, the critical flow energy flux can be calculated using the control variables to determine the flow enthalpy at each time step (since RELAP5-3D[®] only calculates the flow specific internal energy, not the specific enthalpy).

4.6 Applications of RELAP5-3D/ATHENA for Modeling of the HTGR

In this section, we identified two applications of RELAP5-3D for integrated systems modeling that includes a nuclear reactor and heat transport systems that use high-temperature high-pressure gas.

4.6.1 High- and low-pressure conduction cool-down accident analyses of the prismatic NGNP HTGR

Systems models of the prismatic block version of the NGNP VHTR were developed using RELAP5-3D/ATHENA.³¹ The interactions of various heat transfer modes are illustrated in Fig. 27(a). The transient scenarios were reported to be based on the values calculated by General Atomics for an equilibrium cycle GT-MHR core.³¹ The systems model for the NGNP VHTR also included the RCCS. The heat transfer paths for the radiation mode in the RCCS are shown in Fig. 27(b).

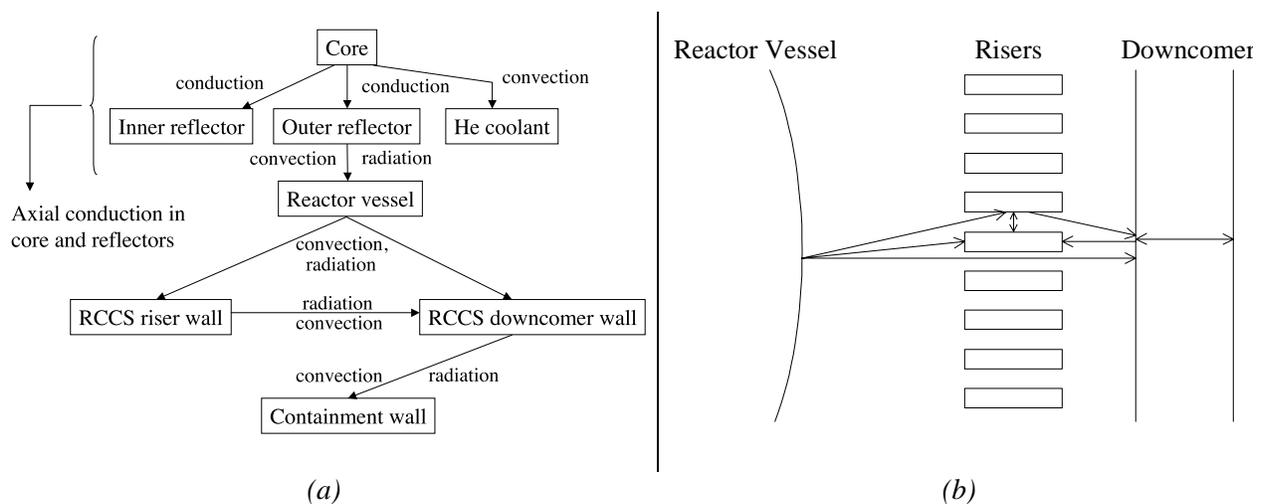


Fig. 27. (a) Heat transfer interactions in the RELAP5-3D/ATHENA model for the NGNP VHTR; (b) radiation paths as modeled in RELAP5-3D between the pressure vessel and the RCCS.^{24, 31}

The VHTR pressure vessel model included both active and stagnant coolant volumes. The model included a detailed representation of the structures within the core, including the inner and outer reflectors, upper and lower reflectors, the core barrel, the upper plenum shield, and the reactor vessel wall and the upper head, as illustrated in Fig. 28(a). The vessel model accepted coolant inlet temperature, coolant outlet pressure as the boundary conditions. The inlet flow rate was adjusted for the steady-state calculations to obtain the desired outlet temperature.

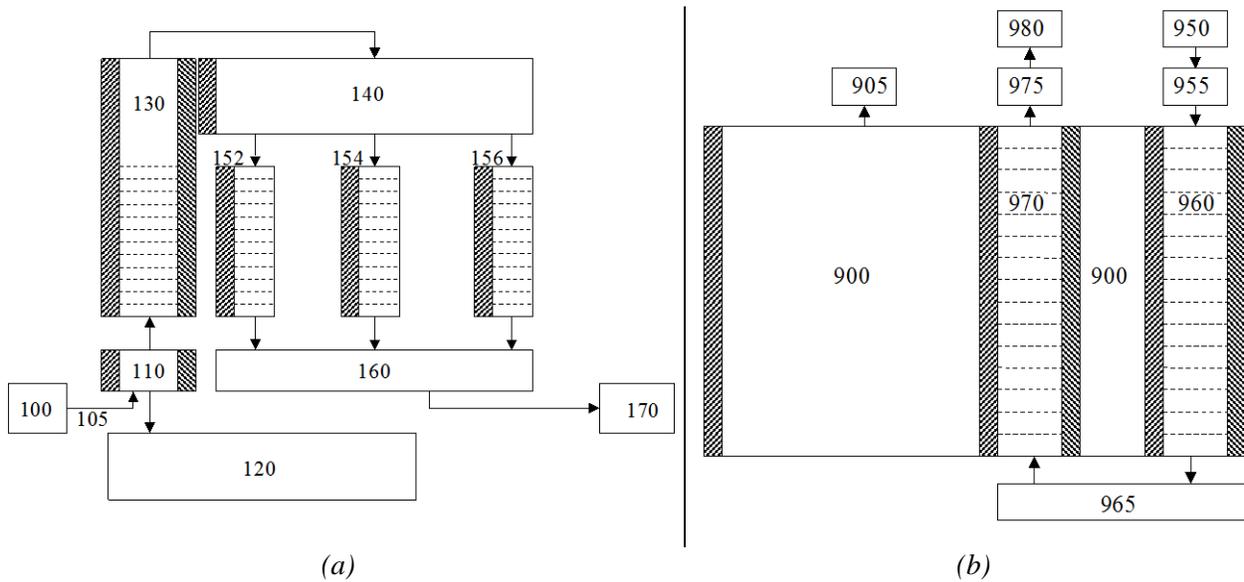


Fig. 28. (a) Hydraulic nodalization of the VHTR pressure vessel; (b) nodalization of the reactor cavity.²⁴

To model the dynamics during an accident condition, a model of the reactor cavity was also incorporated, as shown in Fig. 28(b). The cavity model included a containment air volume, the containment concrete wall and the surrounding soil, and the RCCS. In the RCCS model, air enters the inlet plenum above the downcomer flows to the bottom of the reactor compartment where it is distributed to the riser channels. The hot air leaving the risers is collected in a plenum and then discharged back to the atmosphere. Emissivity values of 0.8 were used for the core barrel, reactor vessel, and RCCS structures. An emissivity of 0.1 was used for the RCCS downcomer wall facing the reactor vessel because it has a reflecting surface with approximately 7.5-cm insulation behind the surface.

The RELAP results were benchmarked against previous high- and low-pressure conduction cool-down transient calculations performed at General Atomics for the GT-MHR. For matching decay heat curves, the peak fuel temperatures calculated by RELAP were reported to be slightly below the values reported by General Atomics, which was attributed to a better estimate of convective heat transfer in the bypass regions calculated by RELAP.³¹

4.6.1.1 Flexible-conversion ratio fast reactor systems evaluation

The flexible-conversion-ratio (FCR) fast reactor project was intended to assess the performance characteristics of conceptual designs of certain fast reactor systems that use either lead or liquid salts as coolants. The comprehensive evaluation can be found in Todreas³². An integrated model of the reactor system was developed in RELAP5-3D/ATHENA that included the primary system, the secondary system, and the power conversion system. A systems layout of the RELAP5-3D model along with the associated subsystem and component nodalization is shown in Fig. 29.

The RELAP5-3D model was built in five stages:

1. An overall model of the primary system was developed with the core represented as two channels: hot channel representing a group of hot fuel assemblies and average channel modeling the rest of the core.
2. A detailed IHX model was created separately, optimized, and then connected to the primary loop within the reactor vessel.
3. The reactor vessel auxiliary cooling system (RVACS) with guard vessel, the lead-bismuth gap between the reactor and the guard vessel, dimples on the outer guard vessel wall and perforated plate for heat transfer enhancement were added, and analysis of the RVACS decay heat removal capability was conducted.
4. A complete PCS with the turbine, compressors, recuperators, and the precooler was connected to the primary system through the IHX to simulate overall system response to accident conditions.
5. A preliminary design of a passive secondary auxiliary safety system (PSACS) to aid RVACS decay heat removal was conducted. The passive system was built in RELAP5-3D and connected to the PCS.

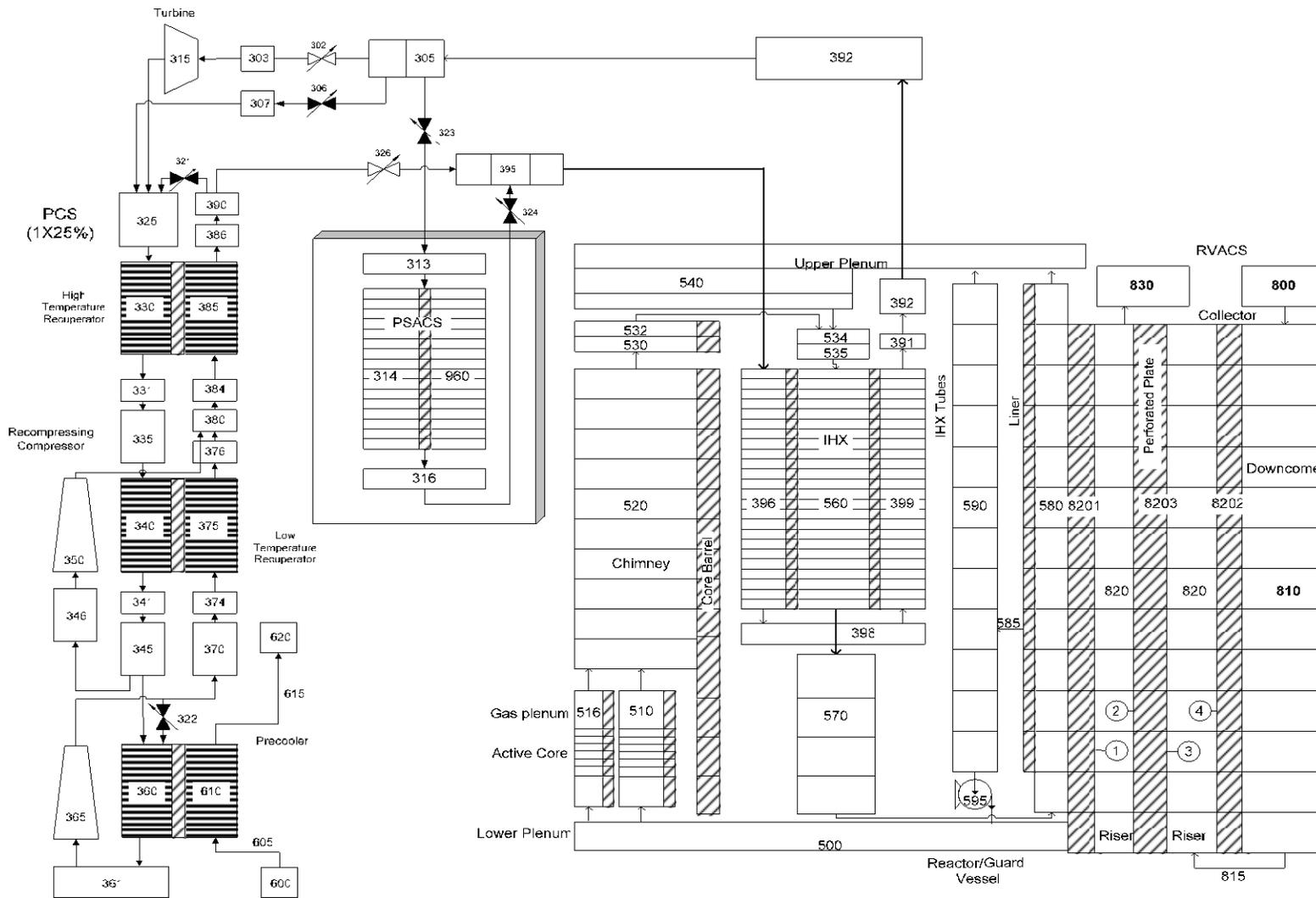


Fig. 29. Integrated layout of the primary and secondary heat transport systems and RVACS.³²

DRAFT

For the purposes of HTGR applications, the relevance of this document lies with the RELAP5-3D model of the PCS. The PCS is recompression S-CO₂ cycle developed at Massachusetts Institute of Technology (MIT) under a NERI and Generation-IV program funding through Sandia National Laboratory (SNL). One of the challenges in implementing the S-CO₂ power cycle scheme is to overcome excessive pressure drops in the interconnecting pipes and distribution plena. One solution proposed by the MIT study is to employ parallel modules and pipes and by using two 300-MW(t) trains in parallel as rendered in Fig. 30. Each loop of the S-CO₂ PCS is capable of generating 265-MW(e) [600-MW(t)] power corresponding to one intermediate heat exchanger. The nominal thermodynamic cycle with the associated state parameters is shown in Fig. 31.

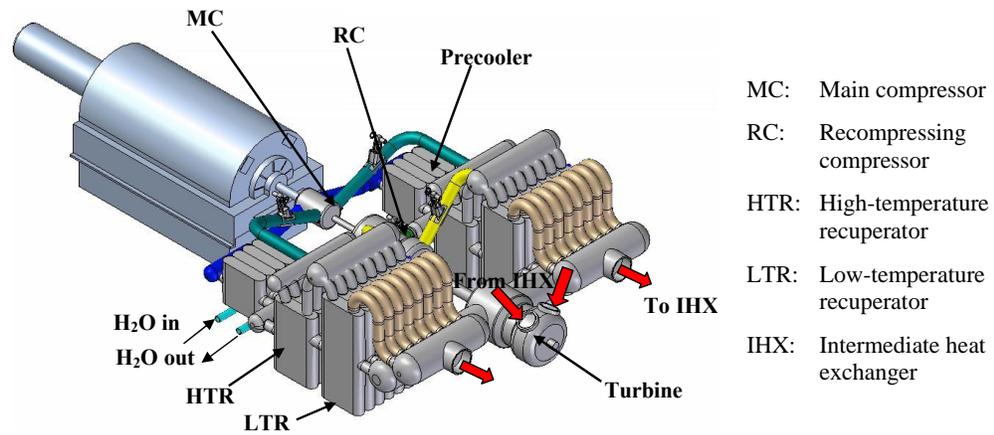


Fig. 30. Isometric view of the 600-MW(t) power conversion system layout. [Adapted from Todreas³²]

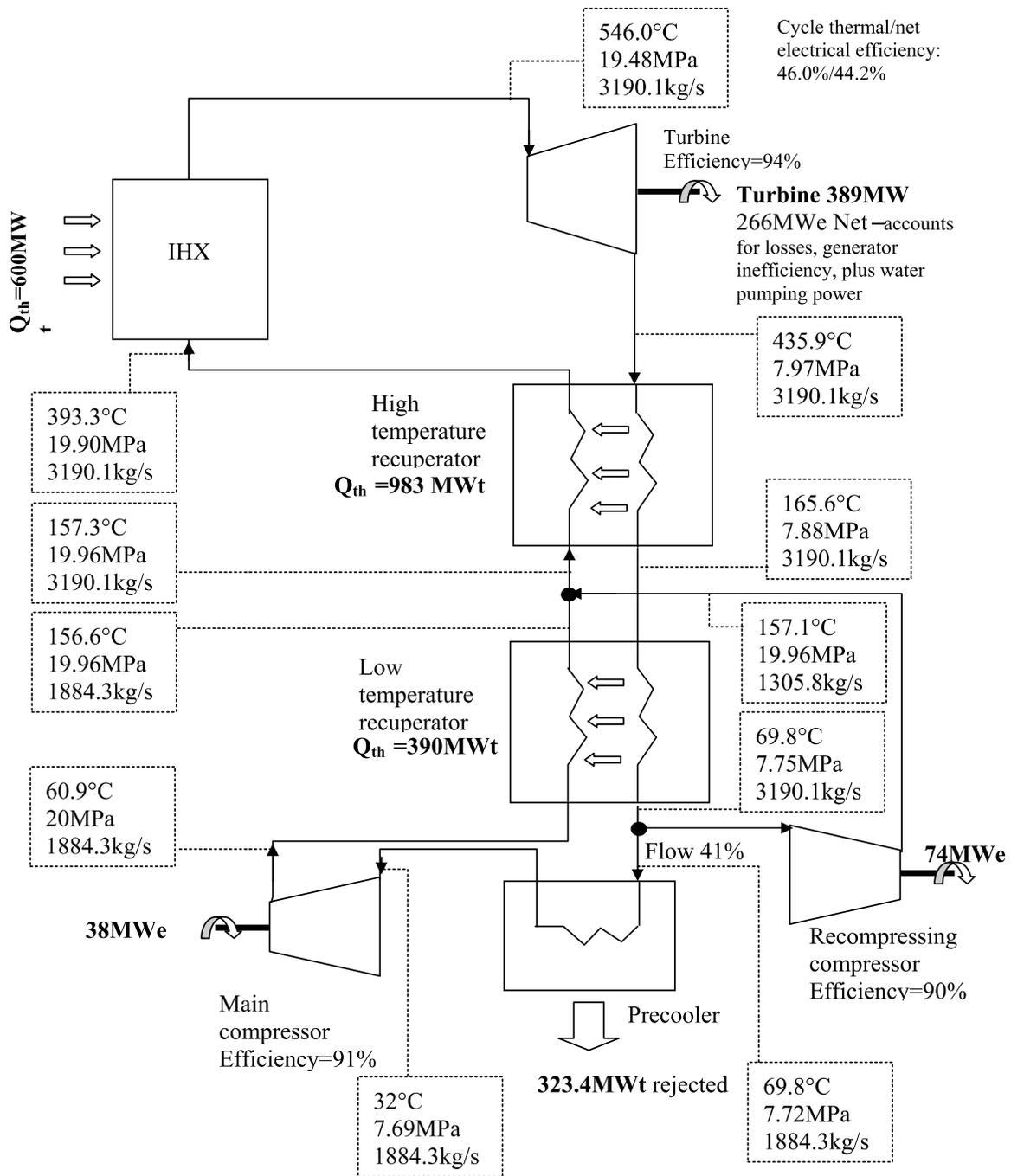


Fig. 31. Thermodynamic state points of the S-CO₂ cycle for the 600-MW(t) power conversion system design.³²

The RELAP5-3D model nodalization diagram of the S-CO₂ power conversion system is depicted in Fig. 32. Volumes 300 and 398—as shown in Fig. 32—are the pressure and temperature boundary conditions of the cycle. The main components of the cycle include turbine, compressors, high- and low-temperature recuperators, pre-cooler, and shaft and generator. The turbine represented by volume 315 is modeled with shaft speed of 3600 rpm and efficiency of 94%. The turbine is connected to the hot side of the high-temperature recuperator shown as volume 330. The flow is then directed into the hot side of the low-

temperature recuperator, represented by volume 340. Both high- and low-temperature recuperators were modeled as heat exchangers with vertical semicircular channels with a diameter of 2 mm. In volume 345, the flow is split into two streams: 40% of the original flow is directed into the recompressing compressor, represented by volume 350. The remaining 60% of the stream is cooled in the precooler—volume 360—to 32°C, after which it is pumped through main compressor, represented by volume 365. The precooler is a heat exchanger in which the gas is the primary fluid on the tube side, and water is on the secondary shell side. The water flow is simulated by time-dependent volumes 600 and 620. The mass flow rate of water through the precooler is kept constant at 4625 kg/s, and the inlet temperature is assumed to be 20°C. Both compressors are modeled as homologous pumps.

Once disconnected from the grid, the turbine provides energy to drive compressors mounted on the same shaft and circulate CO₂ flow through the IHXs making it possible to remove significant power from the reactor vessel without electrical power supply. A proportional-integral (PI) controller is used—as shown in Fig. 32—to regulate the valve position to maintain an acceptable turbine speed.

The PCS was optimized for the IHX outlet CO₂ temperature of 546°C—which is the turbine inlet temperature—and the total volume of recuperators and precooler of 120 m³. The cycle operates between pressures of 7.7 MPa and 20 MPa. The cycle low temperature was determined to be 32°C, which is just above the critical point of CO₂. The cycle achieves a net electrical efficiency of 44%, which also accounts for all losses including water pumping power and switchyard losses.

All cycle heat exchangers were selected as HEATRIC™ printed circuit heat exchangers (PCHEs)—except for the IHX. All the heat exchangers were assumed to have straight channels with semicircular cross section. More information on HEATRIC™ PCHE can be found in the literature³³⁻³⁵ and on the company web site.³⁶

4.6.1.2 Comments on the RELAP5-3D model of the flexible-conversion-ratio fast reactor system

The primary objective of implementing a RELAP5-3D model of the FCR fast reactor is to demonstrate that, for a number of systems identified in the study, the clad integrity is never compromised during an unprotected station blackout incident. A station blackout represents the loss of off-site power. An unprotected station blackout is usually considered to be the most challenging hypothetical accident, where in addition to the loss of off-site power, the reactor fails to scram. The study proposes certain design features for lead-alloy-cooled and liquid-salt-cooled fast reactors to assure that the safety objectives are met.

The reason the FCR fast reactor study was discussed here is because it included an integrated RELAP5-3D model of the plant (i.e., the primary heat transport loop, the secondary heat transport loop, and the PCS). Within the model, these tightly coupled systems were allowed to interact dynamically with each other. This is an important feature for control and protection systems design and analysis purposes.

However, the study—being primarily a safety-demonstration tool—does not address the critical elements of control system simulation practices. Safety demonstrations usually fall into the domain of protection systems. Protection systems—from the standpoint of system complexity—are fairly primitive systems that are designed to perform certain limited functions, usually to completion, which means that once a protection system is triggered or activated, the entire sequence of protective functions is required to complete to reset the system. The triggering mechanism is typically multiply redundant safety-grade independent instrumentation.

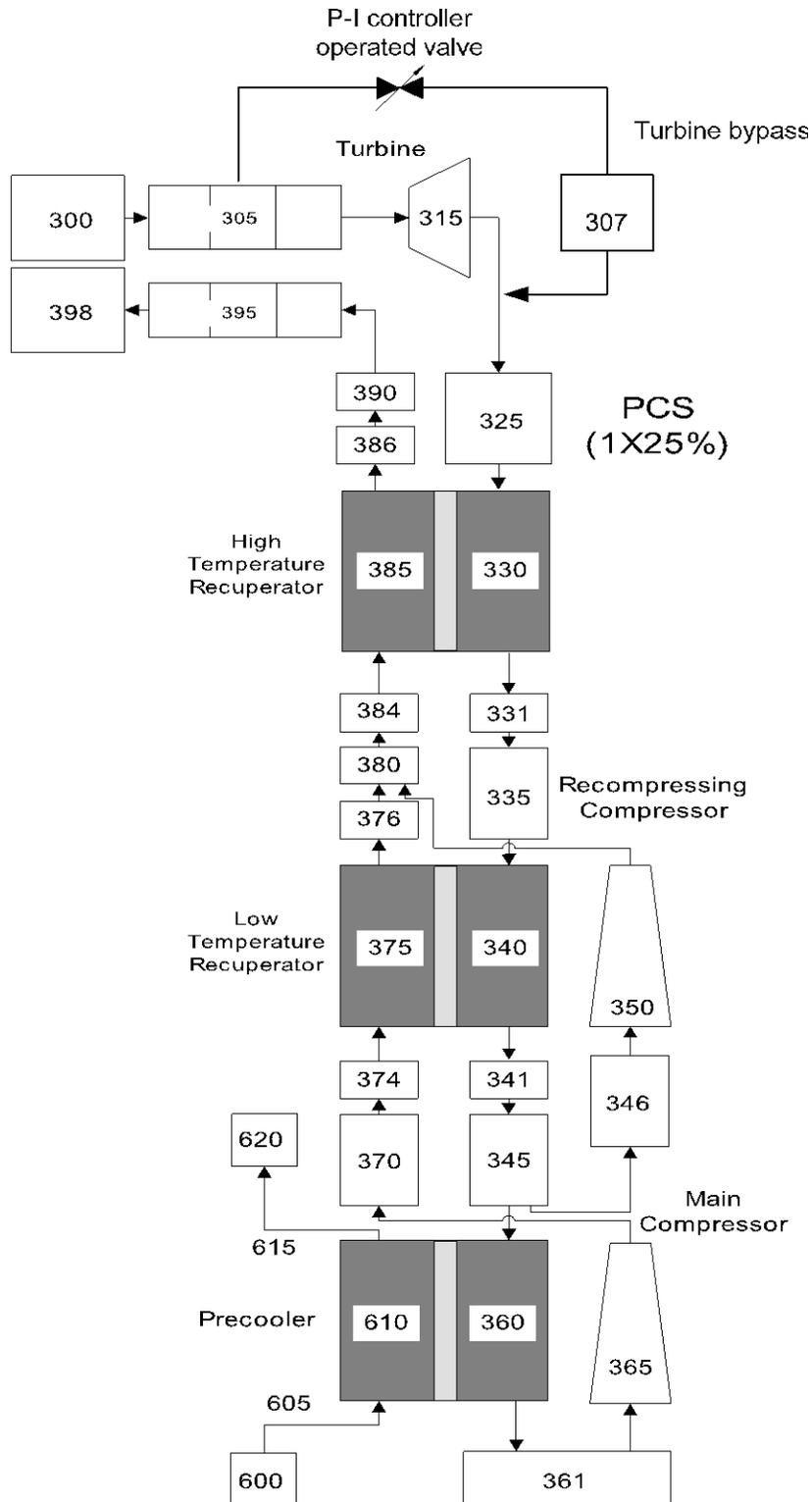


Fig. 32. RELAP5 nodalization structure of the PCS.

Control system functions are generally more sophisticated algorithms than the protection system functions, but the domain of operation is more restricted (i.e., normal operating conditions and certain transients that do not cause significant deviations from nominal conditions). A comprehensive control system simulation should not only include the dynamics of the system it is intended to control, but also the physics and dynamics of the sensors and actuators that are involved in the measurement of processes, and control of components or systems. Key parameters for control are typically those that deal with the response time of individual elements and components. A realistic simulation with representative time constants is expected to demonstrate whether the overarching control objectives can be met with a set of specifications. These parameters usually have physical implications that impose certain design characteristics for sensors and actuators. Typically, control performance objectives delineate a domain of acceptable parameters for these control elements. It is required that the control elements (i.e., either the sensor or the actuator) maintain their specifications within this acceptable domain over its entire life cycle as well as the entire range of operating conditions of the plant.

4.7 Necessary Features for Integrated Systems Simulation of the Reactor and Balance of the Plant for Control Systems Analysis Purposes

RELAP5 contains the minimum set of building blocks to perform a wide range of control and protection system simulations. The primitives listed in Table 1 provide a useful set of commands to interact with the main module of the code that executes the system transients.

The lag and lead-lag controllers and proportional-integral controller are plug-and-play components that can be rapidly used for implementing control strategies. However, more sophisticated control algorithms usually have more demanding computational requirements that would not be efficiently defined using these built-in control primitives. Optimal control, robust control, adaptive control, and model predictive control are just a few among these approaches. These control methods are usually avoided for controlling the primary system functions because the simpler controls are sufficient but can be implemented for the PCS, such as the turbine control. RELAP5 currently does not support the higher level control algorithms.

One of the shortcomings of the RELAP5 code system—from the control systems simulations perspective—is that it does not allow incorporation of user-created external subroutines that can perform other computations and communicate the results with the main application in a predetermined protocol. This would significantly extend the capabilities of the code system and allow design and analysis simulations of a much larger set of control systems.

Advanced reactor and plant system designs, including the HTGR, usually employ digital instrumentation and control systems. Almost all the safety-related and nonsafety-related functions are performed by digital systems—sometimes with an analog backup system as a redundant means. The level of sophistication in digital system implementations is expected to increase as the regulatory bodies have better understanding of the failure modes and mechanism of these systems. Incorporation of the sophistication of these systems and their potential failures will be a major challenge for engineers. In particular, it is expected that the plants would employ full automation of startup and shutdown transitions. The startup and shutdown modes are special control modes which the control system detects the need to switch into or out of. The complexity of these operations in conjunction ability to switch into and out of manual control smoothly makes the automation multistate event-based process. The automation may prove to be the most challenging part of the control algorithm.

The possibility for unintended and unexpected adverse system interactions increases with the degree of automation. The role of the control designer expands to operations engineer with a requirement the control design anticipate all potential normal and abnormal scenarios that may occur in operation.

RELAP5 is mostly a time domain tool, in that it allows continuous-time or discrete-time system definitions. It does allow creation and definition of trip variables that assume Boolean values. However, this capability is not sufficient to define the dynamics of an event-based system.

One way of modeling digital systems for modeling purposes is by creating a finite-state machine representation. A finite-state machine—also called finite-state automata—is defined as a device that is capable of representing a language according to well-defined rules.³⁷ A language constitutes a formal way, among many others, of representing the logical behavior of discrete-event systems.

Combining the environments for continuous- or discrete-time systems and discrete-event systems create a hybrid simulation environment. A hybrid simulation environment can have asynchronous events and process variable changes over the course of the simulation time, which would allow simulating the dynamic interactions of a continuous-time system, such as a reactor and thermal fluid system, and an event-driven system, such as a digital control system. This would allow incorporation of failure modes that are unique to digital instrumentation and control systems into the control and protection system simulations.

Another challenge in modeling these complicated systems is the communication network. In the earlier nuclear plant designs where analog control systems were used, data transfer was accomplished through point-to-point wired connections which carry a single signal. However, digital instrumentation and control systems employ highly sophisticated fiber optic communication networks to transmit control and protection system inputs and outputs in an efficiently and timely manner. The fiber optic networks carry many signals on the same network. Issues of timing and handling of missed or corrupted communications is an area of control and safety review. RELAP does not offer any tools to represent the timing and delay effects of digital communications either by fiber network or represent communication failures. If external subroutine definitions are allowed, these capabilities can be implemented and incorporated into the RELAP5 code system by control engineers.

4.8 MELCOR

MELCOR is a fully integrated, engineering-level computer code whose primary purpose is to model the progression of accidents in LWR nuclear power plants. MELCOR was developed by Sandia National Laboratory for the U.S. Nuclear Regulatory Commission (NRC) as a second-generation plant risk assessment tool and the successor to the Source Term Code package. It is specifically designed to represent accidents which proceed to core degradation and relocation of structural components. Originally, MELCOR was capable only of modeling LWRs, but recent additions of material properties allow it to simulate gas, liquid metals, and liquid salts as coolants. Additional modifications have added secondary plant components to represent hydrogen production systems and gas turbines and compressors so that a full NGNP plant can be modeled.

A broad range of severe accident phenomena in both BWRs and PWRs are treated in MELCOR in a unified framework. Current uses of MELCOR include estimation of fission product source terms and their sensitivities and uncertainties in a variety of applications. MELCOR is also used to analyze design basis accidents for advanced reactor designs, such as ESBWR, EPR and APWR.

The MELCOR code is composed of an executive driver and a number of major modules, or packages, that together model the major systems of a reactor plant and their interactions. Reactor plant systems and their response to off-normal or accident conditions include:

- thermal-hydraulic response of the primary reactor coolant system, the reactor cavity, the containment, and the confinement buildings;
- core uncovering (loss of coolant), fuel heatup, cladding oxidation, fuel degradation (loss of rod geometry), and core material melting and relocation;

- heatup of reactor vessel lower head from relocated fuel materials, and the thermal and mechanical loading and failure of the vessel lower head, and transfer of core materials to the reactor vessel cavity;
- core-concrete attack and ensuing aerosol generation;
- in-vessel and ex-vessel hydrogen production (due to metal-water reaction in LWRs), transport, and combustion;
- fission product release (aerosol and vapor), transport, and deposition;
- behavior of radioactive aerosols in the reactor containment building, including scrubbing in water pools and aerosol mechanics in the containment atmosphere, such as particle agglomeration and gravitational settling; and
- impact of engineered safety features on the thermal-hydraulic and radionuclide behavior.

Various code packages designed as modular structures allow exchange of complete and consistent information among them. The design of intermodular communication allows complete coupling of modeled phenomena at every time step of the simulation. The numerical advancement scheme employs both explicit and implicit schemes. Explicit schemes are used for slower heat transfer processes, and implicit schemes are employed for hydrodynamics.

The MELCOR models systems and components are composed of a user-defined arrangement of “control volumes.” Control volumes are the basic building blocks of the simulation. No requirement for a specific, predefined nodalization for components allows user to control the degree of detail needed for specific simulation. Reactor-specific geometry is, however, imposed in modeling the reactor core in which core degradation and relocation can occur.

The original concept of MELCOR was for coarse mesh modeling with certain limitations in representation of structural details in the heat transport systems.

The following descriptions are taken largely from the MELCOR code manual.³⁸

4.9 STRUCTURE OF MELCOR

A top-level structure of the MELCOR code system is shown in Fig. 33. MELCOR is composed of a number of packages that model different accident phenomenon or control the execution of the program.

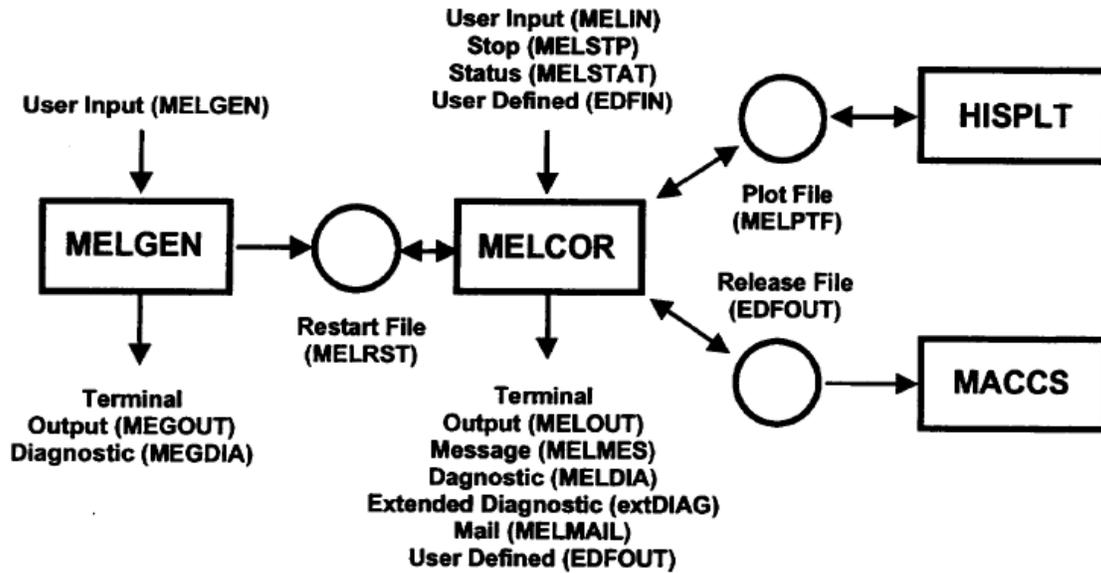


Fig. 33. Code structure of MELCOR.³⁸

The physical phenomena modeled by MELCOR are grouped into coding packages. The user invokes particular modeling feature by calling the package. Each package requires user input data for geometry and user-controlled selections to complete the component modeling descriptions. The documentation is organized around the package. Packages contained in MELCOR are listed with a brief description in Table 2.

Table 2. Packages contained in MELCOR

PACKAGE	DESCRIPTION
BH	<ul style="list-style-type: none"> Bottom head. This model was developed by the Oak Ridge National Laboratory, and is an alternative to the lower plenum modeling in COR.
BUR	<ul style="list-style-type: none"> Burn (combustion) of gases. Compares conditions within control volumes against criteria for deflagrations and detonations; initiates, and propagates deflagrations involving hydrogen and carbon monoxide; calculates burn completeness and flame speed.
CAV	<ul style="list-style-type: none"> Core-concrete interactions. CORCON-MOD3 with enhanced sensitivity analysis and multicavity capabilities.
CF	<ul style="list-style-type: none"> Control functions. Evaluates user-specified “control functions” and applies them to define or control various aspects of the computation such as opening and closing of valves; controlling plot, edit, and restart frequencies; defining new plot variables; etc.
CND	<ul style="list-style-type: none"> Condenser package. Models the effects of the isolation condenser system (ICS) and passive containment cooling system (PCCS), both of which use heat exchangers submerged in large water pools, intended primarily for some BWRs and the SBWR design concepts.

Table 2. (continued)

PACKAGE	DESCRIPTION
COR	<ul style="list-style-type: none">• Core behavior. Evaluates the behavior of the fuel and other core and lower plenum structures including heatup, candling, flow blockages, debris formation and relocation, bottom head failure, and release of core material to containment.
CVH	<ul style="list-style-type: none">• Control volume hydrodynamics. In conjunction with the FL package, evaluates mass and energy flows between control volumes.
CVT	<ul style="list-style-type: none">• Control volume thermodynamics. Evaluates the thermodynamic state within each control volume for the CVH package.
DCH	<ul style="list-style-type: none">• Decay heat. Used by other packages to evaluate decay heat power associated with radionuclide decay.
EDF	<ul style="list-style-type: none">• External data files. Controls the reading and writing of large external data files, closely interfaced with the control function and transfer process packages.
EOS	<ul style="list-style-type: none">• Equation of state. The CVT, H2O, and NCG packages are stored as one block of code under this name.
ESF	<ul style="list-style-type: none">• Engineered safety features. Models the thermal-hydraulics of engineered safety features that cannot be effectively modeled by building appropriate components or systems using the CVH, FL, HS, and CF packages.
EXEC	<ul style="list-style-type: none">• Executive package. Controls execution of MELGEN and MELCOR.
FDI	<ul style="list-style-type: none">• Fuel dispersal interactions. Models ex-vessel debris relocation, heat transfer, and oxidation due to fuel-coolant interactions and high-pressure melt ejection.
FL	<ul style="list-style-type: none">• Flow paths. Models, in conjunction with the CVH package, the flow rates of gases and liquid water through the flow paths that connect control volumes.
H2O	<ul style="list-style-type: none">• Water properties. Evaluates the water properties based on the Keenan and Keyes equation of state extended to high temperatures using the JANAF data. This set of routines is in the “EOS” code package.
HS	<ul style="list-style-type: none">• Heat structures. Models the thermal response of heat structures, and mass and heat transfer between heat structures and control volume pools and atmospheres. Treats conduction, condensation, convection, and radiation as well as degassing of unlined concrete.
MP	<ul style="list-style-type: none">• Material properties. Evaluates the physical properties of materials for other packages except for common steam and noncondensable gas properties (H2O and NCG).
NCG	<ul style="list-style-type: none">• Noncondensable gas equation of state. Evaluates the properties of noncondensable gas mixtures using an equation of state based on the JANAF data.
PAR	<ul style="list-style-type: none">• Passive autocatalytic hydrogen recombiner. Includes general models for modeling hydrogen recombiners in the containment.
PROG	<ul style="list-style-type: none">• Part of MELGEN/MELCOR executive package separated for computer library and link purposes.
RN	<ul style="list-style-type: none">• Radionuclide behavior. Models radionuclide releases, aerosol and fission product vapor behavior, transport through flow paths, and removal due to ESFs. Allows for simplified chemistry.
SPR	<ul style="list-style-type: none">• Sprays. Models the mass and heat transfer rates between spray droplets and control volumes.
TF	<ul style="list-style-type: none">• Tabular functions. Evaluates user-selected “tabular functions” to define or control various aspects of the computations such as mass and energy sources, integral decay heat, plot, edit, and restart frequencies, etc.
TP	<ul style="list-style-type: none">• Transfer process. Controls the transfer of core debris between various packages and the associated transfer of radionuclide within the RN package.
UTIL	<ul style="list-style-type: none">• Utility package. Contains various utilities employed by the rest of the code.

The main simulation packages are described more fully in the following sections.

4.9.1 Control Function (CF) package

The Control Function (CF) package is a general-purpose interface for user-defined mathematical functions. As the name indicates, the functions may be used to simulate the actual sensors and controls of the reactor system but are also used for controlling the simulation manually or incorporating physical interactions that are not provided in MELCOR's physics packages. For example, a control function may be used to apply a time-dependent boundary condition as a simplification to modeling the actual system that interacts with the model. The fuel pebble model in MELCOR-H2 of surface and maximum temperature in spherical geometry is an example in which the CF package is used to model a physical process not available in the MELCOR system.

The CF package allows the user to define functions using variables in the MELCOR database as input. The output values of the control functions are themselves variables in the database, each calculated from the start-of-step values of the variables which define its arguments. The output values of the CF functions are available to the other physics packages. Both real-valued and logical-valued control functions are available.

Note that each control function has a unique value at any time, because all of its arguments (which are other variables in the MELCOR database) are explicit functions of time. It may include a numerical integration or other logic so that its value depends on the history of its arguments over time. This is in contrast to tabular functions, which are functions in the pure mathematical sense. A tabular function accepts arguments and returns function values that depend only on current values of the arguments.

The CF package serves primarily as a utility.

1. The CF package has access to the MELCOR database of variables for use as arguments. The variable database requires that specific coding be included in the packages to include an internal variable in the database. Only a limited number of variables used in the modeling in the code are included in the database and are available for use as control function arguments. Programming changes to the MELCOR database program are required to add variables that are needed but not predefined in the data tables. The difficulty of programming changes can limit the uses of the control function.
2. The executive or any physics package may refer to a control function (meaning the value of that control function) by number.

Applications of control functions

A real-valued control function may be used to define an input quantity for a physics package, allowing the input to be a function of current conditions in the system being modeled. The possibilities include time-dependent effects from unmodeled parts or processes in the plant. For example:

1. rate of mass or enthalpy addition, or temperature of a mass source or sink (negative source) in the CVH package;
2. value of an independent thermodynamic variable in a time-specified volume in the CVH package;
3. velocity in a time-dependent flow path in the FL package;
4. fraction of a flow path, which is open (to represent valves, breaches, blow-out panels, etc.) in the FL package;
5. laminar friction coefficient in a flow path segment in the FL package (this is used to model the effects of filter loading);
6. inlet temperature for the dT/dz model in the COR package; and
7. fission power in the COR package.

Logical- or real-valued control functions may be used to initiate or control the operation of components or models as conditions change in a calculation. Examples include:

1. opening and closing of valves in the FL package,
2. operation of pumps in the FL package, and
3. failure of the lower head in the COR package.

In all of these cases, complex functions may be built up as desired. For example, a relief valve may be controlled as a function of the pressure difference between two control volumes, including appropriate static head terms. The different setpoints in a multibank relief valve system may also be modeled, and a block or bypass valve may be included if desired.

Proportional-integral-differential (PID) control function

This control function is used in control system design defined by the equation

$$f^n = R_1 a_1^n + R_2 \int_{t^n} a_1(t) dt + R_3 \left. \frac{da_1}{dt} \right|_{t^n}, \quad (4.9-1)$$

where R_1 , R_2 , and R_3 are input as real constants. The PID control function can be evaluated using the built-in derivative—either centered difference or forward difference—and integral functions.

Hysteresis (HYST) control function

The HYST control function is used to model the type of hysteresis behavior exhibited by components such as relief valves, which are opened as the controlling variable (e.g., differential pressure), increases, and closed as it decreases with a dead band between. The behavior can be mathematically expressed as

$$f^n = \begin{cases} \max[f^{n-1}, f_{LOAD}(a_1^n)], & a_1^n \geq a_1^{n-1} \\ \min[f^{n-1}, f_{UNLOAD}(a_1^n)], & a_1^n < 0 \end{cases}, \quad (4.9-2)$$

where f_{LOAD} and f_{UNLOAD} represent functional relationships for the upper and lower curves of the hysteresis loop. When the variable a_1^n (e.g., a differential pressure on a check valve) goes above the upper curve, f_{LOAD} , the control variable is loaded (e.g., check valve opens). Similarly, when a_1^n goes below the lower curve, f_{UNLOAD} , the control function state is unloaded (e.g., check valve closes). When it is between the curves, the function remains its last state, either loaded or unloaded.

Trips

The MELCOR control function package includes a variety of TRIP functions. Each requires either a logical or a real argument. Additional arguments may be required to define the necessary setpoints. The latter class of function is used to model switching phenomena involving a dead band (such as a heater, which turns on when the temperature falls below T_1 , and does not turn off until the temperature has risen above T_2).

In its simplest form, a controlled parameter has only two states—OFF and ON, which can be represented as a logical function. MELCOR, however, employs a more general implementation where trips have been implemented as real-valued functions. The function value is zero if the trip is off and nonzero if it is on.

User-defined functions

In order to simplify the addition of special-purpose functions, interfaces are provided for ten user-defined functions with names FUN1, FUN2, ..., FUN10. Each subroutine is coded as a function of five real arguments and includes an error flag in its calling sequence.

In order to make use of the interfaces, the user must generate his/her subroutines in the form

```
REAL FUNCTION FUNn(A1, A2, A3, A4, A5, IERROR).
```

The arguments A1 through A5, defined as for any other type of control function, may be used as desired in evaluating FUNn.

4.9.2 Core (COR) package

The MELCOR COR package calculates the thermal response of the core and lower plenum structures, including the portion of the lower head directly beneath the core, and models the relocation of core materials during melting, slumping, and debris formation. The features of the COR package is based primarily on the physical geometry and design features of LWR cores and fuel designs. The structures can be adapted approximately for NGNP fuel and core geometry. For example, its debris field simulation is used to model the pebble bed geometry. The prismatic fuel core models to date have used the more general CVH and FL packages to model core nodes. The COR package also calculates a simplified mechanical response of the lower head to the differential pressure between the lower plenum inside the vessel and the reactor cavity outside the vessel. An alternative modeling of lower plenum and lower head phenomena is optionally available through the separate bottom head (BH) package. Multiple structures are modeled as separate components within a single core cell. Intact components include fuel pellets, cladding, canister boxes, and other structures, such as control rods. Particulate debris is also modeled as a possible component within a core cell.

All important heat transfer processes are modeled for each cell component. Thermal radiation among the various components within a cell and between cells in both the axial and radial directions is included, as well as radiation to boundary structures, such as the core shroud or upper plenum, and to a liquid pool. Melting of boundary steel structures, with addition of the molten steel to the core debris, may be modeled using appropriate input to the HS package. Gap radiation/conduction between fuel and cladding and axial conduction in each of the components is modeled. Convection to the fluid in adjacent control volumes is modeled for a wide range of fluid conditions and structure surface temperatures, including nucleate and transition film boiling.

The core degradation model treats eutectic reactions that lead to liquefaction below normal melting points, dissolution reactions that lead to significant fuel relocation below the UO₂ melting temperature, “candling” of molten core materials (i.e., downward flow and refreezing), and the formation and relocation of particulate debris. Various geometric variables (e.g., cell surface areas and volumes) are updated for changing core geometry.

Changes in core flow resistance resulting from relocation of core materials may be modeled, but the connection to the hydrodynamic packages (CVH and FL) is not automatic. Input on FLnnnBk records is required to specify which core cells are associated with each flow path involving the core. Because only

CVH and FL model the flow of water and gases, the effects of blockages on circulation can be modeled only to the extent that the CVH/FL nodalization can resolve that circulation.

Each core cell may contain one or more components of conventional LWR fuel design. Seven intact components are modeled:

1. fuel pellets,
2. cladding,
3. BWR canister walls,
4. supporting structure,
5. nonsupporting structure, and
6. other structure.

NGNP core models do not utilize the LWR fuel features. As discussed in Sect. 4.12.1, the pebble bed core is modeled using a particulate debris option of the COR model to represent the coolant flow in the core region. Prismatic fuel core model, which is discussed in Sect. 4.12.2, is modeled using CVH, HS, and FL components rather than using the COR package.

A lumped parameter approach is used for each component within a cell; therefore, each component is represented by a single temperature. All heat transfer processes between components are approximated by point differences between temperatures (as opposed to an integrated average difference using a spatial distribution of temperatures over the control volume). All thermal calculations are done using internal energies of the materials, and the mass and internal energy of each material in each component are tracked separately to conserve total mass and energy.

Several geometric variables are used to further describe the cells. For each structural component a surface area is defined for convection and oxidation calculations; the canister components have defined surface areas for each side to communicate separately with the channel and bypass control volumes. The effects of conglomerate debris on component surface areas are factored into the oxidation calculations, and for oxidation of debris, separate Zircaloy and steel surface areas are used. Equivalent diameters for each component are also specified for use in various heat transfer correlations. Cell boundary areas for inter-cell radiation (both axially and radially) are defined. Volumes of components and the “empty” fluid space are tracked for core slumping and flow blockage calculations.

For each radial ring, the user can define up to three representative penetrations (e.g., instrumentation tubes or guide tubes) in the lower head, specifying their mass and surface area. The lower head is modeled as a hemispherical shell of user-specified thickness and composition. The user must specify the thickness and composition of an arbitrary number of radial nodes (not to exceed 24) beginning from the outer surface of the hemisphere and progressing inward. In addition to stainless steel, which is included in the COR package database, the user may specify up to six materials in a composite lower head. Hence, with appropriate materials properties (MP) package input, the user may model insulation, carbon steel, and a stainless steel liner if desired. The outer node (surface) communicates with the CVH fluid in the reactor cavity, and downward-facing boiling heat transfer to a flooded cavity is modeled. The inner node (surface) communicates thermally with both the penetrations and the debris. Heat transfer from the debris to the lower head and its penetrations is modeled parametrically. A one-dimensional solution is used to determine the temperature profile through the lower head. The temperature profile and the loading of the vessel can be used by the lower-head mechanical model to predict creep-rupture failure of the lower head using the Larson-Miller parameter and a life-fraction rule.

The COR package uses an explicit numerical scheme for advancing the thermal state of the core through time. To address potential numerical instabilities in the COR model, a subdivided-time step capability has been developed to allow the COR package to take multiple time steps across a single system time cycle. All energy generation and heat transfer rates are evaluated at the beginning of a COR package’s time step based on current temperatures, geometric conditions, and an estimate of the local fluid conditions

(calculated by the COR package dT/dz model to reflect the temperature variation of a control volume containing many individual core cells). The net energy gain (or loss) across the COR package time step is determined for each component by multiplying these rates by the COR package time step. The COR package time step is automatically adjusted based on user-supplied control parameters. The temperature change for any component with total mass greater than a user-specified minimum is limited to a user-specified maximum. If the calculated temperature change is greater than this limit; the core time step is reduced. If the energy input to any fluid volume changes from previous values in such a way as to possibly result in numeric instability between the COR and CVH packages, the system time step may be immediately cut or a reduction may be requested for the next system cycle.

4.9.3 Control volume hydrodynamics (CVH) package

The Control Volume Hydrodynamics (CVH) and Flow Path (FL) packages model the thermal-hydraulic behavior of liquid water, water vapor, and gases in MELCOR. Modeling is based on a discrete control volumes connected by flow paths. Connections are defined by input to the FL package described in the following section.

All hydrodynamic material including the coolant (water or helium), vapor and fog, and noncondensable gases, each with its associated energy calculation resides in control volumes. The control volume contains a multicomponent fluid. The model represents the conservation of mass and energy of each component. The CVH package does not include core structures or core debris, other heat structures, fission products, aerosols, water films on heat structures or ice (e.g., for ice condenser containment models).

Mass and energy sources and sinks

CVH input allows the definition of explicit sources and sinks (negative sources) of mass and/or energy as boundary conditions to represent unmodeled parts of the system. Additional sources and sinks may be imposed by other packages during a MELCOR calculation; these are included automatically and do not require input to CVH. Heat sources are included from the Core (COR), Cavity (CAV), Fan Cooler (FCL), Fuel Dispersal Interactions (FDI), Radionuclide (RN), Spray (SPR), and Heat Structure (HS) packages. Because a thermochemical reference point is used in thermodynamics, gas combustion modeled in the Burn (BUR) package does not involve an explicit heat source; the heat of combustion is implicit in the enthalpy functions.

4.9.4 Flow Path (FL) package

FL input includes all definition of flow resistance, including any frictional losses associated with the walls and unrecoverable form loss of control volumes and blockages calculated by the COR package. Special models including externally controlled flow areas (valves), forced flows, and momentum sources (pumps) are also defined by FL input in conjunction with functions defined by the Tabular Function (TF) and Control Function (CF) packages.

As shown in Fig. 34, each flow path connects two control volumes. Each connection is referred to as a junction; the two junctions associated with a flow path may be at different elevations. One volume is referred to as the *from* volume and the other as the *to* volume, thus defining the direction of positive flow.

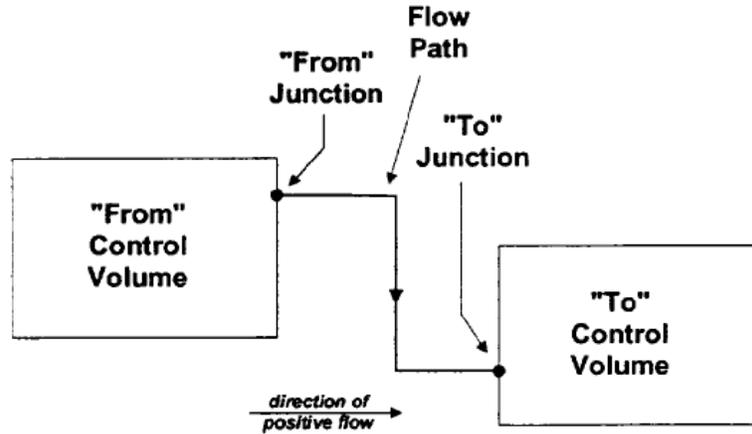


Fig. 34. Flow path definition.³⁸

A flow path may represent a pipe-like connection in a tank-and-tube model, or the open area of a separating surface (cell boundary) in a finite-difference-like model. The former case represents the limit of a control volume when residence effects are not important. The primary difference is in the definition of junctions and control volumes.

All dissipative pressure drops between volumes are assumed to take place within the flow paths connecting them. Contributions from both form loss and wall friction are included in the dissipative losses.

The form loss calculation is based on user-input loss coefficients, K , given by Eq. (4.9-3), which may be different for forward and reverse flow.

$$\Delta P_{\varphi} = -\frac{1}{2} K \rho_{\varphi} |v_{\varphi}| v_{\varphi}, \quad (4.9-3)$$

where ρ is density, v is velocity, and φ is a subscript P or A to denote pool or atmosphere.

Special flow path models

Several additional models are available for use in flow paths. These can be used to modify the fraction of the flow path area that is open, define momentum sources in the path, specify the velocity in the path, modify the treatment of two-phase flow, include the effects of momentum flux, or model blockage of the path by materials such as core debris.

Valves

The user may include a valve in a flow path to control the fraction of the area of the path that is open. The open area of the flow path is defined as the fully open area multiplied by the fraction open. Valves do not modify the areas of flow path segments and, therefore, do not affect the dependence of wall friction on volumetric flow.

Pumps and fans

Pumps can be included in flow paths. In the flow path momentum equation, they are modeled as introducing a pressure “boost,” which is ordinarily a function of the volumetric flow through the path. In defining a pump, the flow should be thought of as the independent variable and the pressure head delivered by the pump as the dependent variable; the actual flow on any time step is calculated from the balance of this head (as a function of flow) against static, frictional, and acceleration pressure differentials in the rest of the flow circuit.

There are two types of pumps available in MELCOR. The first, referred to as “FANA,” was originally intended to model a fan that impels the atmosphere through a flow path. It can also be used to represent a constant speed coolant pump, although in a very simple form. The second, called “QUICK-CF,” simply uses a control function to define the pressure head, allowing the user complete freedom but also giving him complete responsibility for all details.

Both models are numerically explicit; that is, the pressure head is based on conditions at the start of the MELCOR system time step and remains unchanged throughout the step—even if the CVH package is subdividing the main time step.

The MELCOR-H2 model contains steady state models of the momentum and flow in gas turbines and compressor which are more detailed representations of the head/flow relationship. These models are contained in Sects. 4.11.2 and 4.11.3.

Time-dependent flow paths

Velocities in a flow path can be specified by the user through control functions or tabular functions. The specified velocity is used for both the atmosphere and the pool. The void fraction is calculated using the standard model.

Modeling breaks and failures

All types of failures which lead to the opening of additional paths for fluid flow are modeled by using flow paths containing valves which are defined to open when a failure criterion is reached. This includes pipe breaks, melt-through or catastrophic failure of the pressure vessel, failure of rupture disks and blowout panels, and failure of containment.

4.9.5 Heat Structure (HS) package

The MELCOR HS package calculates heat conduction within an intact, solid structure, and energy transfer across its boundary surfaces into control volumes. The heat structure itself is a general-purpose, solid volume. HS modules can represent pressure vessel internals and walls, containment structure and walls, fuel rods with nuclear or electrical heating, steam generator tubes, and piping walls.

Figure 35 illustrates a heat structure in a CVH control volume. The geometry of the solid can be rectangular, as shown in Fig. 35, cylindrical, spherical, or hemispherical geometry.

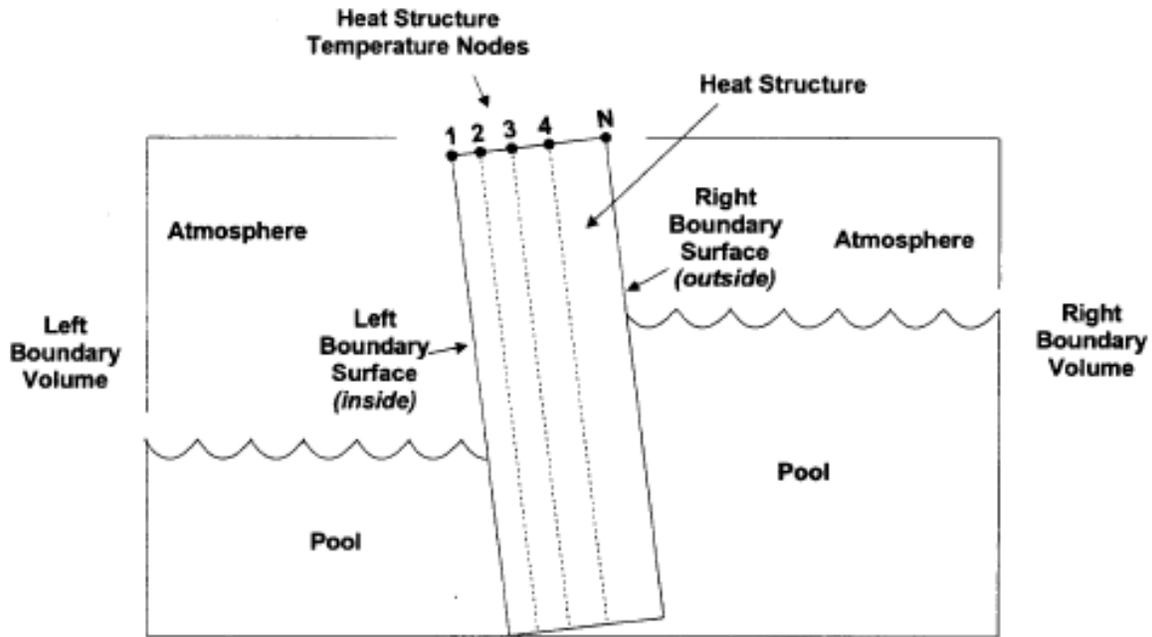


Fig. 35. Heat structure in a control volume.³⁸

Finite-difference equations are used to advance the temperature distribution of a heat structure in time during MELCOR execution or to obtain its steady-state temperature distribution. These equations are obtained from an integral form of the one-dimensional heat conduction equation and boundary conditions using a fully implicit numerical method.

4.9.6 Material Properties (MP) package

The MELCOR MP package models the physical properties needed by many of the various physics packages using analytical laws, correlations, or lookup tables. These properties include thermodynamic state and transport properties needed for structural materials as well as transport properties for water and noncondensable gases. Material properties needed for modeling gas-cooled reactors have been added to the library of materials in the MELCOR-H2 version of the code.

4.10 MELCOR-H2 Extensions for VHTR Plant Models

MELCOR-H2³⁹ is an extended version of MELCOR designed to couple a detailed MELCOR model of nuclear reactors with modular secondary system components and thermochemical cycles for the production of hydrogen and electricity. The main emphasis of MELCOR has been the reactor core and the containment models under severe accident conditions, but MELCOR physics packages are able to represent most secondary loop components. By proper assembly of the physics packages representing control volumes (CVH), flow paths (FL), and heat structure (HS), modules can represent the normal components of vessels, pipes, and valves that are used in NGNP designs. However, some significant models are lacking. MELCOR-H2 has added components which are not modeled in the standard MELCOR physics packages.

Current MELCOR-H2 extended capabilities include:

- the ability to simulate secondary system components such as compressors, turbines, and the intermediate heat exchanger;

- sulfur-iodine (SI) chemistry;
- Westinghouse hybrid sulfur (HyS) chemistry;
- neutron point kinetics;
- pebble fuel heat transfer model; and
- a real-time, interactive graphical user interface.

The extensions are general-purpose packages that can be adapted through input to represent a range of secondary plant loop arrangements and components.

MELCOR-H2 provides fully integrated simulation capability of a nuclear power plant that is attached to a process plant, which allows execution of transient response of the plant to various disturbances including those originating due to disturbances in the heat loads of the plant. For illustration of the capabilities, a schematic of the reactor (primary cycle), power conversion system (secondary cycle), and the SI process cycle is shown in Fig. 36.

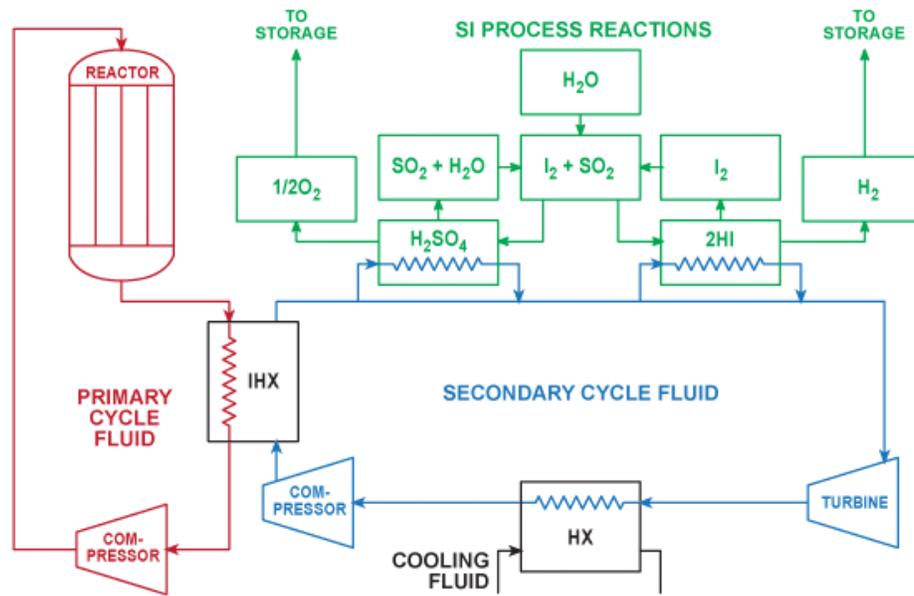


Fig. 36. Schematic of a nuclear reactor that is fully coupled to a thermochemical sulfur-iodine cycle and the power conversion system.³⁹

Rodriguez indicates that the following transients can be performed with MELCOR-H2:

1. Loss of flow accidents
 - a. Primary system
 - b. Secondary system
2. Chemical leaks from the process loop
 - a. H_2 , SO_2 , H_2SO_4 , etc.
 - b. H_2 deflagration
3. Air ingress, graphite oxidation
4. System feedback, core reactivity effects, system perturbations
5. System startup, turbine and compressor transients, plant design changes, etc.

MELCOR-H2 has also added a display of system transient variables calculated at each time step of the execution of simulation in real time on the graphical user interface (GUI). The interactive GUI (Fig. 37) also allows changing certain input parameters as the simulation is executed and observing the response of the system as the simulation progresses.

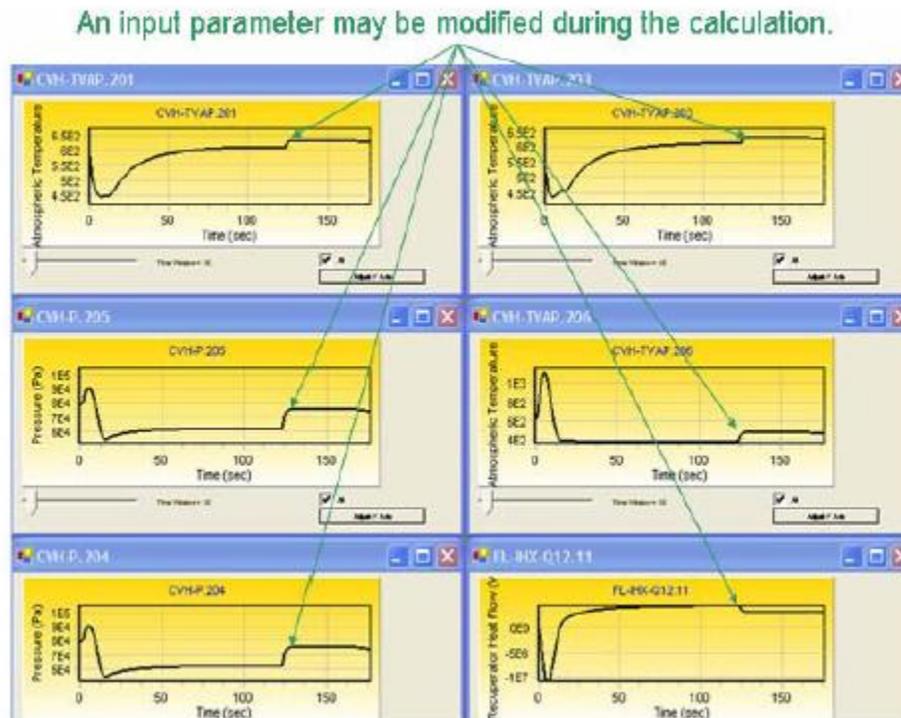


Fig. 37. Snapshot of the graphical user interface of MELCOR-H2.³⁹

The MELCOR-H2 system models are currently in a developmental stage and can be expected to undergo further additions and refinements to make the MELCOR-H2 a production code for control and protection

system analysis. A certain amount of benchmarking of the MELCOR code to other codes has been reported but the version should not be considered a verified code.

4.11 Modeling the Secondary Loop and the Balance of Plant in MELCOR

The following modeling sections which describe the formulations in MELCOR-H2 are extracted from Rodriguez³⁹ with minor editing and condensing of the original text.

4.11.1 Gas turbine, compressor, and heat transfer models

A closed Brayton cycle (CBC) for electrical power generation plants is being considered for a portion of the energy conversion of NGNP. A typical configuration in which the CBC is in parallel with hydrogen production is shown in Fig. 36. The Brayton cycle, in this example, is a single shaft design, meaning that the turbine, compressor, and electrical generator are all on the same shaft. For the closed cycle design, a heat exchanger to cool the fluid exiting the turbine before entering the compressor is thermodynamically necessary. Hence, these three components for the model are necessary and are developed to be compatible in the simulation. Other configurations are possible with the MELCOR-H2 models. This section describes these three related components for a CBC. The MELCOR-H2 models are all described in Rodriguez³⁹.

The MELCOR-H2 turbine and compressor models grew out of work by Tournier and El-Genk at the Institute for Space and Nuclear Power Systems at the University of New Mexico^{40,41}. Their turbine model was designed primarily for steady state thermal cycle analysis of the NGNP and other reactors. The models of the turbine and compressor in these earlier codes employ solutions of the steady-state conservation equations fluid momentum, energy, and mass. The same turbine and compressor models have been incorporated into MELCOR-H2 as quasi-steady models of the gas flow and energy conversion processes. The quasi-steady approximations neglect the time derivative terms in the conservation equations and are appropriate for the range of time scales in which the dynamics of interest are much slower than the dynamics for the storage of shaft momentum and storage of energy and mass in the working fluid of the turbine and compressor. Also the model does not include the dynamics of the shaft momentum. Shaft speed is an input to the fluid model. The fixed shaft speed input is appropriate for the normal operating condition in which the shaft is synchronized to the grid. However, the fixed speed model would not simulate the necessary dynamics and interactions between control and process models for the overspeed transient that follows a load rejection transient. In this transient, the generator becomes electrically disconnected from the grid, losing the grid's regulation of shaft speed. The plant controls and/or safety systems must act to prevent a damaging overspeed of the turbine-compressor-generator shaft.

In addition to the quasi-steady approximations of conservation equations, the performance modeling ancestry of the MELCOR turbine and compressor models leads to a modeling approach that bases the performance on the fundamental geometric parameters of the turbine design. To explain this approach, it is noted that a simpler and more common approach, as in RELAP, is to input performance maps which relate flow, torque, and pressure change in the turbine. The performance maps are steady-state parametric relationships. They may be obtained from external detailed turbine design calculations or may be based on homologous relationships that normalize performance maps for a whole class of similar turbines or compressors in average functional relations written in terms of dimensionless variables. The performance maps contain the essential relationships between pressure, flow, and momentum transfer in functional or tabular form which are needed for the dynamic model. The alternative approach used in MELCOR-H2 is to derive the performance maps from the actual turbine or compressor geometric parameters.

The approach used in MELCOR-H2 requires detailed geometrical data for the turbine, such as the rotor diameters, blade angles, blade chord length, blade pitch, and so forth. An initialization routine in the code then uses built-in analytical and empirical physical relationships collected by Tournier and El Genk from

the open literature to compute parameters in performance mapping functions needed for the modeling calculations. The initialization calculation for the turbine is, in effect, an open-source turbine design code like the proprietary codes used by turbine vendors. These performance relationships are then fed to the quasi-steady calculation of shaft power and exiting fluid conditions for the device. The advantage of the MELCOR-H2 approach is that the model can be tailored very exactly to a specific turbine design. The disadvantage is the need for detailed geometric data on the turbine to construct the model. In many instances, only the turbine manufacturer would have access to such data. The performance that is calculated by MELCOR also depends on the selection of the empirical relationships which are used in the model. These relationships, which are described in this section, are from the open literature. These relationships have a known accuracy regarding the fit to experimental data but unknown impact on the accuracy of the application. Another problem is that at early stages of development when scoping and feasibility studies are being done, the actual turbine design and the data needed for generating the model may not yet exist. The authors address the issue of input data in their example of a construction of a model of the Japanese GTHT300 6-stage axial-flow turbine. Publicly available data sources lacked sufficient detail to fully determine the model inputs. The report goes through the assumptions and estimates that were necessary to fill in missing data. The approach matched turbine design to the available operating point data using rules of thumb for turbine design. The remaining unknown parameters were then adjusted to optimize the system performance. This approach assumes that the designers of the actual system would follow a similar optimization approach and find a similar optimum configuration. The complete input data which were assembled for the GTHT300 model are provided in the Appendix D of Rodriguez³⁹. These data serve as a guide for other turbine modeling cases. Despite the need for estimating and approximating the missing input, the performance maps match published data for the GTHT300 very well. The success of the model probably reflects a very deep understanding of turbine design and performance mapping calculations by the developers of the MELCOR-H2 turbine and compressor models. The requirement for such skills to formulate the model input set-up raises the difficulty level for the user in developing a full system model.

The following sections go through the modeling equations in some detail both to explain how the difficult problem of turbine and compressor modeling is solved and to have some basis for discussing the limitations of the model.

Nomenclature for turbine and compressor models

A	Cross-sectional flow area (m^2)
c	Gas sonic velocity (m/s) $c = \sqrt{\gamma RT}$
C	Actual chord length of blade (m)
C_L	Blades lift coefficient based on mean vector velocity
C_p	Specific heat at constant pressure (J/kg.K)
CR	Convergence ratio, $CR = \cos \phi_1 / \cos \phi_2$
C_v	Heat capacity at constant pressure (j/kg.K), $C_v = C_p - R$
C_x	Axial chord length of blade (m), $C_x = C \times \cos \Phi$
D	Diameter (m)
D_{eq}	Equivalent diffusion ratio (suction surface peak velocity/outlet velocity)
D_{eq}	Equivalent hydraulic diameter (m)
D_{hub}	Hub diameter of rotor wheel (m)
e	Internal energy per unit mass (J/kg)
f	Darcy friction factor
F_t	Tangential loading parameter
h	Enthalpy per unit mass, $h = e + P/\rho$ (J/kg)

\hat{h}	Stagnation (or total) enthalpy per unit mass, $\hat{h} = h + 0.5\bar{\alpha}_3 V^2$ (J/kg)
H	Height of blades (m)
h^{CV}	Convective heat transfer coefficient (W/m ² .K), $h^{CV} = Nu \lambda / D_{eq}$
H_{TE}	Boundary-layer shape factor, $H_{TE} = \delta_{TE}^* / \theta_{TE}$
i	Blade incidence angle at leading edge (°)
i_C	Negative stall incidence angle of blades cascade (°)
i_o	Blade incidence angle for zero camber (°)
i_S	Positive stall incidence angle of blades cascade (°)
i_{SR}	Reference stalling incidence angle for turbine cascade with $S/C = 0.75$ (°)
i^*	Optimum design incidence angle at leading edge of compressor blades (°)
K_{inc}	Off-design incidence correction factor
k	Boltzmann constant, $k = 1.3804 \times 10^{-23}$ J/K
L	Length of flow channel (m)
L_{fin}	Length of heat transfer fins (m)
\dot{m}	Mass flow rate of working fluid (kg/ s)
M	Molecular weight (kg/mole)
Ma	Gas Mach number, $Ma = V / c$
N	Shaft angular speed in rotations per minute (rpm)
N_a	Avogadro number, $N_a = 6.0225 \times 10^{23}$ molecules/mole
N_{rot}	Number of rotor blades
N_{sta}	Number of stator blades
Nu	Coolant Nusselt number
O	Throat width between blades in cascade (m)
P	Pressure (Pa)
\hat{P}	Stagnation (or total) pressure, $2\hat{P} = P + 0.5\bar{\alpha}_3 \rho V^2$ (Pa)
Pe	Peclet number, $Pe = Re \cdot Pr$
Pr	Coolant Prandtl number, $Pr = \mu C_p / \lambda$
r	Average radius of blade (m), $r = 0.5 \times (r_{hub} + r_{tip})$
R	Gas constant, $R = R_g / M$ (J/kg.K)
R	Radius (m)
Re	Flow Reynolds number, $Re = \rho V D_{eq} / \mu$
S	Pitch or distance between blades in cascade (m)
S_{fin}	Finned heat transfer surface area (m ²)
S_{un}	Unfinned heat transfer surface area (m ²)
R_g	Universal gas constant, $R_g = k N_a = 8.3143$ J/mole.K
t	Time (s)
t_{max}	Maximum blade thickness (m)
t_{TE}	Thickness of blades trailing edge (m)
T	Temperature (K)
U	Rotor tangential velocity (m/s), $U = R\omega$
\vec{V}	Gas absolute velocity vector (m/s)

V_r	Gas radial velocity component (m/s)
V_x	Gas meridional velocity component (m/s)
V_θ	Gas tangential velocity component (m/s)
\bar{V}	Average flow velocity in channel (m/s)
\vec{W}	Gas relative velocity vector with respect to rotor wheel (m/s), $\vec{W} = \vec{V} - \vec{U}$
\dot{W}	Rate of mechanical work done by working fluid on surroundings (W)
Y	Pressure loss coefficient of a blade cascade
Z/C	Relative position of maximum camber, measured from leading edge
Z_{TE}	Spanwise penetration depth between primary and secondary loss regions (m)

Greek

Angle between gas absolute velocity vector and meridional plane (degrees)

$\bar{\alpha}_n$	Coefficient which accounts for the nonuniformity of velocity profile
$\bar{\alpha}_2$	Velocity profile correction factor, $\bar{\alpha}_2 = 1.020$ for turbulent flow
$\bar{\alpha}_3$	Velocity profile correction factor, $\bar{\alpha}_3 = 1.056$ for turbulent flow
β	Blade angle relative to meridional plane ($^\circ$)
γ	Ratio of specific heat capacities, $\gamma = C_p/C_v$
Γ^*	Blade circulation parameter (dimensionless)
δ	Boundary layer thickness (m)
δ^*	Boundary layer displacement thickness (m)
δ_{fin}	Thickness of heat transfer fins (m)
δ_M	Mach number correction to incidence angle ($^\circ$)
Δi_s	Stalling incidence angle correction for other S/C values (degrees)
ΔP	Total pressure loss (Pa)
$\Delta\Phi$	Kinetic energy loss coefficient
ζ	Camber angle of compressor blades ($^\circ$), $\zeta = \beta_1 - \beta_2 $
η	Efficiency, dimensionless
θ	Boundary layer momentum thickness (m)
λ	Thermal conductivity (W/m.K)
μ	Coolant dynamic viscosity (kg/m.s)
ρ	Density (kg/m ³)
σ	Blade cascade solidity, $\sigma = C/S$
τ	Blades clearance gap (m)
ϕ	Angle between gas relative velocity vector and meridional plane (degrees)
Φ	Blades stagger angle measured from axial direction (degrees)
ω	Shaft angular speed (radians/s)

Subscript/Superscript

θ	Tangential or “whirl” component
AM	Loss model of Ainley and Mathieson ⁴²
b	Coolant bulk

<i>C</i>	Compressor
<i>cas</i>	Casing of turbomachinery
<i>disk</i>	Disk friction losses degraded to gas enthalpy increase
<i>fin</i>	Heat transfer fins
<i>hub</i>	Hub of impeller
<i>LE</i>	Leading edge of blades
<i>n</i>	Iteration number
<i>o</i>	Value for constant properties case
<i>p</i>	Profile losses
<i>r</i>	Radial component
<i>s</i>	Secondary losses
<i>T</i>	Turbine
<i>TC</i>	Tip clearance losses
<i>TE</i>	Trailing edge of blades
<i>Tip</i>	Tip of impeller
<i>w</i>	Wall surface
<i>wind</i>	Windage mechanical losses
<i>x, z</i>	Axial component
<i>0</i>	Inlet of contraction/expansion zone (previous blade trailing edge)
<i>1</i>	Inlet of blades cascade (leading edge)
<i>2</i>	Outlet of blades cascade (trailing edge)
<i>(n)</i>	Best estimate at present iteration
<i>(n + 1)</i>	New value at completion of iteration

4.11.2 Turbine modeling equations

Figure 38 illustrates the basic configuration of an axial-flow turbine with three stages. Each stage consists of a cascade of stationary blades (Inlet Guide Vanes, IGV, or Stator, S), which increase the swirl (tangential) velocity of the gas in the direction of rotation, followed by a cascade of rotating blades (Rotor, R), which absorb the gas swirl velocity and convert it to rotor mechanical (or kinetic) energy. Both processes in the turbine operate at the expense of gas static pressure, so that the gas pressure decreases as the gas flows through each blade cascade. It is a common practice in axial-flow turbomachines to design a multistage turbine for nearly constant axial flow velocity throughout. To achieve this result, the annular flow area must increase from inlet to outlet since the gas pressure and density decrease as the gas flows through the turbine. Typically, an exit guide vane cascade (EGV) follows the last turbine stage to remove any residual swirl velocity and convert the radial component of kinetic energy into axial energy which then can be used to increase the static pressure. Although not shown on the figure, a diffuser follows the EGVs to recover as much kinetic energy as possible, as well as to direct the flow to its intended destination. Similarly, an inlet flow passage precedes the inlet guide vanes. The inlet flow design can range from a smooth axial bell-mouth inlet to a complex side-inlet, depending on the application.

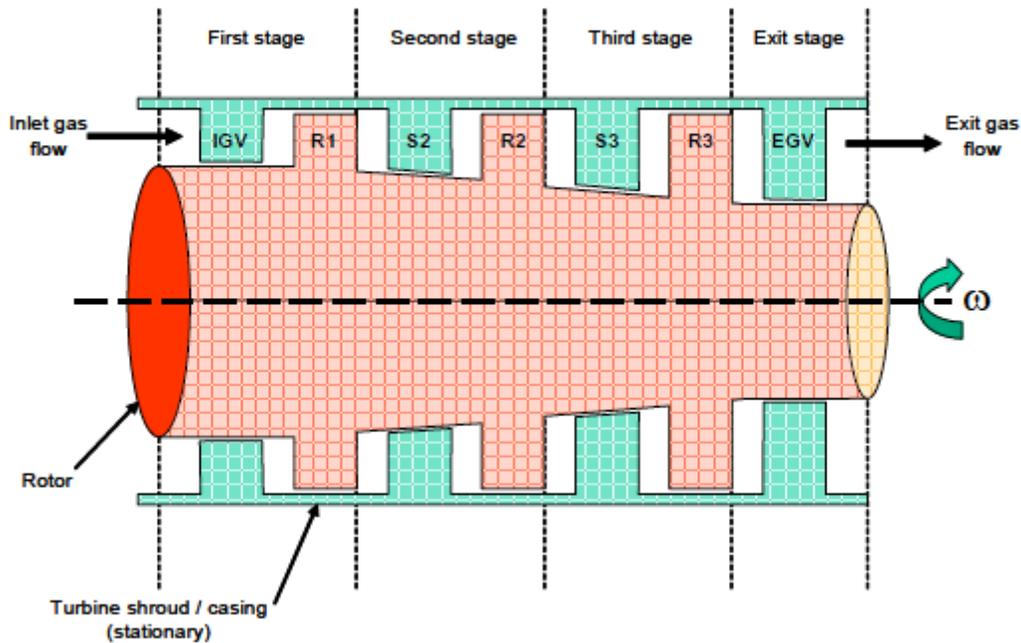


Fig. 38. Schematic of a multistage axial-flow turbine.³⁹

The model is based on steady state conservation of flow, energy, and mass which means that no time derivative terms are retained in the conservation equations. Also, no equation for conservation of shaft momentum is included in the model. The shaft speed is an input in the parameterization.

Velocity diagrams (or triangles) at the leading and trailing edges of a turbine rotor cascade as shown in Fig. 39 are a fundamental tool for all turbomachinery aerodynamic design and analysis. Since successive blade cascades alternate between stator and rotor, it is necessary to be able to view the velocity vectors in both stationary and rotating coordinate systems at any location. An orthogonal coordinate system (x, θ) is used where the meridional coordinate, x , is identical to the axial coordinate (axis of the turbomachinery), and θ is the polar angle of a cylindrical coordinate system. Subscript 1 refers to the cascade inlet station, and subscript 2 refers to the cascade exit station. The velocity in the stationary coordinate system (absolute velocity) is designated by V , and the velocity in the rotating coordinate system (relative velocity) is designated as W . Finally, U is the tangential velocity of the rotating blades ($U = U_\theta$), and α and φ designate the absolute and relative velocity angles, respectively as shown in Fig. 39. The tangential velocity is related to the angular velocity by $U = R\omega$, where R is the average radius of the blade, and ω is the angular velocity in radians per second.

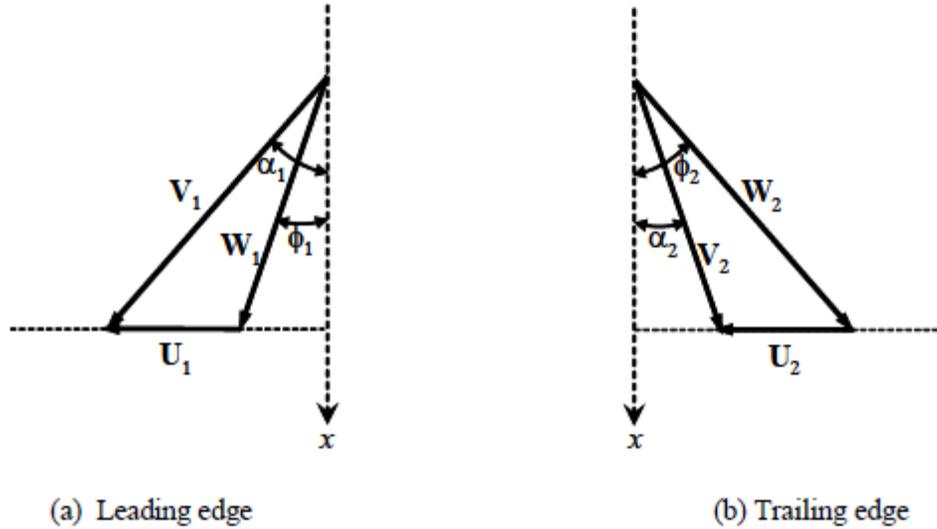


Fig. 39. Velocity triangles for turbine rotor blades.

The total pressure loss coefficient in the flow equation of a turbine blades cascade is the sum of the coefficients for profile losses, secondary losses, trailing edge losses, and tip clearance (leakage). Ainley and Mathieson⁴² have introduced an off-design incidence correction factor, K_{inc} , such that the total pressure loss coefficient under transient and other off-design conditions can be written generally as:

$$Y = K_{inc} \times (1 - Z_{TE} / H) \times Y'_p + Y'_s + Y_{TE} + Y_{TC} \quad . \quad (4.11-1)$$

The main work in formulating the MELCOR-H2 model of the turbine is finding appropriate empirical correlations for the loss terms in Eq. (4.11-1). These equations are given in Rodriguez³⁹. The main reference is Ainley and Mathieson⁴² with contribution from a number of subsequent authors who have developed numerical fits to the graphical correlations in the Ainley and Mathieson monograph or who have refined and improved the formulation of the loss terms. For completeness in reporting on the modeling equations in MELCOR-H2 and to give some indication of the input detail, the formulae for the loss coefficients in MELCOR-H2 model are collected in Appendix A.

The numerical solution of a multistage turbomachinery component proceeds in the direction of the flow; that is, when conditions are known at the entrance of a section, the outlet conditions are calculated as a function of inlet conditions, from section to section and stage to stage, moving downstream. Each stage consists of a stator half-stage, followed by a rotor half-stage (except the EGVs, which are followed by a diffuser). The numerical subscript {0} indicates the inlet of contraction/expansion zone (previous blade trailing edge), {1} the inlet of blades cascade (leading edge), and {2} the outlet of blades cascade (trailing edge). A half-stage consists of an isentropic expansion section {0-1} between two cascades, followed by a blades section⁴³ that exhibits pressure losses. All fluid and flow conditions are assumed known at station {0}. The solution proceeds in the direction of flow to calculate the flow conditions at stations {1} and {2}. The relative gas flow angle, ϕ_2 , at the trailing edge of the blades is a function of the blades angle and the deviation angle, δ :

$$\phi_2 = \beta_2 + \delta \quad . \quad (4.11-2)$$

The deviation angle at the trailing edge of a turbine blade cascade is calculated using a correlation developed by Zhu and Sjolander⁴⁴, as:

$$\delta = 17.3 \frac{(S/C)^{0.05} \times (\phi_1 + \beta_2)^{0.63} \times \cos^2(\Phi) \times (t_{\max}/C)^{0.29}}{(30 + 0.01\beta_1^{2.07}) \times \tanh(\text{Re}_{2C}/200,000)} , \quad (4.11-3)$$

where all angles are expressed in degrees. The Reynolds number at the trailing edge is based on the relative gas velocity and the actual blade chord. The Reynolds number is defined as $\text{Re}_{2C} = (\rho_2 W_{2C}) / \mu_2$.

The model assumes that the flow does not turn in the expansion zone:

$$\alpha_1 = \alpha_o \quad (4.11-4)$$

This means that the trailing edge of the upstream cascade controls the direction of the flow as it impinges onto the leading edge of the next cascade. If the angle of attack is such that the incidence angle, $i_1 = \phi_1 - \beta_1$, is small, then the blade cascade operates near optimum design conditions.

The remaining equations for a stage consist of three steady state conservation equations for fluid momentum, energy, and mass and two equations of state. The two equations of state are given by

$$h_2^{(n+1)} = h_2^{(n)} + C_{p2}^{(n)} \times (T_2^{(n+1)} - T_2^{(n)}) \quad (4.11-5)$$

$$P_2^{(n+1)} = \rho_2^{(n+1)} R Z_2^{(n)} T_2^{(n+1)} \quad (4.11-6)$$

Conservation of mass, energy, and momentum at steady state are given by:

$$\dot{m} = \rho_2^{(n+1)} V_2^{(n+1)} A_2 \cos \alpha_2^{(n)} \quad (4.11-7)$$

$$\dot{m} \hat{h}_1 = \dot{m} \left(h_2^{(n+1)} + \frac{\bar{\alpha}_3}{2} (V_2^{(n+1)})^2 \right) + \dot{Q}_{loss} - \dot{W}_T^{disk} \quad (4.11-8)$$

$$\hat{P}_1 - P_2^{(n+1)} = (1 + Y) \times \frac{\bar{\alpha}_3}{2} \rho_2^{(n+1)} (V_2^{(n+1)})^2 \quad (4.11-9)$$

where $\bar{\alpha}_3$ is the velocity profile correction factor. $\bar{\alpha}_3 = 1.056$ for turbulent flow. \dot{m} is the mass flow rate (not the mass storage rate). The superscripts, n and $n+1$, indicate the current and next iteration values.

The system of equations in (4.11-5) through (4.11-9) form an algebraic system for $V_2^{(n+1)}$, $\rho_2^{(n+1)}$, $P_2^{(n+1)}$, $T_2^{(n+1)}$, and $h_2^{(n+1)}$. The system is solved by first forming an inner iteration loop holding the Q_{loss} , \dot{W}_T^{disk} , and Y constant. The absolute gas flow angle at the trailing edge is given by

$$\alpha_2^{(n)} = \phi_2^{(n)} , \quad (4.11-10)$$

and is also held constant in the inner loop solution.

By substitutions of (4.11-5) through (4.11-8) into (4.11-9), the system reduces to a quadratic equation for V_2 .

$$a(V_2)^2 + b(V_2) + c = 0 \quad , \quad (4.11-11)$$

where

$$a = \frac{\bar{\alpha}_3}{2} \left(\frac{\dot{m}}{A_2 \cos \alpha_2^{(n)}} \right) \times \left(1 + Y - \frac{RZ_2^{(n)}}{C_{p2}^{(n)}} \right) \quad , \quad (4.11-12)$$

$$b = -\hat{P}_1 \quad , \quad (4.11-13)$$

$$c = \left(\frac{\dot{m}}{A_2 \cos \alpha_2^{(n)}} \right) \times RZ_2^{(n)} \times T_{ref} \quad , \quad (4.11-14)$$

$$T_{ref} = T_2^{(n)} + \frac{1}{C_{p2}^{(n)}} \left(\hat{h}_1 - h_2^{(n)} - \frac{Q_{loss} - \dot{W}_T^{disk}}{\dot{m}} \right) \quad . \quad (4.11-15)$$

The quadratic formula using the negative choice of sign for the radical gives the new value for the velocity component

$$V_2^{(n+1)} = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad . \quad (4.11-16)$$

The values of ρ_2^{n+1} , P_2^{n+1} , T_2^{n+1} , and h_2^{n+1} for the new iteration are obtained by back substitution. After each solution, the values of ϕ_2 , Q_{loss} , \dot{W}_T^{disk} , and Y are updated using the system of equations presented in

(4.11-1) through (4.11-3). The iteration continues until the updated values are within a specified tolerance of the previous iteration.

The same technique applies to the stator and rotor leading edges, where subscripts {1} and {2} are replaced with subscripts {0} and {1}, and the loss coefficient $Y = 0$ in the isentropic expansion zones. For the rotor leading edge {1}, the relative flow velocities and the incidence angle are calculated using the velocity triangle Fig. 39 once the absolute gas flow velocity V_1 is obtained, as:

$$W_{1x} = V_{1x} = V_1 \cos \alpha_1 \quad , \quad (4.11-17)$$

$$W_{1\theta} = V_{1\theta} - U_1 = V_1 \sin \alpha_1 - U_1 \quad , \quad (4.11-18)$$

$$W_1^2 = W_{1x}^2 + W_{1\theta}^2 \quad , \quad (4.11-19)$$

$$\tan \phi_1 = \frac{W_{1\theta}}{W_{1x}} \quad , \quad (4.11-20)$$

$$i_1 = \phi_1 - \beta_1 \quad . \quad (4.11-21)$$

The sign convention for tangential velocity is positive in the direction of the impeller velocity (Fig. 39).

The technique for the rotor cascade⁴³ is somewhat different due to the interdependence between mechanical work, losses, absolute gas flow angle, and flow velocity. Again, all flow conditions are assumed known at station {1}, and the relative gas flow angle at the trailing edge,

$$\phi_2^{(n)} = \beta_2 + \delta_2^{(n)} \quad , \quad (4.11-22)$$

is known from (4.11-2) and (4.11-3). The technique uses the state equations (4.11-5) and (4.11-6). The solution method first writes equations for all quantities in terms of the unknown relative velocity $W_2^{(n+1)}$.

The value of $W_2^{(n+1)}$ which satisfies the momentum balance equation is found by a bisection search method. In the bisection, the Y factor and gas flow angles are updated at each bisection trial.

For a given trial value W_2 , the absolute gas velocity at the trailing edge is obtained from the velocity triangle (Fig. 39) as:

$$V_2 = \left(W_2^2 - 2U_2 W_2 \sin \phi_2 + U_2^2 \right)^{1/2} \quad , \quad (4.11-23)$$

and the absolute gas flow angle at the trailing edge is calculated as:

$$\tan \alpha_2 = \frac{\sin \phi_2 - U_2 / W_2}{\cos \phi_2} \quad . \quad (4.11-24)$$

The gas density is obtained from the conservation of mass, as:

$$\rho_2 = \frac{\dot{m}}{A_2 V_2 \cos \alpha_2} \quad . \quad (4.11-25)$$

The cascade shaft work is given by Euler's equation:

$$\dot{W}_T = \dot{m} \times (U_1 V_{10} + U_2 V_2 \sin \alpha_2) \quad . \quad (4.11-26)$$

The gas temperature is obtained from the energy balance equation as:

$$T_2 = T_{ref} - \left(\frac{\bar{\alpha}_3}{2} V_2^2 + \frac{\dot{W}_T}{\dot{m}} \right) / C_{p2}^{(n)} \quad , \quad (4.11-27)$$

where

$$T_{ref} = T_2^{(n)} + \left(\hat{h}_1 - h_2^{(n)} - \frac{Q_{loss} - \dot{W}_T^{disk}}{\dot{m}} \right) / C_{p2}^{(n)} \quad . \quad (4.11-28)$$

The gas pressure is calculated using the ideal gas equation (4.11-6):

$$P_2 = \rho_2 R Z_2^{(n)} T_2 \quad . \quad (4.11-29)$$

Finally, the function $F_2^T(\phi_2, W_2)$ is defined based on the momentum balance equation with the proper definition of the pressure loss factor for a rotor cascade^{45, 46} :

$$F_2^T(\phi_2, W_2) = P_2 + \frac{\bar{\alpha}_3}{2} \rho_2 \times (1 + Y) W_2^2 - P_1 - \frac{\bar{\alpha}_3}{2} \rho_1 \times W_1^2 \quad . \quad (4.11-30)$$

The function F_2^T is a monotonically decreasing function of W_2 and is equal to zero when the momentum balance equation is satisfied. The parameter, $\bar{\alpha}_3$, is the velocity profile correction factor which is $\bar{\alpha}_3 = 1.056$ for turbulent flow. The solution technique finds the zero of this function by performing a bisection search on W_2 . Once the zero of F_2^T has been found, the conservation equations (4.11-25), (4.11-27) through (4.11-30), Euler equation (4.11-26), and velocity triangle relations (4.11-23) and (4.11-24) are all satisfied. Internal iterations are then performed to resolve the dependences of pressure loss factor Y , deviation angle δ_2 , heat losses Q_{loss} , and real gas enthalpy h_2 and compressibility factor Z_2 .

4.11.3 Compressor model

This section describes the compressor performance model. It is modified slightly from the steady-state model by Tournier and El-Genk⁴⁰ to account for off-design and transient conditions. The same general modeling and numerical solution approach used in the turbine model are also applied to the compressor model. The incidence loss model correlations and velocity triangle relationships are selected for compressor pressure flow conditions.

Figure 40 illustrates the basic configuration of an axial-flow compressor with three stages. Each stage consists of a cascade of stationary blades (Inlet Guide Vanes, IGV, or Stator, S), which decreases the swirl (tangential) velocity of the gas in the direction of rotation, followed by a cascade of rotating blades (Rotor, R), which imparts mechanical (or kinetic) energy to the gas by increasing the swirl velocity. The next stator row removes the swirl developed by the rotor cascade to convert kinetic energy into static pressure and to establish the proper swirl velocity for the flow to enter the next rotor stage. Both processes in the compressor contribute to increasing the gas static pressure. It is a common practice in axial-flow turbomachines to design a multistage compressor for nearly constant axial flow velocity throughout. In mirror image of the turbine design, the annular flow area of an axial compressor must decrease from inlet to outlet since the gas pressure and density increase as the gas flows through the compressor. Typically, an EGV follows the last compressor stage to remove any residual swirl velocity and convert that kinetic energy to an increase in static pressure. Although not shown on the figure, a diffuser follows the EGVs to recover as much kinetic energy as possible, as well as to direct the flow to its intended destination. Similarly, an inlet flow passage will precede the inlet guide vanes. This can range from a smooth axial bell-mouth inlet to a complex side inlet, depending on the application.

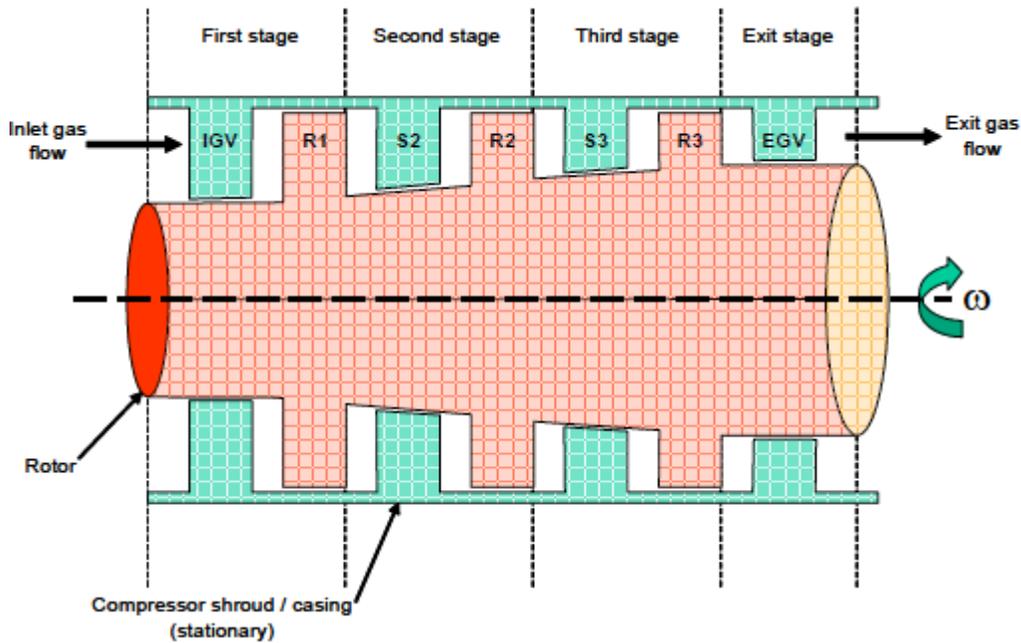


Fig. 40. Schematic of a multistage axial-flow compressor.

Typical velocity triangles at the leading and trailing edges of a compressor rotor cascade are shown in Fig. 41. An orthogonal coordinate system (x, θ) is used where the meridional coordinate, x , is identical to the axial coordinate (axis of the turbomachinery), and θ is the polar angle of a cylindrical coordinate system. Subscript 1 refers to the cascade inlet station, and subscript 2 refers to the cascade exit station. The velocity in the stationary coordinate system (absolute velocity) is designated as V , and the velocity in the rotating coordinate system (relative velocity) is designated as W (Fig. 41). Finally, U is the tangential velocity of the rotating blades ($U = U_\theta$), and α and ϕ designate the absolute and relative velocity angles, respectively.

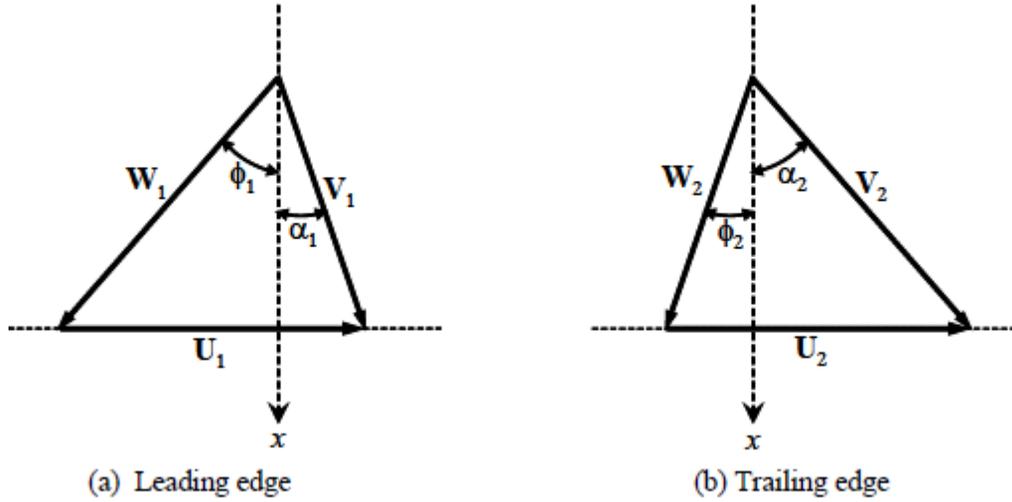


Fig. 41. Velocity triangles of compressor rotor blades.

According to the loss scheme of Koch and Smith,⁴⁷ an improvement of the model of Lieblein⁴⁸, the total pressure loss coefficient of a compressor blades cascade at optimum design conditions is the sum of the coefficients for profile losses and tip clearance (leakage) losses. Aungier⁴⁹ has introduced an off-design incidence correction factor, K_{inc} , so that the total pressure loss factor is written generally as

$$Y = K_{inc} \times (Y_p + Y_{TC}) \quad . \quad (4.11-31)$$

The method of solution for the compressor follows almost the same steps as the turbine model. The following equations are identical to the corresponding turbine equations.

$$\phi_2 = \beta_2 + \delta \quad . \quad (4.11-32)$$

Just as in the turbine model, a compressor half-stage consists of an isentropic contraction section {0-1} between two cascades, followed by a blade section⁴³ which exhibits pressure losses. The flow conditions at station {0} are assumed known, and the solution proceeds downstream to calculate the flow conditions at stations {1} and {2}. The relative gas flow angle, ϕ_2 , at the trailing edge of the blades is a function of the blade angle and the deviation angle, δ :

$$\delta = 17.3 \frac{(S/C)^{0.05} \times |\phi_1 - \beta_2|^{0.63} \times \cos^2(\Phi) \times (t_{max}/C)^{0.29}}{(30 + 0.01\beta_1^{2.07}) \times \tanh(Re_{2c}/200,000)} \quad . \quad (4.11-33)$$

All angles in this equation are expressed in degrees, and the Reynolds number at the trailing edge is based on the relative gas velocity and the actual blade chord. The Reynold's number is defined as

$$Re_{2c} = (\rho_2 W_{2c}) / \mu_2 .$$

The off-design model assumes that the flow does not turn in the expansion zone as in Ainley and Mathieson⁴², i.e.,

$$\alpha_1 = \alpha_0 \quad . \quad (4.11-34)$$

This means that the trailing edge of the upstream cascade controls the direction of the flow as it impinges onto the leading edge of the next cascade. If the angle of attack is correct, that is if the incidence angle $i_1 = \phi_1 - \beta_1 = i^*$, the blades cascade operates near optimum design conditions. An off-design angle of attack, however, will result in large incidence losses, which are then incorporated in the K_{inc} factor whose formula is defined in Appendix B.

The example of a compressor stator cascade at⁴³ is presented to illustrate the solution technique. All flow conditions are known at station {1}. The absolute gas flow angle at the trailing edge, $\alpha_2^{(n)} = \phi_2^{(n)}$ is known from (4.11-32) and (4.11-33).

Linearized equations of state for a real gas are given as follows:

$$h_2^{(n+1)} = h_2^{(n)} + C_{p2}^{(n)} \times (T_2^{(n+1)} - T_2^{(n)}) \quad , \quad (4.11-35)$$

$$P_2^{(n+1)} = \rho_2^{(n+1)} R Z_2^{(n)} T_2^{(n+1)} \quad . \quad (4.11-36)$$

The steady state conservation of mass and energy and momentum can then be written:

$$\dot{m} = \rho_2^{(n+1)} V_2^{(n+1)} A_2 \cos \alpha_2^{(n)} \quad , \quad (4.11-37)$$

$$\dot{m} \hat{h}_1 = \dot{m} \left(h_2^{(n+1)} + \frac{\bar{\alpha}_3}{2} (V_2^{(n+1)})^2 \right) + Q_{loss} - \dot{W}_C^{disk} \quad . \quad (4.11-38)$$

The turbine and compressor solution methods differ in the iteration scheme for the unrecoverable loss terms in the momentum equation. Eq. (4.11-40) uses old values (n) for density and velocity. The corresponding turbine equation for pressure loss, Eq. (4.11-9), uses the updated pressure loss ($n+1$).

$$\hat{P}_1 = P_2^{(n+1)} + \frac{\bar{\alpha}_3}{2} \rho_2^{(n+1)} (V_2^{(n+1)})^2 + \Delta \hat{P}_{loss} \quad , \quad (4.11-39)$$

where the pressure losses are given by:

$$\Delta \hat{P}_{loss} = Y \times \frac{\bar{\alpha}_3}{2} \rho_1^{(n)} (V_1^{(n)})^2 . \quad (4.11-40)$$

The modeling of the compressor's nonideal behavior is contained in the pressure loss factor, Y , whose formulas and empirical relationships are given in Appendix B.

With appropriate algebraic substitutions, the solution resolves to a quadratic in velocity.

$$a(V_2)^2 + b(V_2) + c = 0 , \quad (4.11-41)$$

where

$$\alpha = \frac{\bar{\alpha}_3}{2} \left(\frac{\dot{m}}{A_2 \cos \alpha_2^{(n)}} \right) \times \left(1 + Y - \frac{RZ_2^{(n)}}{C_{p2}^{(n)}} \right) , \quad (4.11-42)$$

$$b = -\hat{P}_2 = \Delta \hat{P}_{loss} - \hat{P}_1 , \quad (4.11-43)$$

$$c = \left(\frac{\dot{m}}{A_2 \cos \alpha_2^{(n)}} \right) \times RZ_2^{(n)} \times T_{ref} , \quad (4.11-44)$$

$$T_{ref} = T_2^{(n)} + \frac{1}{C_{p2}^{(n)}} \left(\hat{h}_1 - h_2^{(n)} - \frac{Q_{loss} - \dot{W}_C^{disk}}{\dot{m}} \right) . \quad (4.11-45)$$

The solution of the quadratic equation is the same as the turbine.

$$V_2^{(n+1)} = \frac{-b - \sqrt{b^2 - 4ac}}{2a} . \quad (4.11-46)$$

In practice, numerical iterations are required, since the heat losses, Q_{loss} , pressure loss coefficient, Y , and gas properties are also functions of the flow conditions at the trailing edge, which are not known a priori.

The same numerical solution technique is applied to the stator and rotor leading edges, where subscripts {1} and {2} are replaced with subscripts {0} and {1}, and the loss coefficient $Y = 0$ in the isentropic contraction zones. For the rotor leading edge {1}, the relative flow velocities and the incidence angle are easily calculated using the velocity triangle (Fig. 41) once the absolute gas flow velocity V_1 is obtained, as:

$$W_{1x} - V_{1x} = V_1 \cos \alpha_1 \quad , \quad (4.11-47)$$

$$W_{1\theta} = V_{1\theta} - U_1 = V_1 \sin \alpha_1 - U_1 \quad , \quad (4.11-48)$$

$$W_1^2 = W_{1x}^2 + W_{1\theta}^2 \quad , \quad (4.11-49)$$

$$\tan \phi_1 = -\frac{W_{1\theta}}{W_{1x}} \quad , \quad (4.11-50)$$

$$i_1 = \phi_1 - \beta_1 \quad . \quad (4.11-51)$$

The sign convention for tangential velocity is positive in the direction of the impeller velocity (Fig. 41).

The technique for the rotor cascade ⁴³ is somewhat different from the stator due to the interdependence between mechanical work, losses, absolute gas flow angle, and velocity triangle. All flow conditions at station { 1 } are known, and the relative gas flow angle at the trailing edge $\phi_2^{(n)} = \beta_2 + \delta_2^{(n)}$, is known. For a given trial value W_2 , the absolute gas velocity at the trailing edge is obtained from the velocity triangle (Fig. 41) as:

$$V_2 = \left(W_2^2 - 2U_2 W_2 \sin \phi_2 + U_2^2 \right)^{1/2} \quad , \quad (4.11-52)$$

and the absolute gas flow angle at the trailing edge is calculated as:

$$\tan \alpha_2 = \frac{U_2 / W_2 - \sin \phi_2}{\cos \phi_2} \quad . \quad (4.11-53)$$

The gas density is obtained from the conservation of mass, as:

$$\rho_2 = \frac{\dot{m}}{A_2 V_2 \cos \alpha_2} \quad , \quad (4.11-54)$$

and the cascade shaft work is given by Euler's equation:

$$\dot{W}_c = \dot{m} \times (U_1 V_{1\theta} - U_2 V_2 \sin \alpha_2) < 0 . \quad (4.11-55)$$

The gas temperature is obtained from the energy balance equation as:

$$T_2 = T_{ref} - \left(\frac{\bar{\alpha}_3}{2} V_2^2 + \frac{\dot{W}_c}{\dot{m}} \right) / C_{p2}^{(n)} , \quad (4.11-56)$$

where

$$T_{ref} = T_2^{(n)} + \frac{1}{C_{p2}^{(n)}} \left(\hat{h}_1 - h_2^{(n)} - \frac{Q_{loss} - \dot{W}_c^{disk}}{\dot{m}} \right) . \quad (4.11-57)$$

The gas pressure is calculated using the state Eq. (4.11-36) as:

$$P_2 = \rho_2 R Z_2^{(n)} T_2 . \quad (4.11-58)$$

Finally, the function $F_2^C(\phi_2, W_2)$ is calculated, using the fluid momentum balance equation with the proper definition of the pressure loss factor for a rotor cascade from Appendix B. The intercept function is defined slightly differently for the compressor compared to the turbine, but the solution method is the same. The function is solved by bisection search on the variable W_2 for the zero intercept of F_2^C .

$$F_2^C(\phi_2, W_2) = P_2 + \frac{\bar{\alpha}_3}{2} \rho_2 \times W_2^2 - P_1 + \frac{\bar{\alpha}_3}{2} \rho_1 \times (Y - 1) \times W_1^2 . \quad (4.11-59)$$

The function F_2^C is a monotonically decreasing function of W_2 , and is equal to zero when the momentum balance equation is satisfied. Once the zero of F_2^C has been found, the conservation Eqs. (4.11-54), (4.11-56), (4.11-57), and (4.11-59); Euler Eq. (4.11-55); and velocity triangle relations Eqs. (4.11-52) and (4.11-53) are all satisfied. Internal iterations are then performed to resolve the dependences of pressure loss factor Y , deviation angle δ , heat losses Q_{loss} , real gas enthalpy, h_2 and compressibility factor, Z_2 .

4.11.4 Transient model of a general purpose heat exchanger.

MELCOR-H2 requires the development and implementation of a number of heat exchanger models (i.e., gas/gas IHX, gas/gas recuperator, and gas/liquid pre-cooler and inter-coolers). These heat exchangers may have different configurations and geometries, such as shell-and-tube heat exchangers, gasketed-plate heat

exchangers, Lamella (or Ramen) heat exchangers, and extended-surface heat exchangers such as plate-fin and tubular-fin heat exchangers.⁵⁰ The heat transfer calculation between generic fluid and heat slab modules lacks the heat transfer coefficients for modeling these configurations. The main enhancement to MELCOR provided by the general purpose heat exchanger is the addition of correlations for various enhanced heat transfer due to the extended surfaces.

To accommodate the different heat exchanger configurations of interest, a generic, transient, and multinode heat exchanger model is developed to simulate single-phase, parallel, and/or countercurrent flow arrangements. This model is not appropriate for steam generators because two phase flow is not treated. The generic heat exchanger model is applied to any particular heat exchanger configuration by selecting appropriate flow path lengths, cross-sectional flow areas, equivalent diameters, and heat transfer areas of the cold- and hot-leg channels. The transient generic heat exchanger model developed in this work for incorporation into MELCOR-H2 is described briefly below. More details on the constitutive governing equations of the problem and the numerical technique used to solve them can be found in Tournier and El- Genk⁴⁰.

The MELCOR-H2 heat exchanger model currently incorporates two different working fluids, helium gas and liquid water, and one structural material, stainless steel 304/316. Additional working fluids and structural materials can easily be incorporated into the general framework of the code. The model uses partial derivatives of the density and internal energy with respect to temperature and pressure in a general formulation so that it can handle nonperfect gases and other highly compressible fluids as well.

The general layout and cell numbering scheme of the heat exchanger is shown in Fig. 42. The governing equations and boundary conditions are discretized on a staggered grid using the control volume integration approach. The coolant in the hot leg, represented by a string of cells ($i = 2$), is separated from the coolant in the cold leg (string $i = 4$) by a solid, heat transfer wall (string $i = 3$). The model uses two additional strings of solid cells ($i = 1$ and $i = 5$), thermally insulated on the far side, to account for the thermal mass of the structure of the heat exchanger. The physical domain is divided into a two-dimensional grid of 5 by Nz cells, on a staggered grid. In the axial direction, each flow channel is divided into Nz numerical cells of identical size ΔZ , and extends from ($j = 1$) to ($j = Nz$). The surface areas of the sides of cell (i,j) are $A_r^{i,j}$, $A_r^{i-1,j}$, A_z^i , $A_r^{i,j}$, $A_r^{i-1,j}$, and A_z^i in the transverse and axial directions, respectively (Fig. 42). The volume of the mass cell (i,j) is $VOL^{i,j}$. The term “cell” refers to the fluid control volume on which mass and energy balance are formulated. On the staggered grid, the fluid density, ρ , pressure, P , temperature, T , and the internal energy, e , are defined at the center of the control volume cells, while the velocity, V_z , and mass flux, G_z , are defined at the center of the faces of these cells (Fig. 42).

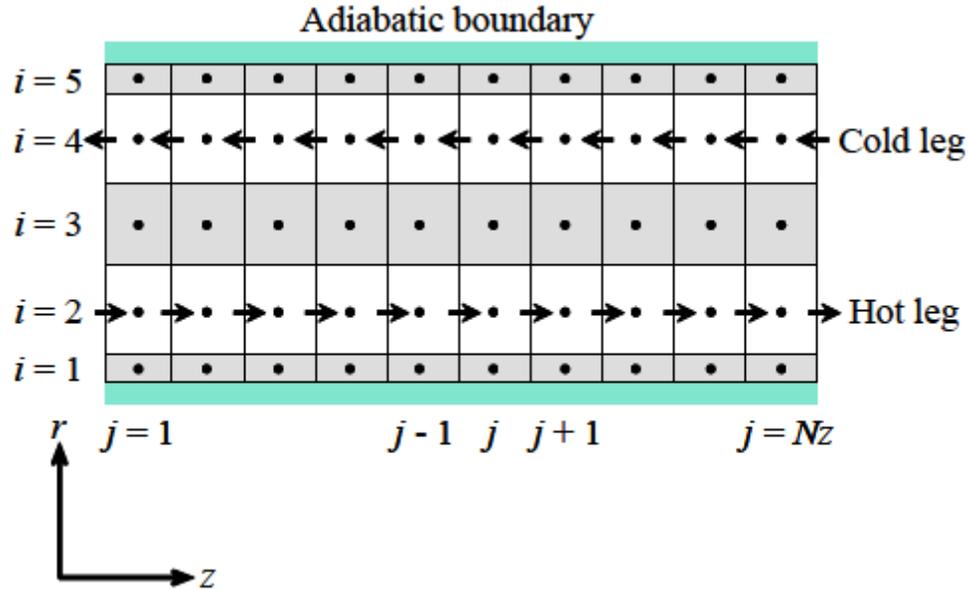


Fig. 42. Cell and flow path schematic for heat exchanger.

The coolant in the hot leg ($i = 2$) enters the heat exchanger at interface ($j = 0$), and exits at interface ($j = Nz$). Therefore, the velocities, $V_z(2,j)$, and mass fluxes, $G_z(2,j)$, are positive. In the case of a parallel flow arrangement, the coolant in the cold leg ($i = 4$) also enters the heat exchanger at interface ($j = 0$) and exits at interface ($j = Nz$). For a counter-current flow arrangement, the coolant in the cold leg ($i = 4$) enters the heat exchanger at interface ($j = Nz$) and exits at interface ($j = 0$). In this case, the velocities, $V_z(4,j)$, and mass fluxes, $G_z(4,j)$, are negative.

At time zero (initial conditions), the model assumes a uniform temperature distribution; that is, all coolant and structural nodal temperatures are initialized at the same value. Furthermore, the pressure and mass flow rate in each coolant leg are assumed uniform at time zero. However, different values of the initial pressure and flow rate can be used for the primary and secondary sides of the heat exchanger.

The boundary conditions used in the model are the following. The hot and cold side walls of the heat exchanger are assumed adiabatic (thermally insulated). The coolant temperature, pressure, and mass flow rate at the entrance of both the hot and cold legs of the heat exchanger model are time-dependent values supplied by other MELCOR-H2 control volumes or boundary conditions.

Given these initial and boundary conditions, the MELCOR-H2 model calculates the nodal temperatures, pressures, and mass fluxes in the heat exchanger as functions of time. The model returns the values for coolant temperatures, pressures, and mass flow rates at the exit of the hot and cold legs to MELCOR-H2.

4.11.4.1 Heat exchanger numerical solution

The SIMPLE-Consistent (SIMPLEC) numerical approach is used in MELCOR-H2 to solve the model on the secondary and primary sides and structural walls of the heat exchanger. SIMPLE-C is a staggered-grid, segregated solution technique by van Doormaal and Raithby⁵¹ which includes two internal iterative steps to resolve the pressure-velocity and temperature-velocity couplings and reduce the linearization errors of the equations of state. Such a discretization method requires much less computational time and storage than finite-element methods. The SIMPLE-C integration approach is, in fact, simple to implement, and the finite-difference forms have a physical interpretation as integrals of the conservation

laws over the control volume cell which leads to a consistent method of approximation for all conservation laws. The solution thus obtained satisfies global conservation even on a nonuniform grid.

The SIMPLE-C algorithm uses a consistent simplification of the momentum correction equations and does not require any pressure under-relaxation (the off-diagonal velocity corrections appearing in the diffusion-convection fluxes are equated to the diagonal velocity correction). The basic iteration procedure follows these steps:

- a. *Energy predictor step*: best estimates of pressures and convective fluxes are used explicitly, and the energy conservation equations are solved for the temperatures, in the coolant channels, and structural walls simultaneously.
- b. *Properties update*: transport properties (conductivities and viscosities) are updated.
- c. *Pressure corrector step*: the simplified (corrected) form of the axial momentum.
- d. Conservation equations are used to relate implicitly the mass fluxes and pressure gradients. The mass fluxes are then eliminated in terms of pressures in the mass balance (continuity) equations, and densities are linearized using the equations of state. The resulting elliptical Poisson equations are solved for the pressure field, which is updated.
- e. *Momentum predictor step*: best estimates of the pressure gradients are calculated explicitly, and the axial momentum conservation equations are solved for the velocity field.
- f. *Properties update*: the coolant (gas and/or liquid) densities are updated.
- g. Iterations to (c) are performed until velocities and pressures converge (that is, until pressure corrections are below a prescribed value).
- h. Iterations to (a) are performed until temperatures converge (that is, until temperature corrections are below a prescribed value).

4.11.4.2 Nusselt number and friction factor correlations

The main phenomenon to model in the heat exchanger is the heat transfer and the pressure drop. The modeling approach in MELCOR-H2 is to incorporate appropriate engineering correlations into the model such that the user input to the components is just the parameters for the physical geometry of the component. These built-in correlations allow the code to be used for engineering design and thermal cycle studies. The code does not rely on normalization of the heat transfer or pressure drop to experimental data or to calculations from a detailed steady state thermal design code for an accurate simulation of the heat transfer or pressure losses in the process. The modeling development has identified and evaluated correlations for heat transfer and friction in the open literature. Selections of correlations have been made by the MELCOR-H2 developers for the conditions in the NGNP.

The Nusselt number is a dimensionless quantity representing a temperature gradient at a surface. It is equal to

$$Nu = hD_{eq} / k , \quad (4.11-60)$$

where h is the surface heat conduction coefficient, D_{eq} is the hydraulic diameter, and k is the fluid conductivity. The Nusselt number is the conventional parameter for correlating the heat transfer capability at a surface with fluid and flow conditions. The Nusselt number for a fully developed laminar flow in a circular coolant channel with a constant heat flux boundary condition, and assuming constant fluid properties, is given by Kakaç and Lui:⁵⁰

$$Nu_1 = 4.36, \quad \text{when } Pe_b D_{eq} / L < 10, \quad (4.11-61)$$

$$Nu_2 = 1.953 \times \left(\frac{Pe_b D_{eq}}{L} \right)^{1/3}, \quad \text{when } Pe_b D_{eq} / L > 100, \quad (4.11-62)$$

where the fluid properties are evaluated at the coolant bulk temperature.

The two Nusselt number formulae may be joined smoothly as proposed by Schlunder by the following asymptotic cubic relationship. Figure 43 shows that the formula gives a smooth transition:

$$\begin{aligned} Nu_o &= \left[Nu_1^3 + Nu_2^3 \right]^{1/3} \\ &= \left[(4.36)^3 + (1.953)^3 \times \left(\frac{Pe_b D_{eq}}{L} \right)^3 \right]^{1/3}. \end{aligned} \quad (4.11-63)$$

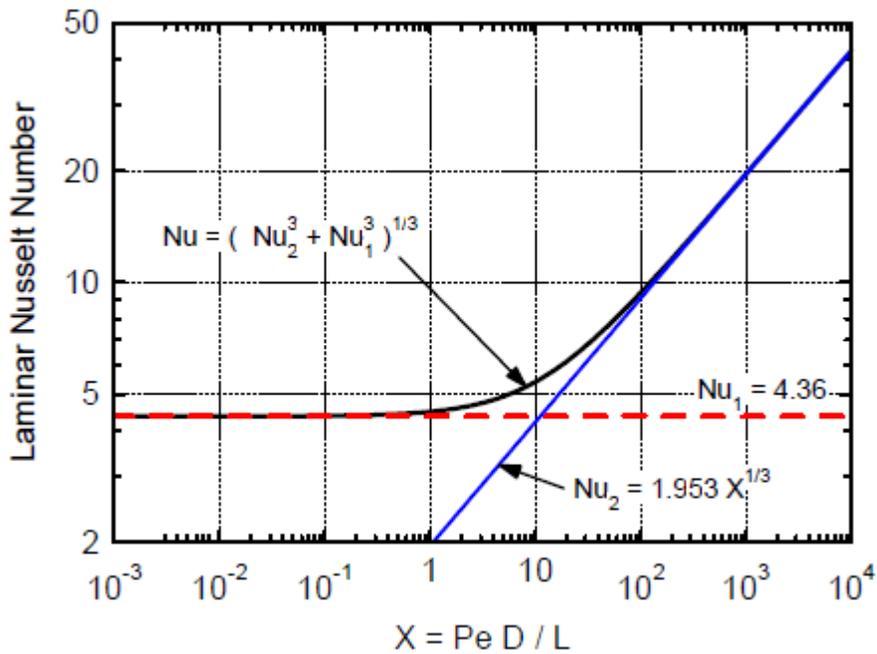


Fig. 43. Laminar Nusselt number for constant heat flux boundary condition.

When the previous correlation is applied to practical heat transfer cases with large temperature differences between the wall and the coolant, the variation of fluid properties with temperature influences the velocity and temperature profiles through the boundary layer and the cross-sectional flow area of the channel.

Correction factors are applied to account for such effects. For the laminar flow of liquids, the Nusselt number of Eq. (4.11-63) is corrected as suggested by Kakaç and Lui⁵⁰:

$$Nu = Nu_o \times \left(\frac{\mu_b}{\mu_w} \right)^{0.14} . \quad (4.11-64)$$

No correction is necessary for the laminar flow of gases.

For the case of turbulent flow in smooth circular tubes, assuming constant properties and a constant heat flux boundary condition, Pethukov and Popov's theoretical calculations based on the three-layer turbulent boundary layer model, with constants adjusted to match a wide variety of experimental data, yields the following relation^{50, 52}:

$$Nu_o = \frac{(f_o / 8) Re_b Pr_b}{1.07 + 12.7 \times (f_o / 8)^{1/2} (Pr_b^{2/3} - 1)} , \quad (4.11-65)$$

where $f_o = (0.79 \times \ln Re_b - 1.64)^{-2}$. The parameter, f_o , is Flonenko's formula for the Darcy friction factor. This correlation predicts the experimental data of gases and liquids with an error <6% in the ranges $10^4 < Re_b < 5 \times 10^6$ and $0.6 < Pr_b < 200$. Gnielinski⁵³ further modified Petukov's correlation so that it covered experimental data in the transition flow region as well, i.e., $2300 < Re_b < 10^4$:

$$Nu_o = \frac{(f_o / 8)(Re_b - 1000) Pr_b}{1 + 12.7 \times (f_o / 8)^{1/2} (Pr_b^{2/3} - 1)} . \quad (4.11-66)$$

Gnielinski's correlation predicts the experimental data of gases (such as air and helium) and liquids (such as water, oil, and glycerin) with an error <6% in the ranges $2300 < Re_b < 5 \times 10^6$ and $0.5 < Pr_b < 200$. This successful and more general correlation is used in the MELCOR-H2 model of a generic heat exchanger.

The effect of thermal boundary conditions is almost negligible in turbulent forced convection. Therefore, Eq. (4.11-66) can be used for both constant wall temperature and constant wall heat flux boundary conditions. For turbulent flow in noncircular channels, the practice of using the hydraulic diameter of the channel in place of the inner tube diameter leads to predicted Nusselt numbers that are within +10% of the experimental data, except for some sharp-cornered channels.⁵⁰ This accuracy is adequate for the overall heat transfer coefficient (and the pressure drop calculations) in most of the practical heat exchanger designs.

To account for nonconstant properties, the turbulent Nusselt number Eq. (4.11-66) is corrected as follows.^{50, 52} For the turbulent flow of liquids:

$$Nu = Nu_o \times \left(\frac{\mu_b}{\mu_w} \right)^n . \quad (4.11-67)$$

The exponent $n = 0.11$ when the liquid is heated ($\mu_w > \mu_b$), and $n = 0.25$ when the liquid is cooled ($\mu_w < \mu_b$). For the turbulent flow of gases:

$$Nu = Nu_o \times \left(\frac{T_b}{T_w} \right)^m . \quad (4.11-68)$$

The exponent $m = 0.47$ when the gas is heated ($T_w > T_b$), and $m = 0.36$ when the gas is cooled ($T_w < T_b$).

The Darcy friction coefficient for smooth channels is shown in Fig. 44 below.

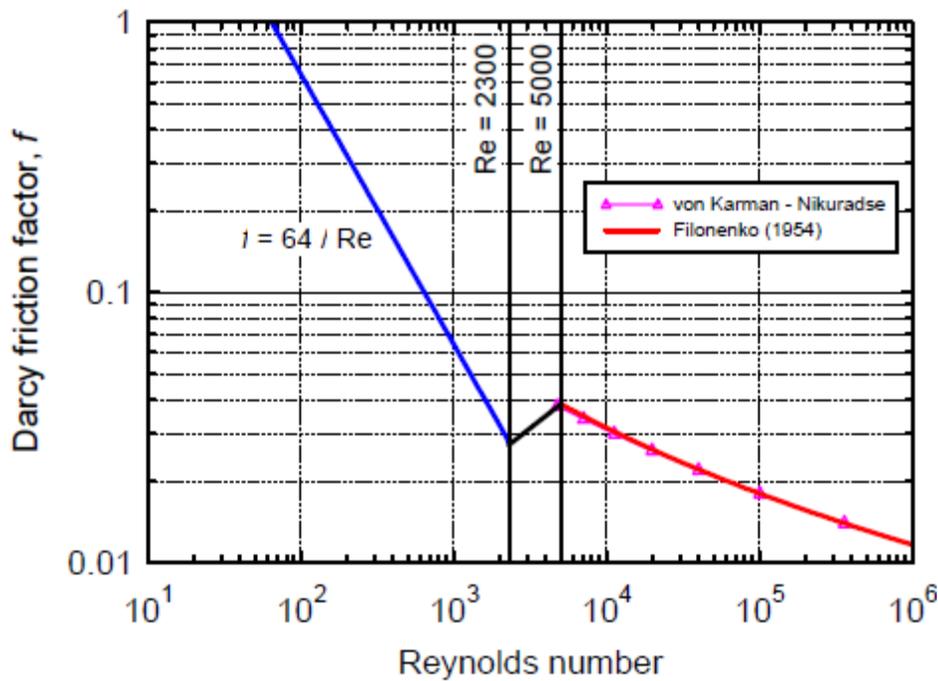


Fig. 44. Darcy friction factor for smooth surfaces.

For a fully developed flow in the turbulent regime, the approximation developed by Filonenko is within 2% error^{50,52} (see red line in Fig. 44 above) and gives an explicit expression for f_o :

$$f_o = (0.79 \times \ln Re_b - 1.64)^{-2} . \quad (4.11-69)$$

For the case of laminar flow in smooth tubes and channels of triangular and trapezoidal cross-sections, the Darcy friction factor is given by:

$$f_o = \frac{64}{\text{Re}_b} . \quad (4.11-70)$$

A linear interpolation is used in the transition region, when $2300 < \text{Re}_b < 5000$ as shown in (see black line in Fig. 44 above).

To account for nonconstant properties from wall to bulk fluid temperature, the friction factor Eq. (4.11-69) is corrected as follows.^{50, 52} For the laminar flow of liquids:

$$f = f_o \times \left(\frac{\mu_b}{\mu_w} \right)^n . \quad (4.11-71)$$

The exponent $n = -0.58$ when the liquid is heated ($\mu_w < \mu_b$), and $n = -0.50$ when the liquid is cooled ($\mu_w > \mu_b$).

For the laminar flow of gases:

$$f = f_o \times \left(\frac{T_b}{T_w} \right)^m . \quad (4.11-72)$$

The exponent $m = -1.0$ when the gas is heated ($T_w > T_b$), and $m = -0.81$ when the gas is cooled ($T_w < T_b$).

For the turbulent flow of liquids that are heated:

$$f = \frac{f_o}{6} \times \left(7 - \frac{\mu_b}{\mu_w} \right) . \quad (4.11-73)$$

For the turbulent flow of liquids that are cooled:

$$f = f_o \times \left(\frac{\mu_b}{\mu_w} \right)^{-0.24} . \quad (4.11-74)$$

For the turbulent flow of gases:

$$f = f_o \times \left(\frac{T_b}{T_w} \right)^m . \quad (4.11-75)$$

The exponent $m = 0.52$ when the gas is heated ($T_w < T_b$), and $m = 0.38$ when the gas is cooled ($T_w > T_b$).

Due to the poor heat transfer characteristics of gases, most heat exchanger designs use extended surfaces (i.e., finned heat transfer surface areas). The heat transfer of extended surfaces is represented in the MELCOR-H2 generic heat exchanger model. In each axial section $\{j\}$, the thermal heat flow between the coolant and the wall is given by:

$$Q_1 = h_j^{CV} (S_{um} + \eta_{fin} S_{fin})_j \times (T_b - T_w)_j . \quad (4.11-76)$$

Where S_{um} is the unfinned heat transfer area, S_{fin} is the finned surface area between coolant and wall, and η_{fin} is the fin's efficiency.⁵⁰ The most common fins are rectangular fins of constant thickness δ_{fin} . For the case of symmetric fins, whose ends are both in contact with the wall, encountered in stacked matrices, for example, the fin efficiency is given by:

$$\eta_{fin} = \frac{\tanh(\alpha)}{\alpha}, \quad \text{where } \alpha = L_{fin} \left(\frac{h^{CV}}{2\lambda_{fin}\delta_{fin}} \right)^{1/2} . \quad (4.11-77)$$

For the case of fins with an adiabatic tip, as in the case of longitudinal fins attached to the outside wall of a tube, for example, the fin efficiency is given by:

$$\eta_{fin} = \frac{\tanh(\alpha)}{\alpha}, \quad \text{where } \alpha = L_{fin} \left(\frac{2h^{CV}}{\lambda_{fin}\delta_{fin}} \right)^{1/2} . \quad (4.11-78)$$

The average fin temperature can then be calculated using:

$$\bar{T}_{fin} = T_b + \eta_{fin} \times (T_w - T_b) . \quad (4.11-79)$$

4.11.5 Hydrogen production modeling

The chemical processes that are used to produce diatomic hydrogen and oxygen from water depend on a series of endothermic chemical reactions that are driven by the nuclear heat from the gas-cooled reactor and/or by electrolysis processes using electrical energy from power plant's electrical generator. Several potential schemes are available. Two of the most promising based on the energy efficiency of the conversion and the availability of the raw materials are based on the SI process.

The two processes modeled by MELCOR-H2³⁸ are (1) the strictly thermochemical SI process and (2) the electrochemical HyS process. Modeling of other hydrogen production processes, such as the Adiabatic UT-3 cycle, is not supported in MELCOR-H2. The developer of the code package—SNL—indicates that these models will be incorporated into MELCOR in future releases. MELCOR-H2 provides a simplified model of the chemical reactions in the SI process that is suitable for modeling system interactions between the chemical plant and the nuclear reactor.

4.11.5.1 SI model

SI chemistry model of MELCOR-H2 involves three major chemical reactions: (1) decomposition of sulfuric acid (H_2SO_4), (2) decomposition of hydrogen iodide (HI), and (3) the Bunsen reaction, which is the low-temperature reconstitution of the two acids.

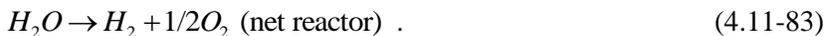
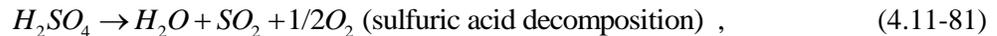
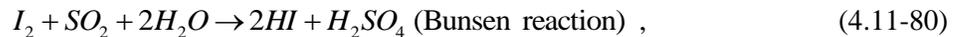


Figure 45 presents the chemical process schematic for the SI cycle plant. Equation (4.11-80) is called the Bunsen reaction and proceeds in liquid phase in Section I of the process cycle. This reaction produces two kinds of acid, sulfuric acid (H_2SO_4) and hydriodic acid [hydrogen iodide (HI) in water] from sulfur dioxide (SO_2), iodine (I_2), and water (H_2O). The mixed acid separates into two types of acid of its own accord (liquid-liquid separation). The acid, which is rich in HI, is HI_x phase (HI_x solution), while the acid, which is rich in H_2SO_4 , is the sulfuric acid phase. After separation of the acids, they are purified, concentrated, and decomposed in the other two reactions. Equation (4.11-81) is the sulfuric acid decomposition reaction that produces oxygen, sulfur dioxide, and water in Section II of the process. Equation (4.11-82) is the HI decomposition reaction that produces hydrogen and iodine and occurs in Section III. With the exception of hydrogen and oxygen, the other products in Eqs. (4.11-81) and (4.11-82) can be reused in the Bunsen reaction step as the reactant material. The endothermic H_2SO_4 decomposition reaction can be operated at about 800–1000°C. The decomposition of hydriodic acid involves an endothermic reaction around 400–500°C. The Bunsen reaction occurs exothermically at about 100°C. The heat source for the two endothermic acid decomposition reactions in the SI cycle is provided

by the nuclear heat transferred by the secondary loop coolant to the heat exchangers in the Sections II and III.

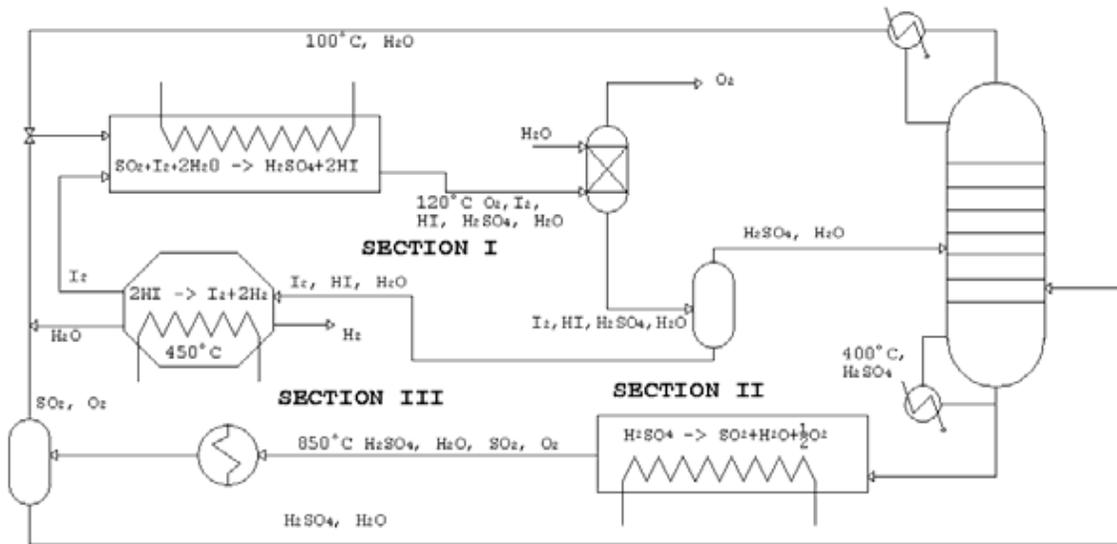


Fig. 45. Process schematic for sulfur-iodine process.³⁹

To model chemical processes, MELCOR-H2 has added a general-purpose, perfectly mixed reaction chamber. The reaction chamber is a control volume in which reactants and heat enter the chamber and products exit the chamber as shown in Fig. 46. The reaction chamber dynamic model tracks species concentrations using individual species mass balance equations and the average temperature of the chamber using an energy balance based on an isothermal mixture. The model uses one-step, effective reaction rate models to represent the chemical process rate dynamics and the ideal gas law to relate pressure and temperature to molar concentration.

Each section of the process is modeled in a single reaction chamber. Separation and mixing processes are approximated as instantaneous and perfect.

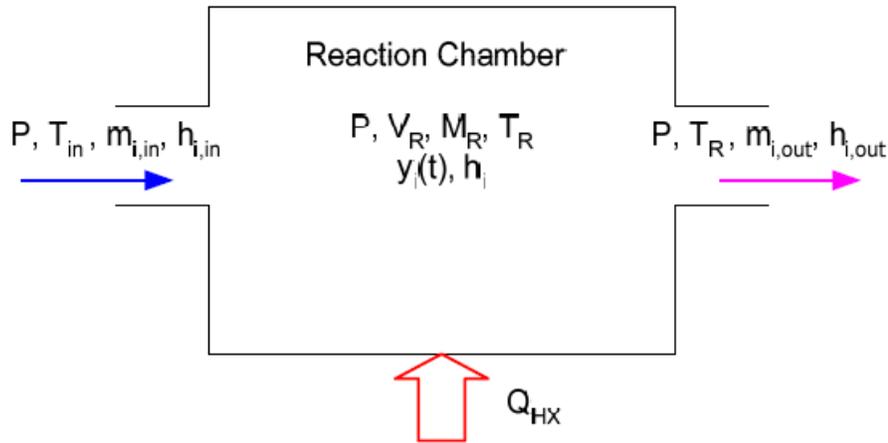


Fig. 46. Schematic of reaction chamber showing input and output variables.³⁹

The equation for modeling species concentration is derived from the general equation for conservation of mass including a term for creation or consumption of a species by chemical reaction.

$$\frac{dM_{i,R}}{dt} = m_{i,in} - m_{i,out} + \frac{dM_{i,RXN}}{dt} , \quad (4.11-84)$$

where

$M_{i,R}$ is the number of moles of species i in the reaction chamber,

$m_{i,in}$ is the molar flow rate of species i into the reaction chamber,

$m_{i,out}$ is the molar flow rate of species i out of the reaction chamber, and

$\frac{dM_{i,RXN}}{dt}$ is the molar rate of reaction of species i .

Note that the total moles in the reaction chamber and the total molar flow rates are given by summing the species variables.

$$M_R = \sum_i M_{i,R} , \quad (4.11-85)$$

$$m_{in} = \sum_i m_{i,in} , \quad (4.11-86)$$

$$m_{out} = \sum_i m_{i,out} . \quad (4.11-87)$$

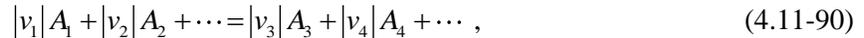
A convenient form for numerical evaluation can be obtained by a series of substitutions. First, the mass equation may be cast in terms of mole fraction, y_i by the substitution

$$y_i = \frac{M_{i,R}}{M_R} . \quad (4.11-88)$$

The perfectly mixed reactor approximation is made by setting the outlet concentration of the reactor equal to the average concentration. The simplicity of the equation masks the significance of the approximation in reaction rate dynamics.

$$y_i = \frac{m_{i,out}}{m_{out}} . \quad (4.11-89)$$

The second substitution replaces the molar rate of reaction with a single rate that is proportional to the reaction rate of all species in the reaction. The parameter is called the extent of reaction. All species involved in a single reaction are proportional according to the stoichiometry coefficients. For a balanced chemical equation of the general form



where

v_i is the signed stoichiometric coefficient for species i (positive for products, negative for reactants),

A_i is the species,

i varies from 1 to the maximum number of reactants and products.

For the reaction represented by Eq. (4.11-90), the rates of change of each of the species are proportional with proportionality constants determined by the stoichiometric coefficients. Since all the rates are algebraically related, it is convenient to set them all equal to a single variable. This variable is usually called the reaction extent, X .

$$\frac{dX}{dt} = \frac{1}{v_1} \frac{dM_{1,RXN}}{dt} = \frac{1}{v_2} \frac{dM_{2,RXN}}{dt} = \frac{1}{v_3} \frac{dM_{3,RXN}}{dt} = \frac{1}{v_4} \frac{dM_{4,RXN}}{dt} = \dots . \quad (4.11-91)$$

Hence, the reaction rates in the species mass equations in the reaction chamber are all replaced by the extent of reaction rate.

$$\frac{dM_{i,RXN}}{dt} = v_i \frac{dX}{dt} . \quad (4.11-92)$$

Making the substitutions into the species mass equation Eq. (4.11-84) indicated by Eqs. (4.11-88), (4.11-89), and (4.11-92) yields the following form for the mass equation.

$$\frac{dy_i M_R}{dt} = m_{i,in} - m_{i,out} + v_i \frac{dX}{dt} . \quad (4.11-93)$$

Summing all the species equations gives

$$\frac{dM_R}{dt} = m_{in} - m_{out} + \Delta v \frac{dX}{dt} , \quad (4.11-94)$$

where

$$\Delta v = \sum_i v_i . \quad (4.11-95)$$

The total moles and the outlet molar flow rate can be eliminated by multiplying Eq. (4.11-94) by y_i and subtracting the result from Eq. (4.11-93).

$$M_R \frac{dy_i}{dt} + y_i \left(m_{in} + \Delta v \frac{dX}{dt} \right) = m_{i,in} + v_i \frac{dX}{dt} . \quad (4.11-96)$$

The terms in the species mass equation are determined with the addition of an equation for rate of the extent of reaction. Because that rate depends on temperature, that reaction rate equation is deferred until the temperature equation is obtained from the conservation of energy equation.

The general conservation of energy is given by the following

$$\frac{dH}{dt} = \sum_i (m_{i,in} h_{i,in}) - \sum_i (m_{i,out} h_{i,out}) + \dot{Q}_{HX} + V_R \frac{dP}{dt} , \quad (4.11-97)$$

where

H is the total enthalpy (including chemical energy) in the control volume.

$h_{i,in}$ is the enthalpy (including chemical energy) of species i entering the reaction chamber,

$h_{i,out}$ is the enthalpy (including chemical energy) of species i leaving the reaction chamber, and

P is the pressure in the reaction chamber.

The total enthalpy on the left hand side of Eq. (4.11-97) can be expanded in terms of the species enthalpy, molar fractions, and total moles

$$\frac{dH}{dt} = \frac{dM_R}{dt} \sum_i y_i h_i + M_R \sum_i h_i \frac{dy_i}{dt} + M_R \sum_i y_i \frac{dh_i}{dt} . \quad (4.11-98)$$

The perfect mixing approximation applied to energy implies that

$$h_{i,out} = h_i , \quad (4.11-99)$$

Substituting Eqs. (4.11-98) and (4.11-99) into the energy Eq. (4.11-97) gives the equation in terms of the species mass fractions and enthalpies.

$$\frac{dM_R}{dt} \sum_i y_i h_i + M_R \sum_i h_i \frac{dy_i}{dt} + M_R \sum_i y_i \frac{dh_i}{dt} = \sum_i (m_{i,in} h_{i,in}) - \sum_i (m_{i,out} h_{i,out}) + \dot{Q}_{HX} + V_R \frac{dP}{dt} . \quad (4.11-100)$$

The mass equation can be used to complete the conversion to intensive form. Multiplying Eq. (4.11-93) by h_i and summing over all i gives

$$\frac{dM_R}{dt} \sum_i y_i h_i + M_R \sum_i h_i \frac{dy_i}{dt} = \sum_i m_{i,in} h_i - \sum_i m_{i,out} h_i + \frac{dX}{dt} \sum_i v_i h_i . \quad (4.11-101)$$

This equation can be subtracted from Eq. (4.11-100) to simplify the equation to the intensive form

$$M_R \sum_i y_i \frac{dh_i}{dt} = \sum_i m_{i,in} (h_{i,in} - h_i) - \frac{dX}{dt} \sum_i v_i h_i + \dot{Q}_{HX} + V_R \frac{dP}{dt} . \quad (4.11-102)$$

Assuming an isothermal reaction chamber allows the change in enthalpy to be replaced by the change in the overall average temperature times the specific heat.

$$dh_i = c_{P,i} dT_R , \quad (4.11-103)$$

where

T_R is the reaction chamber temperature

$c_{P,i}$ is the specific heat at constant pressure for species i .

Inserting the temperature relationship Eq. (4.11-103) into Eq. (4.11-102) gives

$$M_R \sum_i y_i c_{P,i} \frac{dT_R}{dt} = \sum_i m_{i,in} (h_{i,in} - h_i) - \frac{dX}{dt} \sum_i v_i h_i + \dot{Q}_{HX} + V_R \frac{dP}{dt} . \quad (4.11-104)$$

The following summation terms can be collected as a parameter for the equation

$$\Delta h_{RXN} = \sum_i v_i h_i , \quad (4.11-105)$$

$$\bar{c}_P = \sum_i y_i c_{P,i} . \quad (4.11-106)$$

The term Δh_{RXN} accounts for the energy released per mole of reaction as measured by the extent of reaction parameter. The final energy equation is given by

$$M_R \bar{c}_P \frac{dT_R}{dt} = \sum_i m_{i,in} (h_{i,in} - h_i) - \Delta h_{RXN} \frac{dX}{dt} + \dot{Q}_{HX} + V_R \frac{dP}{dt} . \quad (4.11-107)$$

The heat exchanger in the reaction chamber is modeled by a quasi-steady energy balance neglecting energy storage in the structure and helium side gas. The equation gives both the heat transfer rate and the helium outlet temperature.

$$\dot{Q}_{HX} = U \cdot A \cdot \Delta T = M_{He} (h_{He,in} - h_{He,out}) , \quad (4.11-108)$$

where

U is the overall heat transfer coefficient of heat exchanger,

A is the heat transfer surface area,

ΔT is the mean temperature difference between the helium and reaction zone,

m_{He} is molar flow rate of helium stream,

$h_{He,in}$ is molar enthalpy of helium stream at inlet with T_{h1} ,

$h_{He,out}$ molar enthalpy of helium stream at outlet with T_{h2} .

The approach taken by the MELCOR-H2 is to approximate the pressure as constant in the reaction chamber. The logic is that in the actual process system would have pressure control logic in each reaction chamber to regulate the pressure. Thus, the approximation tacitly assumes a perfect pressure controller as part of the reaction chamber model.

$$\frac{dP}{dt} = 0; P = \text{constant.} \quad (4.11-109)$$

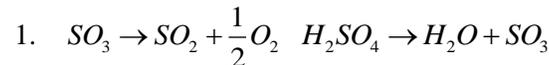
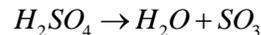
An unfortunate consequence for the purposes of an I}C code is that the constant pressure approximation lacks the capability to introduce pressure disturbances from the chemical process into the overall system response or to model events initiating in the pressure control system, such as a failure of the controller.

The system of equations for the reaction chamber can be closed by the addition of an equation for the reaction rate in the mass equation Eq. (4.11-96) and energy equation Eq. (4.11-107). The main chemical reaction in the SI cycle is modeled with the simplification of a one-step process. Other chemical processes for the separation, concentration, and recycling are neglected or simplified to ideal algebraic equations.

For Section 1 of the SI process in Fig. 45, the depletion rate of sulfur dioxide can be approximated as a one-step reaction^{54,*},

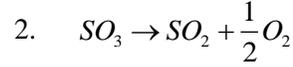
$$-\frac{d[SO_2]}{dt} = k_1 \cdot [I_2] \cdot [H_2O] \cdot [SO_2] \quad (4.11-110)$$

For Section 2, the sulfuric acid decomposition is carried out in two steps. First, sulfuric acid is assumed to be decomposed into water and sulfur trioxide. Second, oxygen and sulfur dioxide are produced by the decomposition of sulfur trioxide.⁵⁵ These steps are



*The notation $[A_i]$ means the molar concentration of species A_i . In SI units, the concentration is given in kmol/m³ or in CGS units, mol/cm³. Based on the data given in Table 3, the units are apparently given in moles per liter. Although not explained in the reference, the extent of reaction rate is related to the reaction rate by

$$\frac{d[A_i]}{dt} = \frac{1}{V_R} \frac{dM_{i,RXN}}{dt} = \frac{v_i}{V_R} \frac{dX}{dt}$$



From the chemical equilibrium calculation, the sulfuric acid decomposition (first reaction) is close to 100% above 700°C.⁵⁵ Therefore, 100% conversion is assumed in this model. Thus, the chemical kinetics equation for Section 2 is reduced to a one step reaction involving only the concentration of SO₃. The Section 2 reaction rate is expressed as

$$-\frac{d[H_2SO_4]}{dt} = -\frac{d[SO_3]}{dt} = k_2 \cdot [SO_3] \quad . \quad (4.11-111)$$

Because the reverse reaction rate of Section 3 is substantial, the definition of the hydrogen iodide depletion rate is significantly more complex. The reaction



can be modeled by

$$\frac{d[H_2]}{dt} = k_3 \cdot [HI]^2 - k_{-3} \cdot [H_2] \cdot [I_2] \quad . \quad (4.11-113)$$

The leading coefficients, k_1 , k_2 , and k_3 , in the reaction rate are temperature dependent. The appropriate temperatures and forms for the equations are given in the following expressions

$$k_1 = A_1 \exp\left(-\frac{E_1}{R} \left\{ \frac{1}{T_1} - \frac{1}{T_0} \right\}\right)$$

$$k_2 = A_2 \exp\left(-\frac{E_2}{RT_2}\right) \quad , \quad (4.11-114)$$

$$k_3 = A_3 \exp\left(-\frac{E_3}{RT_3}\right), k_{-3} = A_{-3} \exp\left(-\frac{E_{-3}}{RT_3}\right)$$

where T_0 is the temperature of the stream entering Section 1. T_1 , T_2 , and T_3 are the temperatures of the three reaction chambers. Data of the reaction rates are given in Table 3.

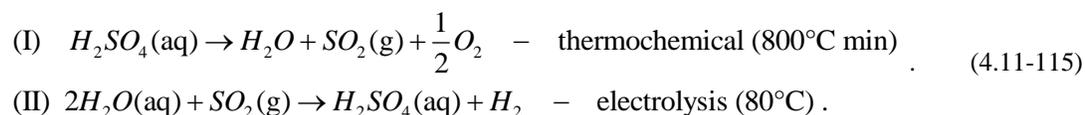
Table 3. Reaction rate parameters

Section 1: Bunsen reaction (Liquid Phase, 120°C)	
Pre-Exponential Factor (A_1)	$3e-6 \text{ L}^2/(\text{mol}^2 \text{ s})$
Activation Energy (E_1)	4.187 kJ/mol
Section 2: H₂SO₄ decomposition (Gas Phase, 850°C)	
Pre-Exponential Factor (A_2)	$6.8e4 \text{ s}^{-1}$
Activation Energy (E_2)	73.1 kJ/mol
Section 3: HI decomposition (Gas Phase, 450°C)	
<i>Reverse Reaction</i>	
Pre-Exponential Factor (A_3)	$1.596e7 \text{ L}/(\text{mol s})$
Activation Energy (E_3)	108 kJ/mol
<i>Forward Reaction</i>	
Pre-Exponential Factor (A_3)	$1e11 \text{ L}/(\text{mol s})$
Activation Energy (E_3)	184 kJ/mol

The system of equations can be solved dynamically for the mole fractions and temperature of the mixture by integration.

4.11.5.2 Westinghouse hybrid sulfur-iodine process*

The Westinghouse HyS cycle has two reactions. Two reactions, one purely chemical, and the second a chemical reaction plus electrolysis produces sulfuric acid and hydrogen from water and sulfur dioxide at low temperature. The two reactions can be written as



The first reaction, sulfuric acid decomposition reaction, is the same reaction in the SI cycle. Therefore, the model developed for the SI cycle can be used directly for this reaction with appropriate modification of recycling flows. Figure 47 presents a schematic diagram for the simplified HyS model.

* The set of equations for the hybrid electrothermal process in this section is reported as given in Rodriguez;³⁹ however, the model description seems incomplete. A formula for the term for current, I , in the reaction rate is not computed. A modeling equation for the electrical circuit including the electrolyzer would seem to be necessary to determine the current. The circuit equation would depend in part on the voltage given here.

Also, the definition of the parameter, N , is given as the “number of electrolyzer” which is not clear. The power term, P , is defined but not used. Presumably, it goes into the energy equation which is not given for a reaction chamber with electrolysis.

A revision to the reference document is needed to correct and clarify the model.

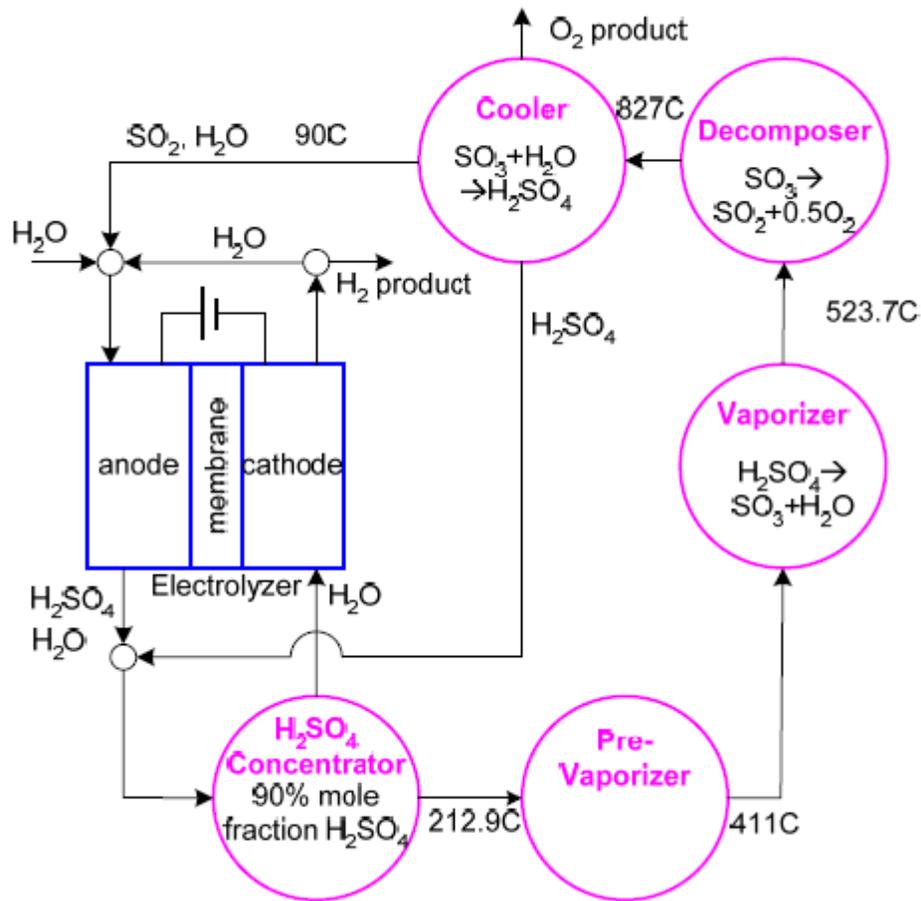


Fig. 47. Schematic for the simplified hybrid sulfur-iodine process.³⁹

The HyS cycle includes both the chemical process driven by chemical potentials and the electrolytic process for separating water into hydrogen and oxygen. The electrolysis process passes a current between two electrodes in an ionic solution, causing charge to concentrate on both electrodes. A thermodynamic analysis of electrolysis provides some insight into modeling electrolyzer behavior.

The electrical work that a spontaneous chemical reaction is capable of producing is directly related to the change in Gibbs free energy, ΔG , of the reaction (II). The change in Gibbs free energy for an electrochemical cell is expressed as

$$\Delta G = \Delta E + P\Delta V - T\Delta S \quad , \quad (4.11-116)$$

where ΔE is the sum of the thermal and electrical work done to the system, $P\Delta V$ is the pressure volume work done to the system, and $T\Delta S$ is the increase in entropy of the system. For a reversible process, the Gibbs free energy expression is simplified as

$$\Delta G = w_{elec} + q - T\Delta S = w_{elec} + T\Delta S - T\Delta S . \quad (4.11-117)$$

Thus, the Gibbs free energy can be written as

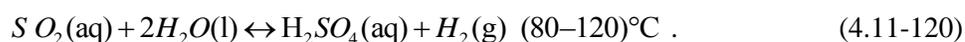
$$\Delta G = w_{elec} . \quad (4.11-118)$$

The electrical work required for a given electrolysis process is given by

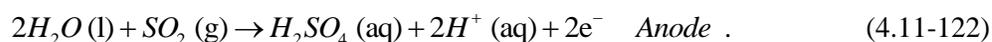
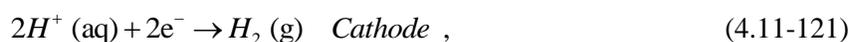
$$E_0 = \frac{\Delta G}{nF} , \quad (4.11-119)$$

where n is the number of charges exchanged in the electrolysis reaction, and F is the Faraday constant (i.e., the charge of 1 mol of electrons)⁵⁶.

For the HyS cycle, the electrolysis reaction is



This reaction cannot be approximated as an elementary one-step reaction; rather, it is composed of at least two component reactions. These reactions are⁵⁷,



The concentration dependent cell energy required is given by the Nernst equation,

$$E = E_0 - \frac{RT}{nF} \ln Q , \quad (4.11-123)$$

where Q is the reaction quotient.

Jeong et al⁵⁷ gives the expressions for the potential at the cathode, anode, and the entire cell as

$$E_{cathode} = -\frac{RT}{nF} \ln \frac{H_2}{[H^+]^2} , \quad (4.11-124)$$

$$E_{anode} = E_0 - \frac{RT}{nF} \ln \frac{[H_2SO_4][H^+]^2}{[H_2O]^2[SO_2]} , \quad (4.11-125)$$

$$E = E_{cathode} + E_{anode} = E_{anode}^0 - \frac{RT}{nF} \ln \frac{[H_2SO_4][H_2]}{[H_2O]^2[SO_2]} . \quad (4.11-126)$$

In these equations, the concentration of each of the constituents is in brackets. Several values are presented in literature for the open circuit potential of the anode. Jeong et al.⁵⁷ gives -0.17 volts and Forsberg et al.⁵⁸ gives -0.29 volts. This open circuit voltage may be calculated from thermodynamic tables of Gibbs free energy. Thus, the value of this potential may vary slightly depending on the source of the thermodynamic data used. In reality, the electrode potential is higher than the theoretical value. The actual voltage of the electrolyzer is composed of a theoretical open circuit voltage and three losses: activation losses, ohmic losses, and concentration losses. Activation losses occur because of the slowness of the chemical reaction taking place. The loss becomes quite large at low current densities, but levels out quickly. Ohmic losses are caused by internal resistance to current flow. This resistance is very difficult to model analytically, as it is dependent on many factors. Generally, an empirical formula is used.

Hydrogen is generated at the cathode. The molar rate of hydrogen generation is directly related to the amount of current supplied by Faraday's law of electrolysis⁵⁹, which states

$$\dot{n}_{H_2, RXN} = \frac{NI}{nF} , \quad (4.11-127)$$

where N is the number of electrolyzer, and I is the total current applied.

If we could control the total current in the electrolyzer as a constant, a constant hydrogen generation can be achievable theoretically as long as the water is supplied to the process and the sulfuric acid is recycled continuously. Water flowing across membrane of the electrolyzer is usually not a concern since the electrolyzer operates with a flooded membrane.

The mass balance in the anode and cathode can be established by the same way in Eq. (4.11-84).

$$\frac{dM_{i,R}}{dt} = m_{i,in} - m_{i,out} + \dot{n}_{i,RXN} , \quad (4.11-128)$$

where

$M_{i,R}$ is the number of moles of species i in the anode or cathode,

$m_{i,in}$ is the molar flow rate of species i into the anode or cathode,

$m_{i,out}$ is the molar flow rate of species i out of the anode or cathode,

$\dot{n}_{i,RXN}$ is the molar generation rate of species i in the anode or cathode.

A detailed energy balance requires a specific design data of the electrolyzer including data for the volume, surface area, solid heat capacity, etc. Total energy supplied through the electrolyzer can be calculated by

$$P = NEI \quad . \quad (4.11-129)$$

4.11.6 Fuel temperature model

4.11.6.1 Analysis method for steady-state temperature profile

The particulate debris field model in MELCOR approximates the temperature of the particles and coolant as a single lumped uniform temperature in a control volume. This modeling approximation is predicated on debris consisting of relatively small particles of decomposed LWR fuel which would be expected to following a serious core degradation event of conventional nuclear plant fuel. The uniform temperature approximation is not appropriate for the packed bed of intact fuel pebbles for an NNGP because these particles are much larger than the assumed particle size of the debris field. To address the limitation of MELCOR, MELCOR-H2 calculates a maximum fuel temperature and surface temperature for an average fuel pebble in each control volume using a Control Function.

The fuel temperature calculation assumes that each fuel pebbles is isolated from other fuel pebbles and, thus, only accounts for convective heat transfer to the primary coolant. The assumption neglects conduction from pebble-to-pebble contact and radiation. The purpose of the calculation is to evaluate approximately the limiting fuel temperatures for operation. The fuel temperatures from the control function calculation are only used for output and are not fed back to the control volume hydraulic model.

The fuel pebble model represents the heat transfer in a fuel pebble by solving the one-dimensional heat equation in spherical geometry with uniform heat generation, uniform thermal conductivity in the fuel, and symmetrical surface conditions*:

*The equations for Eq. (4.11-130) and Eq. (4.11-131) are taken directly from the MELCOR-H2 document,³⁹ but it appears to be the wrong choice for the situation described. The difference between the maximum temperature (T_{max}) to surface temperature

(T_s) for spherical fuel element with uniform heat generation and constant conductivity is given by $\Delta T = T_{max} - T_{s,2} = \frac{\dot{q}r_2^2}{6k_{fuel}}$ which

can be obtained by solving the one-dimensional heat conduction equation in spherical coordinates for the given boundary conditions. This report quotes the equations and derivation as given in the MELCOR-H2 report despite the error. The error does not affect other results. The maximum fuel temperature is calculated in the Control Function for each reactor control volume but appears not to be used in other calculations.

$$q(r) = \dot{q} \frac{4\pi r^3}{3} = 4\pi k_{\text{fuel}} \frac{\frac{\dot{q} r_2^2}{6k_{\text{fuel}}} \left(1 - \frac{r_1^2}{r_2^2}\right) + (T_{s,2} - T_{s,1})}{\frac{1}{r_1} - \frac{1}{r_2}}, \quad (4.11-130)$$

where q is the heat rate in kW, \dot{q} is the volumetric heat generation rate in kW/m³, $T_{s,1}$ is the temperature at r_1 , which is a point very close to the pebble center, ($r_1 = 0.000001$), r_2 is the radius of the pebble, and $T_{s,2}$ is the fuel pebble surface temperature. The temperature differential between the two points can be calculated by

$$\Delta T = T_{s,1} - T_{s,2} = \frac{1}{12} \frac{3qr_2 - 2qr_1 - 4\dot{q}r_2^4 + 6\dot{q}r_2^3r_1}{\pi k_{\text{fuel}} r_1 r_2}. \quad (4.11-131)$$

For the thermal conductivity of the fuel, k_{fuel} , in a packed bed as a function of temperature, an empirical correlation by No et al. was used:⁶⁰

$$k_{\text{fuel}} = 1.1536 - 4(T - T_0), \quad (4.11-132)$$

where T_0 is the reference temperature of 273.16 K.

More details on the core steady state thermal model can be found in Rodriguez et al.^{39, 61}

Analysis method for transient radial temperature profile

For the transient analysis, a first-term approximation from the first term of an exact series exact solution of the spherical geometry is used. The first term is represented by*

$$\theta^* = \theta_0^* \frac{1}{\zeta_1 r^*} \sin \zeta_1 r^*, \quad (4.11-133)$$

where θ^* is the dimensionless temperature at the dimensionless radial distance outward $r^* = r/R$. R is the radius of a fuel pebble.

*This equation for transient radial temperature comes from Rodriguez³⁹ but appears to be the wrong choice for the given problem. The equation given in Rodriguez is for a sphere without internal heat generation which is exposed to a sudden change in bulk fluid temperature at the surface. The forcing terms for changing neutron heat generation, $\dot{q}(t)$ or gradually changing bulk fluid temperature, $T_\infty(t)$ could be added to the series approximation method but appear not to be addressed by the author. The equations are reported as given in the MELCOR-H2 report without correction.

$$\theta^* = \frac{T_s - T_\infty}{T_{s,0} - T_\infty}, \quad (4.11-134)$$

where T_s is the surface temperature and $T_{s,0}$ is the initial surface temperature of the sphere, and T_∞ is the coolant ambient temperature around the sphere. The dimensionless temperature at the sphere center, θ_0^* , is defined by C_1

$$\theta_0^* = C_1 \exp(-\zeta_1^2 Fo) \quad (4.11-135)$$

where and ζ_1 are tabulated constants, and Fo is the Fourier number which is a dimensionless measure of time, $Fo = \frac{\alpha t}{R^2}$ where α is the thermal diffusivity and R is a characteristic dimension. For spherical geometry, R is the radius of the fuel pebble.

4.11.7 Implementation of reactor kinetics in MELCOR-H2

As a severe accident code for LWRs, the original MELCOR code focuses on the events following a severe accident in which an LWR is typically subcritical and the energy source is decay heat. Consequently, MELCOR has never included the dynamics of a critical reactor. Many NNGP events however include criticality or recriticality in the sequence of events. MELCOR-H2 has added a point kinetics model of the neutron power to represent normal operations or accident events in which the reactor remains critical or returns to criticality. The model uses six delay neutron groups as well as dynamic models of the decay heat precursor groups and the dynamics of xenon and samarium. The modeling equations start with the usual form given by

$$\frac{dP}{dt} = \frac{\rho - \bar{\beta}}{\Lambda} P + \sum_{i=1}^6 \lambda_i Y_i + S_0, \quad (4.11-136)$$

$$\frac{dY_i}{dt} = \frac{\beta_i}{\Lambda} P - \lambda_i Y_i, \quad i = 1, \dots, 6, \quad (4.11-137)$$

where P is the reactor thermal power, Y_i is the individual thermal power generated by the i th delayed neutron precursor group, ρ is the total reactivity, S_0 is the neutron power source term (source term in neutrons per second times the power per fission), β_i is the fraction of the i -th precursor group, λ_i is its decay constant, $\bar{\beta}$ is the total delayed neutron fraction $\bar{\beta} = \sum_i \beta_i$, and Λ is the neutron generation time.

The assumption inherent in the point kinetics approximation is that the normalized shape of the neutron

flux distribution is constant. Typically this is a valid approximation for HTGR reactors. An exception is a study of xenon stability which depends on the spatial distribution of flux. Typically, the axial dependence of flux is the most limiting spatial dimension for xenon stability.

The temperature feedback is introduced by decomposing the total reactivity into components,

$$\rho = \rho_{\text{ext}} + \rho_D + \rho_f + \rho_G, \quad (4.11-138)$$

where ρ_{ext} is the external reactivity (i.e., active control), ρ_D is the fuel Doppler feedback reactivity, ρ_f is the fuel density temperature feedback reactivity, and ρ_G is the graphite density temperature feedback reactivity.

The fuel Doppler feedback reactivity is approximated by the expression

$$\rho_D = \chi_D \ln \left(\frac{\bar{T}_f}{T_{f,0}} \right), \quad (4.11-139)$$

where χ_D is the Doppler reactivity coefficient, \bar{T}_f is the volume-averaged fuel temperature, and $T_{f,0}$ is initial fuel average temperature.

The fuel density feedback reactivity is approximated by a second order fit.

$$\rho_f = \chi_{f,1} (\bar{T}_f - T_{f,0}) + \chi_{f,2} (\bar{T}_f^2 - T_{f,0}^2), \quad (4.11-140)$$

where $\chi_{f,1}$ and $\chi_{f,2}$ are the first and second order fuel reactivity coefficients.

The graphite density reactivity feedback for the moderator and reflector is approximated by a fourth order polynomial

$$\rho_G = \sum_{m=1}^4 \chi_{G,m} (\bar{T}_G^m - T_{G,0}^m) \quad (4.11-141)$$

where $\chi_{G,m}$ is the moderator reflector coefficient for the m -th order term, \bar{T}_G^m is the volume averaged temperature for the moderator and reflector raised to the m -th power, and $T_{G,0}^m$ is the initial temperature for \bar{T}_G^m .

The time constant for the prompt neutron equation is very small which restricts the maximum stable time step for forward Euler and Runge-Kutta solutions of the neutron kinetics equation to fairly small values. Since the point kinetics equations are implemented in a Control Function, the stability requirements of this model are not available to be used in setting the time step for the thermal-hydraulic solution. To relax

the constraint on the time step imposed by a conventional forward Euler or Runge-Kutta advancement scheme, MELCOR-H2 introduces a novel solution scheme which is described here.

The numerical solution in MELCOR-H2 involves first writing the time advancement in terms of the analytical solution involving the matrix exponential of the first order system. To avoid the difficult and time-consuming numerical problem of evaluating the matrix exponential at each time step, the solution finds a Padé approximation of the matrix exponential that can be made as accurate as needed by increasing the number of terms in the expansion. The solution shows that numerical stability of the point kinetics can be maintained with a third-order Padé approximation. The Padé approximation makes the neutron kinetics time step limitation greater (less limiting than the thermal-hydraulic simulation). Thus, it is unnecessary to limit the overall system time step due to the numerical stability limitations of the point kinetics solution.

First, the point kinetics equations are written in vector form. Let

$$[\Psi] = [P \ Y_1 \ Y_2 \ Y_3 \ Y_4 \ Y_5 \ Y_6]^T, \quad (4.11-142)$$

$$[S] = [S_0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]^T \quad (4.11-143)$$

$$\{\mathbf{A}\} = \begin{bmatrix} A_{11} & \cdots & A_{17} \\ A_{21} & \cdots & A_{27} \\ & & \\ & & \\ & & \\ A_{71} & & A_{77} \end{bmatrix} = \begin{bmatrix} (\rho - \bar{\beta}) / \Lambda & \lambda_1 & \lambda_2 & \cdots & \lambda_6 \\ \beta_1 / \Lambda & -\lambda_1 & 0 & \cdots & 0 \\ \beta_1 / \Lambda & 0 & -\lambda_2 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ \beta_1 / \Lambda & 0 & 0 & \cdots & -\lambda_6 \end{bmatrix}. \quad (4.11-144)$$

Equations (4.11-136) and (4.11-137) are then written as

$$\frac{d}{dt}[\Psi] = \{\mathbf{A}\} \cdot [\Psi] + [S]. \quad (4.11-145)$$

To obtain an analytical solution, the source term in [S] and the reactivity term in {A} are approximated as constant over a time step. The matrix exponential solution is

$$[\Psi] = \{\exp(\mathbf{A}t)\} \cdot ([\Psi_0] + \{\mathbf{A}\}^{-1} \cdot [S]) - \{\mathbf{A}\}^{-1} \cdot [S], \quad (4.11-146)$$

where $[\Psi_0]$ is the initial condition.

This solution can be used to approximate the actual case in which S_0 and ρ are time-varying by the following advancement scheme.

$$[\Psi]_{n+1} = \{\exp(\{\mathbf{A}\} \Delta t)\} \cdot ([\Psi]_n + \{\mathbf{A}\}^{-1} \cdot [\mathbf{S}]) - \{\mathbf{A}\}^{-1} \cdot [\mathbf{S}] . \quad (4.11-147)$$

The time varying terms can be approximated using a Crank-Nicholson approach

$$A_{11} = \frac{\theta \rho_{n+1} + (1-\theta) \rho_n - \bar{\beta}}{\Lambda} \quad (4.11-148)$$

and

$$S_0 = \theta (S_0)_{n+1} + (1-\theta) (S_0)_n , \quad (4.11-149)$$

where $0 \leq \theta \leq 1$. A value of 0.5 provides the best accuracy in time.

The direct numerical solution of Eq. (4.11-147) is both computationally difficult and time-consuming because of the evaluation of the matrix exponential. A numerical solution replacing the matrix exponential with its Padé approximation reduces the numerical load while maintaining accuracy and numerical stability. The Padé approximation function, $P(p,q,)$, is the ratio of two polynomials, where p and q indicate the order of the numerator and denominator polynomials respectively. The Padé approximation can be made as accurate as necessary by increasing the order of the solution. MELCOR-H2 has found that $P(3,3)$ gives sufficient accuracy of the neutron kinetics solution using the time steps equal to or greater than the time step needed for numerical stability in the thermal-hydraulics solution. Padé polynomials for $\exp(x)$ up to order 3×3 are given in Table 4.

Table 4. Padé approximation of the exponential function

p	$q=0$	$q=1$	$q=2$	$q=3$
0	$\frac{1}{1}$	$\frac{1}{1-x}$	$\frac{2}{2-2x+x^2}$	$\frac{6}{6-6x+3x^2-x^3}$
1	$\frac{1+x}{1}$	$\frac{2+x}{2-x}$	$\frac{6+2x}{6-4x+x^2}$	$\frac{24+6x}{24-18x+6x^2-x^3}$
2	$\frac{2+2x+x^2}{2}$	$\frac{6+4x+x^2}{6-2x}$	$\frac{12+6x+x^2}{12-6x+x^2}$	$\frac{60+24x+3x^2}{60-36x+9x^2-x^3}$
3	$\frac{6+6x+3x^2+x^3}{6}$	$\frac{24+18x+16x^2+x^3}{24-6x}$	$\frac{60+36x+9x^2+x^3}{60-24x+3x^2}$	$\frac{120+60x+12x^2+x^3}{120-60x+12x^2-x^3}$

The $P(3,3)$ approximation of the matrix exponential in Eq. (4.11-147) can be written as

$$\exp(\{\mathbf{A}\} \Delta t) \cong \left\{ \mathbf{I} - \frac{\{\mathbf{A}\} \Delta t}{2} + \frac{(\{\mathbf{A}\} \Delta t)^2}{10} - \frac{(\{\mathbf{A}\} \Delta t)^3}{120} \right\}^{-1} \cdot \left\{ \mathbf{I} + \frac{\{\mathbf{A}\} \Delta t}{2} + \frac{(\{\mathbf{A}\} \Delta t)^2}{10} + \frac{(\{\mathbf{A}\} \Delta t)^3}{120} \right\} \quad (4.11-150)$$

The form of the advancement using the Padé approximation is then given by

$$[\Psi]_{n+1} = \left\{ \mathbf{I} - \frac{\{\mathbf{A}\} \Delta t}{2} + \frac{(\{\mathbf{A}\} \Delta t)^2}{10} - \frac{(\{\mathbf{A}\} \Delta t)^3}{120} \right\}^{-1} \cdot \left\{ \mathbf{I} + \frac{\{\mathbf{A}\} \Delta t}{2} + \frac{(\{\mathbf{A}\} \Delta t)^2}{10} + \frac{(\{\mathbf{A}\} \Delta t)^3}{120} \right\} \cdot ([\Psi]_n + \{\mathbf{A}\}^{-1} \cdot [\mathbf{S}]) - \{\mathbf{A}\}^{-1} \cdot [\mathbf{S}] \quad (4.11-151)$$

4.12 VHTR Core Models in MELCOR-H2

4.12.1 Modeling the pebble bed reactor core with MELCOR-H2

A sample nodalization scheme found in the literature developed for modeling the PBMR core in MELCOR is shown in Fig. 48. The MELCOR modeling the PBMR work originally appeared in the master's thesis of Hogan.⁶² This figure was repeated in Rodriguez³⁹ which is where this review obtained it.

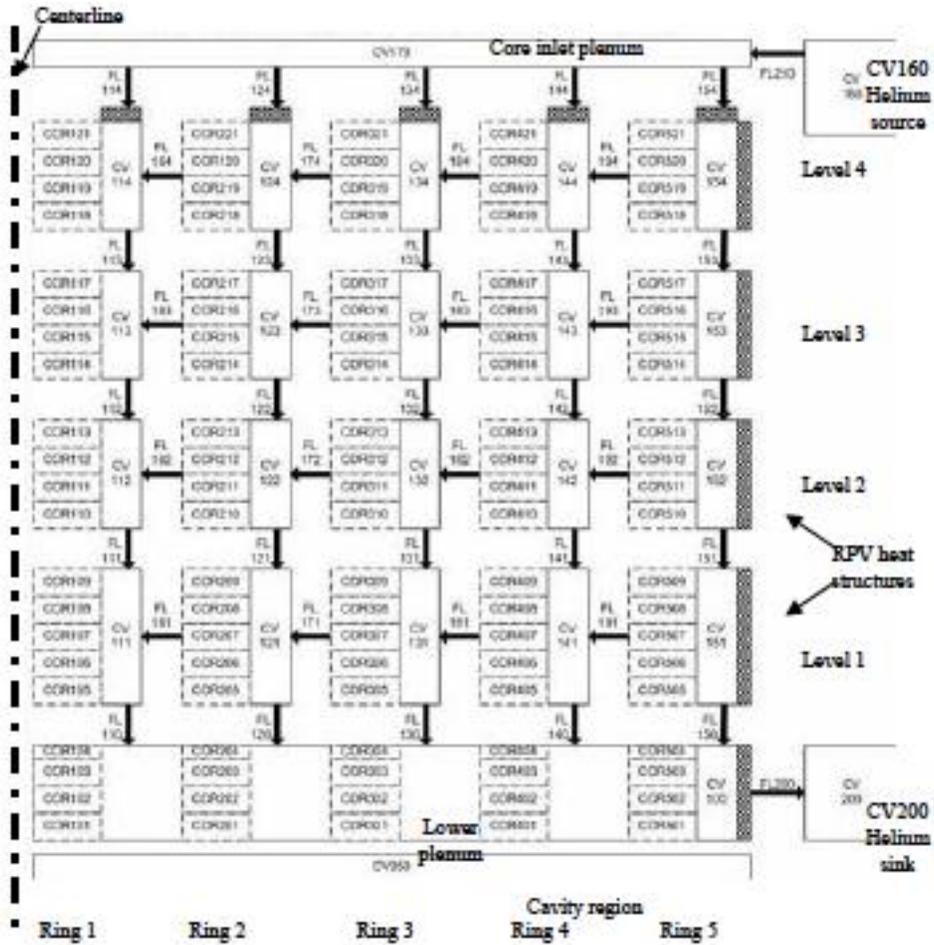


Fig. 48. Nodalization scheme for PBMR model in MELCOR⁶².

4.12.2 Modeling the prismatic VHTR core with MELCOR

The study by Rodriguez et al.³⁹ models the prismatic VHTR core in a three region approximation to the core. The model includes the primary coolant flowing through an annular core region surrounded by the inner and outer reflectors. Control volumes (CV) for the primary coolant and the reflectors were modeled by heat structures (HS) as shown in Fig. 49. This example is not a full system model. Only the reactor vessel and core are modeled. Helium enters the system via a mass and enthalpy source at CV 160. The flow is upward through the outer annulus of the reactor vessel to an upper plenum volume and then across an upper plenum plate, where it is distributed to three radial fuel rings to flow downward through seven axial levels. Among these seven axial levels, the top most is an upper reflector, and the bottom most is a lower reflector. The five in between are active fuel zones. Flow exiting the core flows into a core exit plenum (CV 054) and out of the system through a mass and enthalpy sink at CV 200.

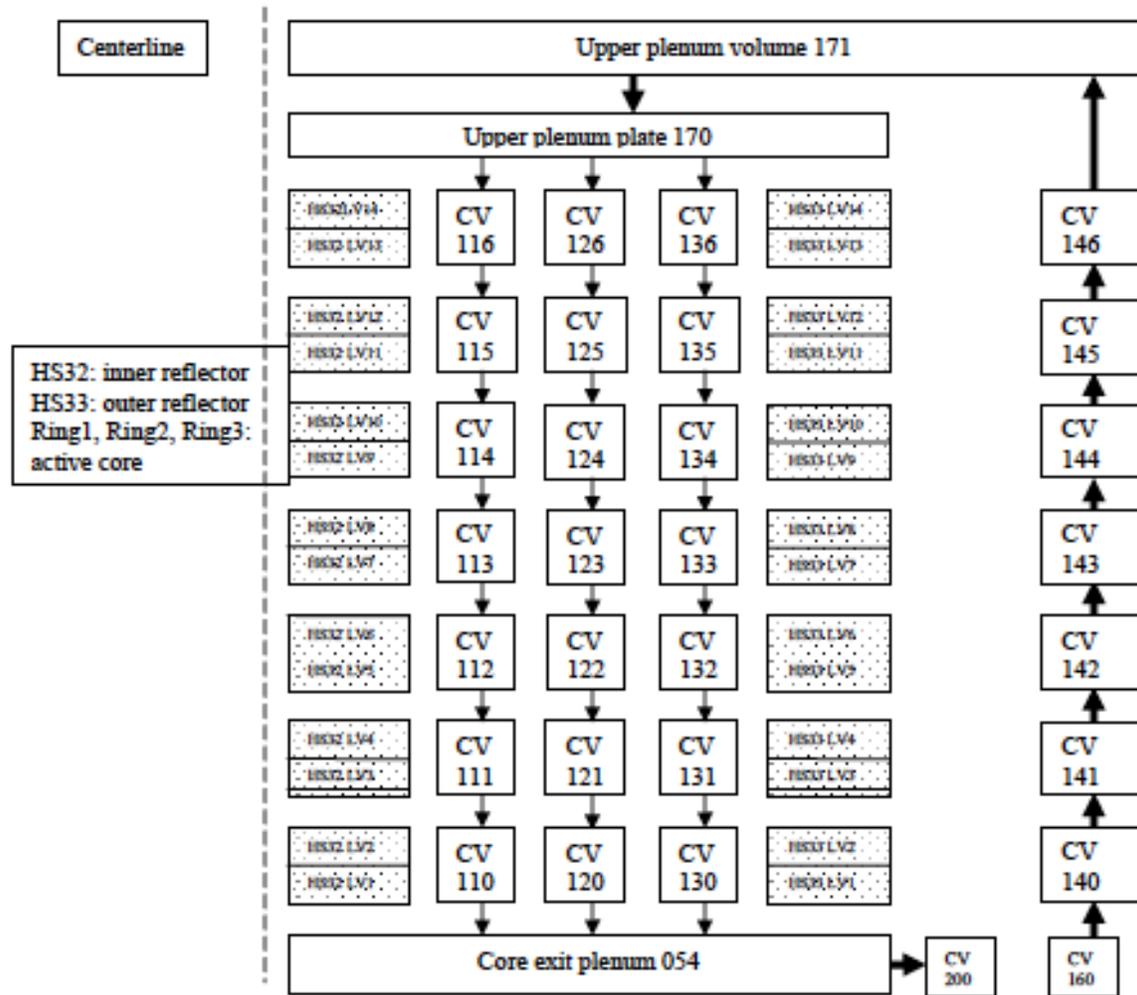


Fig. 49. Nodalization of the simplified NGNP VHTR model in MELCOR-H2.

The core region is composed of three radial regions: an inner reflector region, an active core, and an outer reflector region. These correspond to heat structure HS32, Rings 1–3, and HS33, respectively. This model did not contain COR package input for modeling core and lower plenum structural degradation.

The upper reflector is located above the active core and the outer reflector, and the lower reflector is below them. Since the MELCOR-H2 code does not allow the modeling of an HS adjacent to another HS, the upper reflector region that is located above the active core and the lower reflector region that is located beneath the active core are modeled as control volumes. The upper reflector region that is located above the side reflector and the lower reflector region that is located beneath the side reflector are modeled as heat structures.

5. SUMMARY AND CONCLUSIONS

This report has gathered information on I&C modeling needs for NRC licensing reviews of VHTRs or for development of new NRC regulations or guidance appropriate for the VHTR design. The approach was first to develop a set of transients which might be simulated in support of reviews of I&C system. From that list, the particular modeling features and code phenomena that are needed to represent those transients are developed and discussed. The code phenomena discussion is organized around the main components of a VHTR system. Any special code phenomenon or modeling considerations that are important for an I&C simulation, as distinct from a safety analysis model, are discussed. The report then considers the capabilities of two codes, RELAP and MELCOR, in some detail. The reporting on these two codes is based largely on their code manuals. The code manuals lack discussions of recent additions of components for modeling gas reactors. These aspects of the relied on special reports on the codes and reports on applications of the new features in VHTR modeling efforts. The goal was to describe the models both in terms of their intended capability and in their mathematical formulation.

5.1 General Observations

A great many aspects of NRC review of I&C systems are evident simply from inspection of a design. However, as complexity level increases, at some point, reviewers cannot trust that the operation can be visualized mentally, particularly when interactions between multiple systems are involved. While an engineer may be able to state with some confidence the direction a system will respond, he or she is less able to state quantitatively how far it will go or how fast it will respond. In this situation, the reviewer relies on simulations to see how the full system works. For the most part, the NRC relies on applicants to demonstrate quantitative performance with a calculation or simulation when it is needed. In some instances, the NRC does perform independent studies to confirm applicant's results. The NRC also uses its own calculation models in research for developing new regulatory guidance. The role of simulation and modeling within the NRC may increase with the review of advanced reactors because of the potential for increased complexity in the systems. For example, advanced reactor and plant system designs, including the HTGR, are expected to employ instrumentation and control systems with almost all the safety-related and nonsafety-related functions performed by digital systems—sometimes with an analog system as a diverse backup. The level of sophistication on the control side of the digital system implementations is expected to increase as the regulatory bodies have better understanding of the failure modes and mechanism of these systems. Review of these complex systems and their potential failures will be a major challenge for engineers. In the area of control, it is expected that the plants would employ full automation of startup and shutdown transitions. The startup and shutdown modes are special control modes which the control system detects the need to switch into or out of. The complexity of these operations in conjunction ability to switch into and out of manual control smoothly makes the automation multistate event-based process. The automatic control extends over a much broader range of operations than before. Ensuring that the plant adheres to all requirements and responds safely to all challenges becomes complicated by the much more diverse range of automatic actions that a fully automated plant is programmed to perform. The jobs of the I&C designer and reviewer are, likewise, increased. Ensuring that no unintended adverse interactions with safety functions and unintended violation of the plant's technical specifications becomes part of the control engineer's and the I&C reviewer's jobs. The automation may prove to be the most challenging part of licensing the control algorithm. The need to observe and test the operation of the automation functions under a wide range of conditions will undoubtedly depend on a simulation of the operation under a great variety of normal and abnormal conditions. The NRC may find that having a plant simulation of their own is an indispensable tool in both understanding response and confirming the safety of the design in the review.

This review has covered only the I&C modeling codes. The modeling job is actually somewhat larger than that. I&C codes depend on other computer codes or calculations for much of the modeling input data. Parameters such as turbine performance maps, reactivity coefficients, delay neutron model parameters are produced by a sophisticated calculations in their own right. In developing an I&C modeling capability, the NRC will also have to develop the capability to calculate the parameters needed for input. Also, as noted in the report, many input parameters have a significant uncertainty or have a normal variation over the fuel cycle or with aging. Evaluating the system interactions may require a range of values to be used to fully explore the parameter space fully. These parameter ranges come from other calculations and detailed knowledge of the plant. Obtaining complete and appropriate input data for the modeling codes is always a major challenge, and this task has not been addressed in this review.

The codes that have been reviewed, MELCOR and RELAP5, have a long history with extensive qualification on their original purpose of modeling LWRs. The extensions and new features that have been added for modeling gas-cooled reactors have a lesser history and qualification. These versions of the code have been developed in the same nuclear safety analysis culture and have followed the same software engineering processes, but the gas reactor results should still be considered more cautiously and reviewed more carefully for accuracy and reasonableness. Additional verification studies, experience with the use of new gas reactor features, and qualification of results against operating reactor performance when it becomes available will raise the confidence level that can be placed in the results. Also the codes may not have all the features that are needed for all I&C studies. Additional work may be needed to develop special features for control modeling, network communications, modeling of remotely placed sensors, and other features not yet identified. At this stage of development, the available codes for I&C analysis should be considered developmental and not production codes.

Neither MELCOR nor RELAP5 is well-suited for I&C analysis. These codes have the necessary thermal hydraulic components for the full plant simulation, but those components have a great many features that are necessary only for safety analysis in LWRs that burden the simulation and burden the user trying to develop the simulation of a plant. What is mainly needed for I&C is a simple, fast-running process model for driving a detailed model of the control system. In MELCOR and RELAP5, just the opposite case exists. MELCOR and RELAP5 have detailed process models with unnecessary special features for LWRs coupled to primitive capabilities for modeling controls. Neither has tools for fully representing the control system in every detail. Neither has an interface to a control analysis tool like MATLAB/SIMULINK or sophisticated graphical user interface for representing the controls system design visually. Using these codes for I&C review would be time consuming and require substantial investment in training and input data development.

5.2 Observations on RELAP5

RELAP5 contains a set of reactor system building blocks with which to develop VHTR models that are suited for a wide range of control and protection system simulations. Models of VHTRs with near full plant scope have already been assembled and demonstrated. The single phase gas-reactor thermal hydraulics is overlaid on a structure that was developed specifically for modeling two-phase flow problem in LWRs. RELAP's hydrodynamic formulation is designed to reduce gracefully to a single phase model so that it appears that the additional capability does not hinder the gas reactor simulations. The thermal hydraulics is primarily a one-dimensional model which is entirely suitable for I&C models. RELAP5's three-dimensional version of the thermal hydraulics is limited to a coarse mesh. It is unclear if RELAP's three dimensional flow model is capable of simulating parts of VHTRs which may exhibit significant three-dimensional effects (such as the lower plenum in prismatic cores or the core region in pebble bed designs). In general, three-dimensional effects are not major concern in I&C models.

RELAP code has provided special models for gas turbines, compressors, steam generators, valves, and heat exchangers such that most configurations of the NGNP plants that have been proposed could be

simulated. No chemical process models for hydrogen generation have been developed for interfacing with the RELAP code. Models of the chemical plant would be limited to boundary conditions that apply a predefined heat load to the system or a heat exchanger with a predefined temperature entering at predefined temperature and flow.

The range of conditions that RELAP is capable of simulating covers all the transients that are conceived of in this report. This includes all the normal and abnormal operating events and design basis accidents. For beyond design basis events such as air and water ingress, RELAP has some capability for simulating multicomponent fluids and chemical reactions so that air and water ingress events could be modeled. This capability has not been demonstrated. One of RELAP's modeling limitations that would affect the air ingress event is that a junction cannot model counter current flow for a single phase. Hence, RELAP would not be able to simulate the physics of a break in which hot gas flows out the top of the break while cold outside air flows in at the bottom of the break. Also, RELAP is generally limited to cases in which the fuel and structures remain intact so that the full evolution of an air or water ingress would not be possible. Severe accident modeling is generally not the main emphasis of I&C cases so these limitations on modeling severe accidents are not a major concern.

Within the control simulation capability, the set of control components is fairly complete for modeling conventional controls. Components that are available in the library such as the lag and lead-lag controllers and proportional-integral controller are plug-and-play components that can be used for implementing control strategies. Like all RELAP input, the data for the controls are implemented by card image-like inputs that specify connections and parameters. However, more sophisticated control algorithms usually have more demanding computational requirements that would not be efficiently defined using these built-in control primitives. Optimal control, robust control, adaptive control, and model predictive control are just a few among these approaches. These control methods are usually avoided for controlling the primary system functions because the simpler controls are sufficient but can be implemented for the PCS, such as the turbine control. RELAP5 currently does not support the higher level control algorithms.

One of the shortcomings of the RELAP5 code system—from the control systems simulations perspective—is that it does not allow incorporation of user-created external subroutines that can perform other computations and communicate the results with the main application in a predetermined protocol. This would significantly extend the capabilities of the code system and allow design and analysis simulations of a much larger set of control systems. An interface to Matlab, for example, would allow a much greater range of control designs to be developed using the Matlab/Simulink for control development and analysis and simulation testing of the design by coupling to the RELAP5 simulation.

Another challenge in modeling these complicated systems is the communication network. In the earlier nuclear plant designs where analog control systems were used, data transfer was accomplished through point-to-point wired connections which carry a single signal. However, digital instrumentation and control systems employ fiber optic communication networks to transmit control and protection system inputs and outputs in an efficient and timely manner. The fiber optic networks carry many signals on the same network. Issues of timing, sneak circuits, and handling of missed or corrupted communications is an area of control and safety review. The review of such communications currently lacks a tool to simulate a full communication system with various rates of communications failures to show the actual consequences to the system response. RELAP does not offer any tools to represent the full range of timing and delay effects of digital communications either on a network or represent communication failures.

5.3 Observations on MELCOR

MELCOR is a fully integrated, engineering-level computer code whose primary purpose is to model the progression of severe accidents in LWR nuclear power plants. It is specifically designed to represent accidents which proceed to core degradation and relocation of structural components. Recent additions to

the code have made it possible to simulate gas-cooled reactors. These additions include additional material properties for helium coolant and the reaction products needed for severe accident analysis and special component models for a full plant simulation. The new component models include axial flow turbomachines, a counter-flow heat exchanger, neutron point kinetics, pebble fuel heat transfer, and two chemical processes for hydrogen production. Some of the additions seem to be of a preliminary nature, and problems in their formulation have been noted in the text. Even though the modeling structure contains the special features for degradation and relocation fuel and structure which are largely unneeded for I&C models, the code is also capable of modeling the normal and abnormal operating events and design basis events that have been proposed in this report as needed for the I&C modeling tool for the NRC. The one-dimensional hydrodynamic equations and the numerical solution technique are suitable for I&C calculations over a wide range of conditions.

The control simulation capability for MELCOR is fairly limited. It includes standard blocks for the basic arithmetic operations and special control operations such as hysteresis, PID control, and trips. In contrast to RELAP5, however, MELCOR has the capability for user-defined functions. These functions are used both to simulate the actual controls system and to simulate physical processes that are not contained in the supplied process models. The control functions, for example, are used for the pebble fuel heat transfer model. The control functions are limited to a maximum of five real inputs which would seem to limit their usefulness in general programming. Also, the modeling of control by writing a subroutine would require a higher level of skill than the general NRC analyst who is not a specialist in FORTRAN coding would be comfortable with. In general, the assembly of control and protection system models using MELCOR might be a task best contracted with the MELCOR developers or other MELCOR specialists. Just as in RELAP, MELCOR would also benefit from an interface to a more user-friendly control modeling environment such as MATLAB/SIMULINK.

The turbine and compressor models are somewhat unique compared to usual practice in I&C modeling codes. The model is basically a turbine design tool that has been incorporated as a time dependent model. The model may require a more sophisticated understanding by the user of turbine design and calculations than a more traditional performance map model. Also the code is based on quasi-steady rather than dynamic conservation equations. The quasi-steady approach to modeling the fluid would not be satisfactory for fast turbine control events such as turbine trip or loss of secondary flow. The model is suitable for slow power maneuvering transients, steady state thermal cycle analysis, and events in which the turbine dynamics are of secondary importance. The capability for modeling steady state, off-design conditions is better in MELCOR than in the typical performance map model because of the built-in turbine design correlations.

The chemical process models for hydrogen production and their description is a useful addition to the modeling library, particularly the explanation of the reaction rate equations and the data for chemical models. However, the models do not seem fully integrated with the concept of a transient code for full system modeling. One of the approximations in the chemical model is constant pressure in the reaction chamber. This assumption would prevent simulating the actual pressure controls that might be the subject of an I&C model of the hydrogen process or simulating any event that initiates a pressure disturbance in the chemical reaction chamber.

We found the formulation of the fuel pebble heat transfer model questionable and probably unsuitable for use. This is very likely the consequence of the preliminary nature of the research at the time that it was reported.

6. REFERENCES

1. S. J. Ball et al., *An Assessment of The Safety Implications of Control at the Calvert Cliffs-1 Nuclear Plant*, NUREG/CR-4265, Oak Ridge National Laboratory, Oak Ridge, TN, April 1986.
2. R. S. Stone et al., *An Assessment of the Safety Implications of Control at the Oconee-1 Nuclear Plant*, NUREG/CR-4047, Oak Ridge National Laboratory for U.S. Regulatory Commission, Washington, DC, 1985.
3. O. L. Smith et al., *A PWR Hybrid Computer Model for Assessing the Safety Implications of Control Systems*, NUREG/CR-4449, Oak Ridge National Laboratory for U.S. Nuclear Regulatory Commission, Washington, DC, 1985.
4. A. J. Szukiewicz, *Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants: Technical Findings Related to USI A-47—Final Report*, U.S. Nuclear Regulatory Commission, Washington, DC, June 1989.
5. A. J. Szukiewicz, *Regulatory Analysis for Resolution of USI (Unresolved Safety Issue) A-47: Safety Implications of Control Systems in LWR Nuclear Power Plants—Final Report*, U.S. Nuclear Regulatory Commission, Washington, DC, July 1989.
6. C. B. Davis et al., *Thermal-Hydraulic Analyses of Heat Transfer Fluid Requirements and Characteristics for Coupling A Hydrogen Production Plant to A High-Temperature Nuclear Reactor*, IBL/Ext-05-00453, Idaho National Laboratory, Idaho Falls, ID, June 2005.
7. V. Dostal et al., *A Supercritical Carbon Dioxide Cycle for Next Generation Nuclear Reactors*, MIT-ANP-TR-100, Massachusetts Institute of Technology, Boston, MA, March 2004.
8. S. J. Ball et al., *Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTS)—Volume 2: Accident and Thermal Fluids Analysis PIRTS*, NUREG/CR-6944, Vol. 2 (ORNL/TM-2007/147, Vol. 2), Oak Ridge National Laboratory, Oak Ridge, TN, March 2008.
9. P. M. Williams et al., *Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, U.S. Nuclear Regulatory Commission, Washington, DC, March 1989.
10. S. J. Ball et al., *Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTS)—Volume 2: Accident and Thermal Fluids Analysis PIRTS*, NUREG/CR-6944, Vol. 2 (ORNL/TM-2007/147, Vol. 2), Oak Ridge National Laboratory, Oak Ridge, TN, March 2008.
11. "Prismatic HTGR Core Design Description," in *HTGR Technology Course for the Nuclear Regulatory Commission, Module 5A, May 24–26, 2010*, Idaho National Laboratory and General Atomics (2010).
12. S. L. Dixon, *Fluid Mechanics and Thermodynamics of Turbomachinery*, Fifth Ed, Elsevier-Butterworth-Heinemann, New York, NY, 1998.
13. X. Yan, *Dynamic Analysis and Control System Design for an Advanced Nuclear Gas Turbine Power Plant*, Massachusetts Institute of Technology: Cambridge, MA, June 1990.
14. R. L. Panton, *Incompressible Flow*, Second Ed., John Wiley & Sons, New York, NY, 1995.
15. M. N. Özışık, *Basic Heat Transfer*, McGraw-Hill, Inc., New York, 1977.
16. W. M. Kays and A. L. London, *Compact Heat Exchangers*. 3rd Ed., McGraw-Hill, New York, 1984.
17. H. M. Hashemian, *Sensor Performance and Reliability*, International Society of Automation (ISA), Research Triangle Park, NC, 2005.

18. *RELAP5-3D*© Code Manual, Volume I: Code Structure System Models and Solution Methods, INEEL-EXT-98-00834, Idaho National Laboratory, Idaho Falls, Idaho, June 2005.
19. C. B. Davis and C. H. Oh, "The Addition of Noncondensable Gases into RELAP5-3D for Analysis of High Temperature Gas-Cooled Reactors," on *Proceedings of 2003 RELAP5 International Users*, August 27–29, 2003, Yellowstone, MT.
20. R. A. Riemke et al., "RELAP5-3D Code Includes Athena Features and Models," in *Proceedings of ICONE14, International Conference on Nuclear Engineering, July 17–20, 2006, Miami, FL*.
21. W. L. Weaver et al., "An Executive Program for Use With RELAP5-3D," in *Proceedings of the 2001 RELAP5 Users Seminar, September 5–8, 2001, Sun Valley, ID*.
22. D. L. Aumiller et al., "A Coupled RELAP5-3D/CFD Methodology with a Proof-of-Principle Calculation, in *Proceedings of the 2000 International RELAP5 Users Seminar, September 12–14, 2000, Jackson Hole, WY*.
23. N. Anderson et al., "Analysis of the Hot Gas Flow in the Outlet Plenum of the Very High-Temperature Reactor Using Coupled RELAP5-3D System Code and a CFD Code," *Nuclear Engineering and Design*, 238, pp. 274–279 (2008).
24. P. Bayless, "VHTR Thermal-Hydraulic Scoping Analyses Using RELAP5-3D/Athena," in *Proceedings of the 2003 Global Conference, November 16–20, 2003, American Nuclear Society Winter Meeting*.
25. P. D. Bayless, "Prismatic Core VHTR Analysis Using RELAP5-3D/Athena," presented to Idaho National Engineering and Environmental Laboratory, August 28, 2003, Idaho Falls, ID.
26. P. Sabharwall et al., "Temperature Effect on Heated Region Flow Starvation for Gas-Cooled Reactors," in *American Nuclear Society Annual Meeting, June 5–8, 2005, San Diego, CA*.
27. J. E. Fisher and C. B. Davis, "RELAP5-3D Compressor Model," in *Proceedings of the 2005 Space Nuclear Conference, June 5–9, 2005, San Diego, CA*.
28. A. C. Devuono and R. N. Christensen, "Experimental Investigation of The Pressure Effect on Film Condensation of Steam-Air Mixture at Pressure Above Atmospheric Fundamentals of Phase Change: Boiling and Condensation," *ASME-HTD*, 38, pp. 73–80 (1984).
29. K. Schneider, "Siemens Contributions to RCP Modeling and Evaluation of UPTF Test 6," in *Proceedings of the ICAP Meeting, October 18–20, 1989, Bethesda, MD*.
30. *RELAP5-3D*© Code Manual, Volume II: User's Guide and Input Requirements, INEEL-EXT-98-00834, Idaho National Laboratory, Idaho Falls, ID, June 2005.
31. P. E. Macdonald et al., "The Next Generation Nuclear Plant—Insights Gained from the INEEL Point Design Studies," in *Proceedings of ICAPP-04, June 13–17, 2004: Pittsburgh, PA*.
32. N. E. Todreas and P. Hejzlar, *Flexible Conversion Ratio Fast Reactor Systems Evaluation—Final Report*, MIT-NFC-PR-101, Massachusetts Institute of Technology, Boston, MA, June 2008.
33. K. Gezelius, *Design of Compact Intermediate Heat Exchangers for Gas Cooled Fast Reactors*, MIT-ANPTR-103, Massachusetts Institute of Technology, Boston, MA, May 2004.
34. J. Hesselgreaves, *Compact Heat Exchangers: Selection, Design, and Rating*, 1st Ed., Pergamon Press, San Diego, CA, 2001.
35. C. H. Oh et al., "Design Option of Heat Exchanger for the Next Generation Nuclear Plant," *Journal of Engineering for Gas Turbines and Power*, 132(032903-1) (March 2010).
36. *Heatric*™, [Company Web Site], Available from: [Http://www.Heatric.Co.Uk](http://www.Heatric.Co.Uk).

37. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Kluwer Academic Publishers, Boston, MA, 1999.
38. R. O. Gauntt et al., *MELCOR Computer Code Manuals—Vol. 1*, NUREG/CR-6119, Vol. 1, U.S. Nuclear Regulatory Commission, Washington, DC, October 2000.
39. S. B. Rodriguez et al., *Development of Design and Simulation Model and Safety Study of Large-Scale Hydrogen Production Using Nuclear Power*, SAND-2007-6218, Sandia National Laboratories, Albuquerque, NM, October 2007.
40. J.-M. Tournier and M. S. El-Genk, *Models of Turbine and Compressor Units for MELCOR Secondary System Modules*, UNM-ISONPS-2-2006, University of New Mexico's Institute for Space and Nuclear Power Studies, Albuquerque, NM, August 2006.
41. J.-M. Tournier and M. S. El-Genk, "Axial Flow, Multi-Stage Turbine and Compressor Models," *Energy Conversion and Management*, 51, pp. 16–29 (2010).
42. D. G. Ainley and G. C. R. Mathieson, *A Method of Performance Estimation for Axial-Flow Turbines*, Reports and Memoranda No. 2974, British Aeronautical Research Council, December 1951.
43. C. R. Hyman, "Containment Calculations of Debris Conditions Adjacent to the BWR Mark-1 Drywell Shell During the Later Phases of a Severe Accident," *Nuclear Engineering and Design*, 121(3), pp. 379–393 (1990).
44. J. Zhu and S. A. Sjolander, "Improved Profile Loss and Deviation Correlations for Axial-Turbine Blade Rows, in *Proceedings of GT2005 ASME Turbo Expo 2005: Power for Land, Sea, and Air. June 6–9, 2005*, American Society of Mechanical Engineers, Reno-Tahoe, NV, pp. 783–792 (2005).
45. J. H. Horlock, "Losses and Efficiencies in Axial-Flow Turbines," *International Journal of Mechanical Science*, 2, pp. 48–75 (1960).
46. L. Fielding, *Turbine Design—The Effect on Axial Flow Turbine Performance of Parameter Variation*, ASME Press, New York, NY, pp. 130–132 (2000).
47. C. C. Koch and J. L. H. Smith, "Loss Sources and Magnitudes in Axial-Flow Compressors," *Journal of Engineering for Power*, A98, pp. 411–424 (1976).
48. S. Lieblein, "Loss and Stall Analysis in Compressor Cascades," *Journal of Basic Engineering*, 81, pp. 387–400 (September 1959).
49. R. H. Aungier, *Axial-Flow Compressor—A Strategy for Aerodynamic Design and Analysis*. ASME Press, New York, NY, pp. 118–152 (2003).
50. S. Kakaç and H. Liu, *Heat Exchangers—Selection, Rating, and Thermal Design*, CRC Press, New York, pp. 35–38 and pp. 73–138 (1998).
51. J. P. V. Doormaal and G. D. Raithby, "Enhancements of the Simple Method for Predicting Incompressible Fluid Flows," *Numerical Heat Transfer*, 7, pp. 147–163 (1984).
52. B. S. Petukhov, "Heat Transfer and Friction in Turbulent Pipe Flow with Variable Physical Properties," in *Advances in Heat Transfer*, Academic Press, New York, NY, pp. 503–564 (1970).
53. V. Gnielinski, "New Equations for Heat and Mass Transfer in Turbulent Pipe and Channel Flow," *International Chemical Engineering*, 16(2), pp. 359–368 (1976).
54. L. C. Brown et al., *High Efficiency Generation of Hydrogen Fuels Using Nuclear Power*, GA-A24285, Rev. 1, General Atomics, December 2003.

55. C. Huang and A. T-Raissi, "Analysis of Sulfur-Iodine Thermochemical Cycle for Solar Hydrogen Production, Part I: Decomposition of Sulfuric Acid," *Solar Energy* 2005, 78, pp. 632–646 (2005).
56. D. W. Oxtoby and N. H. Nachtrieb, *Principles of Modern Chemistry*, Saunders College Publishing, Philadelphia, PA, 1986.
57. Y. H. Jeong et al., *Optimization of the Hybrid Sulfur Cycle for Hydrogen Generation*, MIT Report MIT-NES-TR-004, MIT, Cambridge, MA, 2005.
58. C. Forsberg et al., "Sulfur Thermochemical Processes With Inorganic Membranes to Produce Hydrogen," in *3rd Topical Conference on Fuel Cell Technology (Embedded Topical)*, 2004 American Institute of Chemical Engineers Spring National Meeting, 2004, New Orleans, LA.
59. J. Larminie and A. Dicks, *Fuel Cell Systems Explained*, 2nd Ed., Wiley, New York, 2003.
60. H. C. No, *PBR System Simulation Code for Depressurization Accident Analysis in a Modular Pebble Bed*, Technical Report, Massachusetts Institute of Technology, Boston, MA, 2001.
61. S. B. Rodriguez et al., "Transient Analysis of Sulfur-Iodine Cycle Experiments and Very High Temperature Reactor Simulations Using MELCOR-H2," *Nuclear Technology*, 166, pp. 76–85 (April 2009).
62. K. J. Hogan, *Pebble Bed Modular Reactor Analysis with MELCOR*, Purdue University, West Lafayette, IN, 2006.
63. J. Dunham and P. M. Came, "Improvements to the Ainley-Mathieson Method of Turbine Performance Prediction," *Journal of Engineering for Power*, 92, pp 252–256 (1970).
64. S. C. Kacker and U. Okapuu, "A Mean Line Prediction Method for Axial Flow Turbine Efficiency," *Journal of Engineering for Power*, 104, pp. 111–119 (January 1982).
65. M. W. Benner et al., "An Empirical Prediction Method for Secondary Losses in Turbines—Part I: A New Loss Breakdown Scheme and Penetration Depth Correlation," *Journal of Turbo-Machinery*, 128, pp. 273–280 (2006).
66. M. W. Benner et al., "An Empirical Prediction Method for Secondary Losses in Turbines—Part II: A New Secondary Loss Correlation," *Journal of Turbo-Machinery*, 128, pp. 281–291 (2006).
67. H. Schlichting, *Boundary Layer Theory*, 7th Ed., McGraw-Hill Book Company, New York, NY, 1979.
68. M. I. Yaras and S. A. Sjolander, "Prediction of Tip-Leakage Losses in Axial Turbines," *Journal of Turbo-Machinery*, 114, pp. 204–210 (1992).
69. T. Matsunuma, "Effects of Reynolds Number and Freestream Turbulence on Turbine Tip Clearance Flow," *Journal of Turbo-Machinery*, 128, pp. 166–177 (2006).
70. R. H. Aungier, *Turbine Aerodynamics—Axial-Flow and Radial-Inflow Turbine Design and Analysis*, ASME Press, New York, NY, 69–79, 2006.
71. D. G. Wilson, *The Design of High-Efficiency Turbo-Machinery and Gas Turbines*, The Massachusetts Institute of Technology (MIT) Press, Cambridge, MA, Chapter 7, pp. 239–278, and Chapter 8, pp. 282–328, 1984.
72. K. M. Boyer and W. F. O'Brien, "An Improved Streamline Curvature Approach for Off-Design Analysis of Transonic Axial Compression Systems," *Journal of Turbo-Machinery*, 127, pp. 475–481 (2003).

DRAFT

APPENDIX A: PRESSURE LOSS COEFFICIENT IN TURBINE BLADES

The following text is largely the same as Rodriguez³⁹. It is slightly reorganized and abridged from the original.

Over the past 50 years, a number of turbine mean-line loss models have been described in the open literature. Perhaps the best known and most completely documented model is that of Ainley and Mathieson published in 1951⁴². This model includes correlations for all loss components (i.e., profile losses, secondary losses, trailing edge losses, and tip clearance (leakage) losses). It is a testimony to the soundness of the Ainley and Mathieson (AM) approach that it has become the foundation for a number of subsequent refinements, most notably those by Dunham and Came⁶³, Kacker and Okapuu⁶⁴, and Benner et al.^{65, 66} for modern, subsonic axial turbines with highly loaded airfoils. The present model capitalizes on the latest refinements proposed by Benner but still relies heavily on the foundation work of Ainley and Mathieson.

In the following, all parameters (such as Reynolds and Mach numbers) are evaluated using the relative gas flow velocities, unless otherwise specified. The total pressure loss coefficient is the sum of the coefficients for profile losses, secondary losses, trailing edge losses, and tip clearance (leakage) losses:

$$Y = (Y_p + Y_s) + Y_{TE} + Y_{TC} . \quad Y = (Y_p + Y_s) + Y_{TE} + Y_{TC} . \quad (\text{A-1})$$

The major contribution of Benner et al.^{65, 66} has been the description of the profile and the secondary losses in a more physical and accurate way. One of the physically unsatisfactory assumptions done in the previous conventional loss schemes was the uniformity of the loss generated in the airfoil surface boundary layer across the span, which produces erroneous values of the secondary loss component. Benner proposed a new loss scheme, which requires a correlation for the spanwise penetration depth of the passage vortex separation line ($Z_{TE} < H/2$) at the trailing edge:

$$(Y_p + Y_s) = (1 - Z_{TE} / H) \times Y'_p + Y'_s . \quad (\text{A-2})$$

The profile loss coefficient is an improvement over that by Kacker and Okapuu,⁶⁴ based on more recent turbine cascade data⁴⁴:

$$Y'_p = 0.914 \times [K_{in} Y'_{p,AM} K_p + Y_{shock}] \times \left(\frac{Re_{2C}}{2 \times 10^5} \right)^{K_{RE}} , \quad (\text{A-3})$$

where

$K_{in} = 0.825$ for axial entry nozzles, $K_{in} = 2/3$ for reaction blades, and

$K_{Re} = -0.575$ for $Re_{2C} = (\rho_2 W_2 C) / \mu_2 < 2 \times 10^5$.

The term, $Y'_{p,AM}$, is the Ainley-Mathieson profile loss coefficient which will be defined in Eq. (A-5) and the Y_{shock} is the shock coefficient which will be defined in Eq. (A-8).

The Mach number correction factor in Eq. (A-3) is calculated by the formula given by Kacker and Okapuu⁶⁴:

$$K_p = 1 - K_2 \times (1 - K_1), \quad (\text{A-4a})$$

where

$$K_1 = 1 \text{ for } Ma_2 \leq 0.2, \quad (\text{A-4b})$$

$$K_1 = 1 - 1.25 \times (Ma_2 - 0.2) \text{ for } Ma_2 > 0.2, \text{ and} \quad (\text{A-4c})$$

$$K_2 = (Ma_1 / Ma_2)^2. \quad (\text{A-4d})$$

The profile loss coefficient, $Y'_{p,AM}$, introduced by Ainley and Mathieson is an interpolation between the results of two special sets of cascade tests ($\beta_1 = 0$ and $\beta_2 = \phi_2$):

$$Y'_{p,AM} = \left\{ Y_{p,AM}^{(\beta_1=0)} + \left| \frac{\beta_1}{\phi_2} \right| \left(\frac{\beta_1}{\phi_2} \right) \left[Y_{p,AM}^{(\beta_1=\alpha_2)} - Y_{p,AM}^{(\beta_1=0)} \right] \right\} \times \left(\frac{t_{\max} / C}{0.2} \right)^{K_m \beta_1 / \phi_2}, \quad (\text{A-5a})$$

where

$$K_m = +1 \quad \text{for } t_{\max} / C \leq 0.2, \quad (\text{A-5b})$$

$$K_m = -1 \quad \text{for } t_{\max} / C > 0.2. \quad (\text{A-5c})$$

The results of Ainley and Mathieson, for a cascade with ($\beta_1 = 0$ and $t_{\max} / C = 0.2$) are also well correlated by (see Fig. A-1):

$$Y_{p,AM}^{(\beta_1=0)} = 0.13 + \frac{S}{C} \left[A + \frac{S}{C} \left(B + C \times \frac{S}{C} \right) \right], \quad (\text{A-6a})$$

where the coefficients A , B , and C^* are functions of the TE relative gas flow angle:

$$A = -0.275862 - 0.0173298 \times \cos(7.49775 \times \phi_2 - 285.4), \quad (\text{A-6b})$$

$$B = -4.28277 \times 10^{-7} \times \phi_2^4 + 1.11388 \times 10^{-4} \times \phi_2^3 - 1.02971 \times 10^{-2} \times \phi_2^2 + 0.401733 \times \phi_2 - 5.38018, \quad (\text{A-6c})$$

$$C = 2.31562 \times 10^{-7} \times \phi_2^4 - 6.25296 \times 10^{-5} \times \phi_2^3 + 5.9553 \times 10^{-3} \times \phi_2^2 - 0.237718 \times \phi_2 + 3.32301. \quad (\text{A-6d})$$

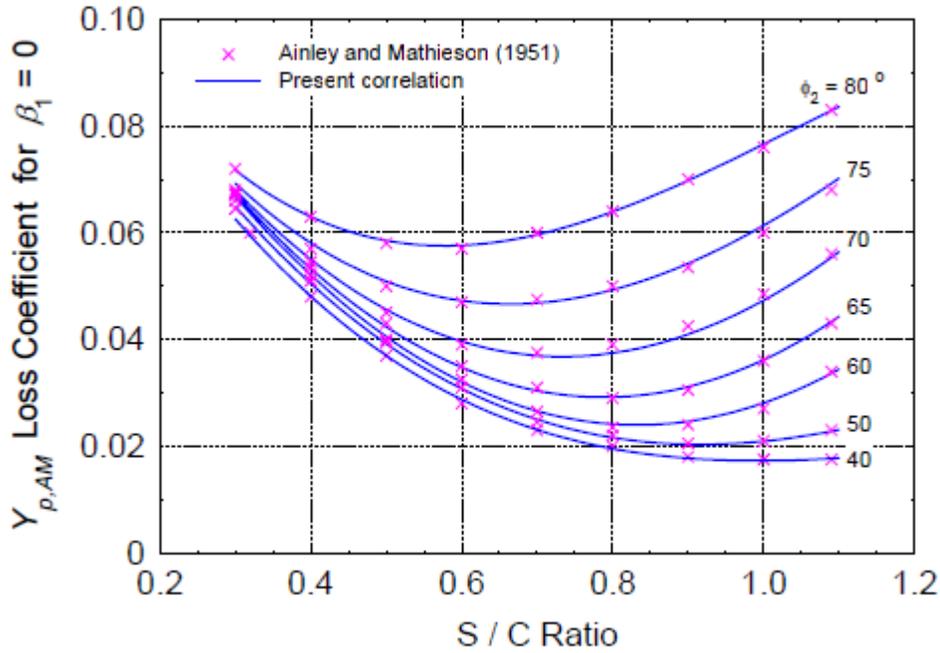


Fig. A-1. Profile loss coefficient for $(\beta_1 = 0$ and $t_{max}/C = 0.2$)⁴².

The results reported by Ainley and Mathieson for cascades with $(\beta_1 = 0$ and $t_{max}/C = 0.2)$ are well correlated by (see Fig. A-1):

*The notation in the reference document³⁹ regarding the C parameter is not clear, but it appears C is used to represent two different quantities in the same equation. Based on context, we believe that S/C is an input parameter representing the ratio of blade pitch to chord length, whereas C in the numerator of the last term is a different local variable for the correlation and is defined in Eq. (A-6d). Perhaps the fonts for the two variables are different but, if so, the difference is small and the intention is of the author is not obvious.

$$Y_{p,AM}^{(\beta_1=\alpha_2)} = 0.31 + \frac{S}{C} \left[-0.776 + \frac{S}{C} \left(B + C \times \frac{S}{C} \right) \right], \quad (\text{A-7a})$$

where the coefficients B and C are function of the TE relative gas flow angle:

$$B = 3.52951 \times 10^{-4} \times \phi_2^2 - 2.9723 \times 10^{-2} \times \phi_2 + 1.40393, \quad (\text{A-7b})$$

$$C = -2.31614 \times 10^{-4} \times \phi_2^2 + 2.00615 \times 10^{-2} \times \phi_2 - 0.670492. \quad (\text{A-7c})$$

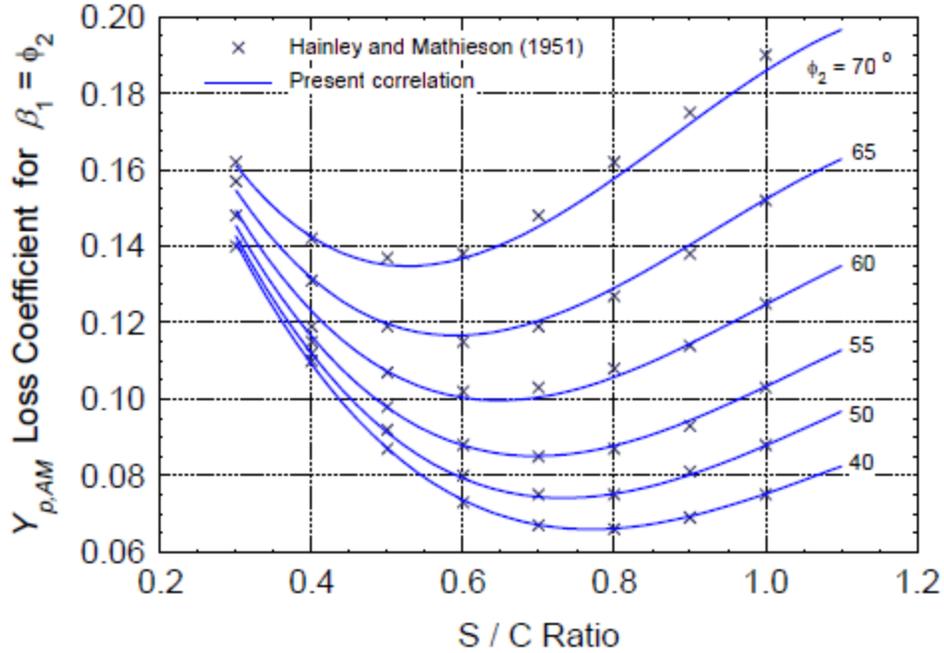


Fig. A-2. Profile loss coefficient for ($\beta_1 = \phi_2$ and $t_{\max}/C = 0.2$).⁴²

These results for cascades with a maximum blade thickness of ($t_{\max}/C = 0.2$) are corrected for different thicknesses using the last factor on the right side of Eq. (A-5a). Note that all the angles in these formulas are in degrees.

Cascade tests in the decades following the publication of the Ainley and Mathieson loss model have revealed that the profile loss coefficient is generally dependent on the Mach number, even in the subsonic flow regime. Compressibility can affect Y_p in two ways, by causing shocks at blade leading edges and by affecting the flow acceleration within blade channels [the correction factor K_p in Eq. (A-3)]. The shock losses can occur at relatively low average inlet Mach numbers, due to the local flow acceleration adjacent

to the highly curved leading edges. These losses, appearing in Eq. (A-3), are calculated by formula give by Kacker and Okapuu⁶⁴:

$$Y_{shock} = \frac{\rho_1 W_1^2}{\rho_2 W_2^2} \times \frac{r_{hub}}{r_{tip}} \times \frac{3}{4} (Ma_1^{hub} - 0.4)^{1.75} \quad \text{when } Ma_1^{hub} > 0.4, \quad (\text{A-8a})$$

$$Y_{shock} = 0 \quad \text{when } Ma_1^{hub} \leq 0.4. \quad (\text{A-8b})$$

For the flow to be in equilibrium, the gas flow and pressure must vary radially. The incident Mach number, always higher at the hub radius than at the midspan radius, is related to the mean incident Mach number by Kacker and Okapuu⁶⁴:

$$\frac{Ma_1^{hub}}{Ma_1} = \begin{cases} 5.751579 \times \left(\frac{r_{hub}}{r_{tip}}\right)^2 - 10.8509 \times \left(\frac{r_{hub}}{r_{tip}}\right) + 6.15292, & \frac{r_{hub}}{r_{tip}} \leq 0.95 \\ 1.0, & \frac{r_{hub}}{r_{tip}} > 0.95 \end{cases} \quad (\text{A-9a})$$

for a reaction stage (rotor), and

$$\frac{Ma_1^{hub}}{Ma_1} = \begin{cases} 4.07224 \times \left(\frac{r_{hub}}{r_{tip}}\right)^2 - 6.64366 \times \left(\frac{r_{hub}}{r_{tip}}\right) + 3.70492, & \frac{r_{hub}}{r_{tip}} \leq 0.8 \\ 1.0, & \frac{r_{hub}}{r_{tip}} > 0.8 \end{cases} .$$

(A-9a)

Figure A-3 shows the fitted correlation and the experimental data of Kacker and Okapuu

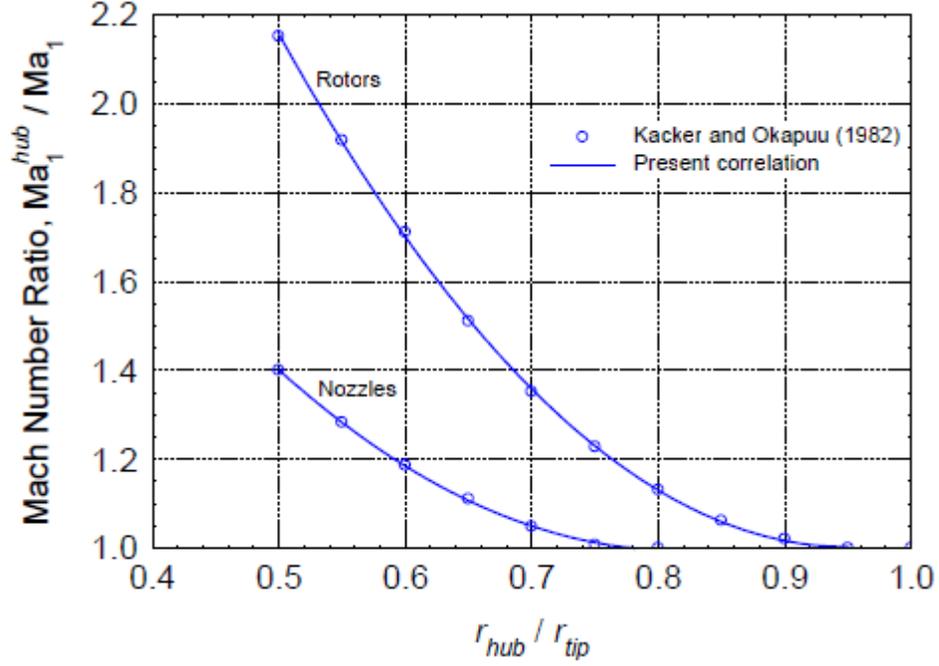


Fig. A-3. Inlet Mach number ratio for turbine blades.⁶⁴

The spanwise penetration depth (Z_{TE}) of the separation line between the primary and the secondary loss regions, appearing in Eq. (A-2), is given by Benner⁶⁵:

$$\frac{Z_{TE}}{H} = \frac{0.10(F_t)^{0.79}}{\sqrt{CR} \times (H/C)^{0.55}} + 32.7 \left(\frac{\delta^*}{H} \right)^2, \quad (\text{A-10})$$

where the tangential loading parameter, F_t , is given by:

$$F_t = 2 \frac{S}{C_x} \times \cos^2(\phi_m) \times [\tan(\phi_1) + \tan(\phi_2)], \quad (\text{A-11})$$

and the mean velocity vector angle is given by:

$$\tan(\phi_m) = \frac{1}{2} [\tan(\phi_1) + \tan(\phi_2)]. \quad (\text{A-12})$$

The convergence ratio in Eq. (A-10) is given as $CR = \cos \phi_2 / \cos \phi_1$.

The boundary layer displacement thickness at the inlet endwall, δ^* , in Eq. (A-10), is given by Schlichting⁶⁷:

$$\delta^* = \frac{\delta}{8} = \frac{0.0463x}{(\rho_1 W_{1x} / \mu_1)^{0.2}}. \quad (\text{A-13})$$

Assuming a power-law turbulent velocity profile with an exponent of 1/7. The reference length, x , in Eq. (B-13) is taken as half the blade axial chord (i.e., $x = C_x/2$).

The secondary losses coefficient in Eq. (A-2) is given by Benner et al.⁶⁶:

$$Y'_s = \frac{0.038 + 0.41 \times \tanh(1.2\delta^*/H)}{\sqrt{\cos\Phi} \times CR \times (H/C)^{0.55} \times (C \cos\phi_2 / C_x)^{0.55}} \text{ when } H/C \leq 2.0, \quad (\text{A-14a})$$

$$Y'_s = \frac{0.052 + 0.56 \times \tanh(1.2\delta^*/H)}{\sqrt{\cos\Phi} \times CR \times (H/C) \times (C \cos\phi_2 / C_x)^{0.55}} \text{ when } H/C > 2.0, \quad (\text{A-14b})$$

Again, all the angles in these formulas are in degrees.

The trailing edge losses, representing the pressure losses due to TE blockage, are expressed in terms of the blockage itself (i.e., the ratio of trailing edge thickness to the throat opening of the cascade itself). Kacker and Okapuu⁶⁴ expressed these losses in terms of the kinetic energy loss coefficient, $\Delta\Phi_{TE}$, for axial entry nozzles ($\beta_1 = 0$) and impulse blades ($\beta_1 = \phi_2$), as shown in Fig. A-4. The difference lies in the thicknesses of the profile boundary layers at the trailing edges of blades: impulse blades, with their thick boundary layers, have lower trailing edge losses. The trailing edge thickness contributes significantly to the drag of highly accelerating cascades. For blades other than the two types shown in Fig. A-3, the loss coefficient for the trailing edge kinetic energy losses is interpolated in a manner similar to Eq. (A-5a) as Kacker and Okapuu⁶⁴:

$$\Delta\Phi_{TE} = \Delta\Phi_{TE}^{(\beta_1=0)} + \left| \frac{\beta_1}{\phi_2} \right| \left[\Delta\Phi_{TE}^{(\beta_1=\alpha_2)} - \Delta\Phi_{TE}^{(\beta_1=0)} \right], \quad (\text{A-15a})$$

where

$$\Delta\Phi_{TE}^{(\beta_1=0)} = 0.595628 \times \left(\frac{t_{TE}}{O} \right)^2 + 0.122642 \times \left(\frac{t_{TE}}{O} \right) - 2.27958 \times 10^{-3} \quad (\text{A-15b})$$

for an axial entry nozzle (Fig. A-4), and

$$\Delta\Phi_{TE}^{(\beta_1=\alpha_2)} = 0.310658 \times \left(\frac{t_{TE}}{O}\right)^2 + 0.0656168 \times \left(\frac{t_{TE}}{O}\right) - 1.43176 \times 10^{-3}. \quad (A-15c)$$

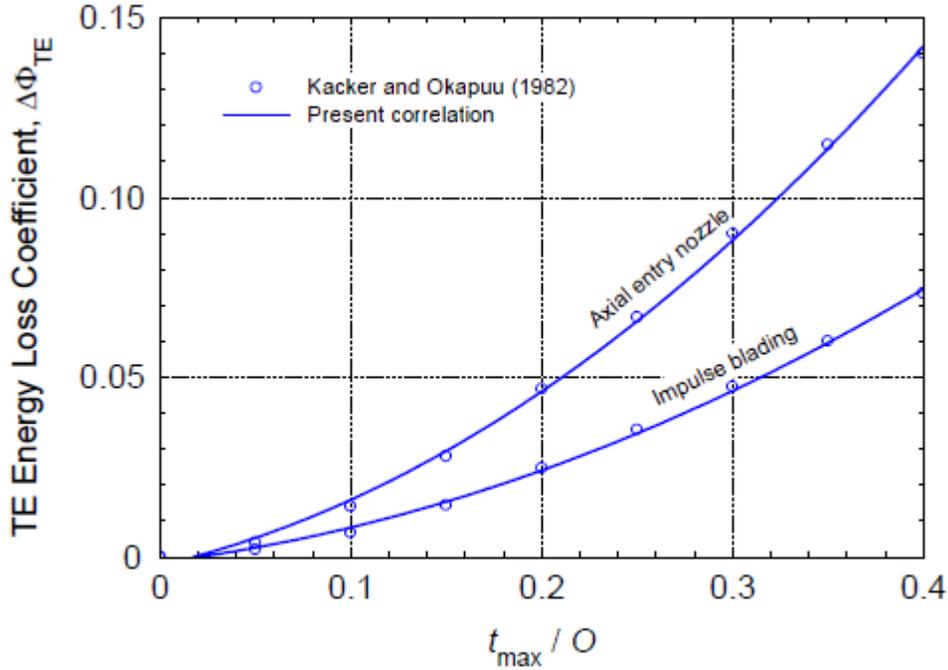


Fig. A-4. Loss coefficient for trailing edge losses, based on Kacker and Okapuu.⁶⁴

for an impulse blading (Fig. A-4). The kinetic energy loss coefficient, $\Delta\Phi_{TE}$, is converted to a pressure loss coefficient using the following relationship:

$$Y_{TE} = \frac{\left\{ 1 - \frac{\gamma-1}{2} Ma_2^2 \left(\frac{1}{1-\Delta\Phi_{TE}} - 1 \right) \right\}^{-\gamma/(\gamma-1)} - 1}{1 - \left(1 + \frac{\gamma-1}{2} Ma_2^2 \right)^{-\gamma/(\gamma-1)}}. \quad (A-15d)$$

Because a turbine operates with some clearance between the tips of the rotor blades and the casing, a fraction of the fluid leaks across the tips, causing a reduction in turbine work output. Yaras and Sjolander⁶⁸ and Matsunuma⁶⁹ reviewed existing methods for predicting the tip-leakage losses in the light of detailed studies conducted recently in turbine cascades. The improved model proposed by Yaras and Sjolander⁶⁸ states:

$$Y_{TC} = Y_{tip} + Y_{gap}, \quad Y_{TC} = Y_{tip} + Y_{gap}, \quad (A-16a)$$

where the tip leakage losses are given by:

$$Y_{tip} = 1.4K_E \frac{C}{S} \times \frac{\tau}{H} \times \frac{\cos^2 \phi_2}{\cos^3 \phi_m} \times C_L^{1.5}, \quad (\text{A-16b})$$

and the gap losses, contributing a smaller amount to the overall end loss, are given by:

$$Y_{gap} = 0.0049K_G \frac{C}{S} \times \frac{C}{H} \times \frac{\sqrt{C_L}}{\cos \phi_m}. \quad (\text{A-16c})$$

The blade lift coefficient, C_L , is given by Ainley and Mathieson⁴² as:

$$C_L = 2 \frac{S}{C} \times \cos(\phi_m) \times [\tan(\phi_1) + \tan(\phi_2)]. \quad (\text{A-17})$$

For midloaded blades $K_E = 0.5$ and $K_G = 1.0$, and for front- or aft-loaded blades $K_E = 0.566$ and $K_G = 0.943$ Yaras and Sjolander⁶⁸.

In off-design conditions, the pressure loss coefficient in Eq. (A-1) is modified to include an additional term, K_{inc} , which

$$Y = K_{inc} \times (1 - Z_{TE} / H) \times Y_p' + Y_s' + Y_{TE} + Y_{TC} \quad (\text{A-18})$$

Aungier⁷⁰ fit the experimental data of Ainley and Mathieson⁴² to the following functions:

$$\text{When } i < 0, \quad K_{inc} = 1 + 0.52 \times |i / i_s|^{1.7} \quad (\text{A-19})$$

$$\text{When } i \geq 0, \quad K_{inc} = 1 + |i / i_s|^{2.3 + 0.5 \times i / i_s} \quad (\text{A-20})$$

Figure A-5 shows K_{inc} as a function of the ratio of the incidence angle, $i = \phi_1 - \beta_1$, to the stalling incidence angle, i_s ,

$$i_s(\phi_2, \xi, S / C) = i_{SR}(\phi_2, \xi) + \Delta i_s(\phi_2, S / C) \quad (\text{A-21})$$

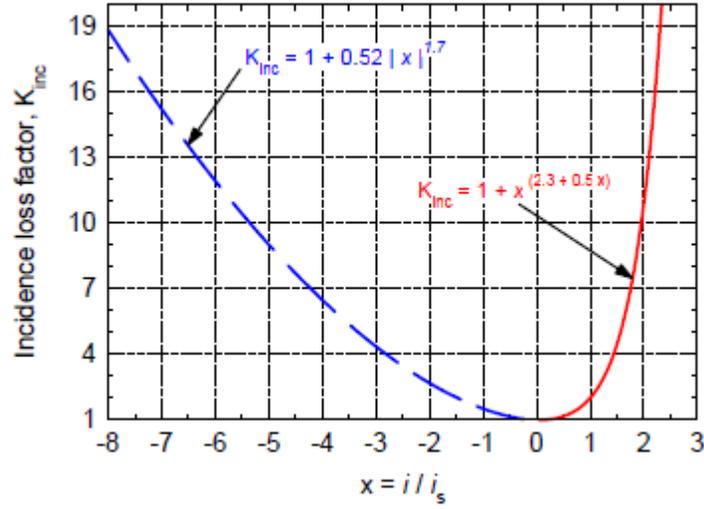


Fig. A-5. Off-design incidence correction factor for turbine blades.⁷⁰

An upper limit of $K_{inc} = 20$ is required in the model.

The stalling incidence angle, i_s , is a function of ϕ_2 , $\xi = \beta_1 / \phi_2 S / C$, ϕ_2 , $\xi = \beta_1 / \phi_2$, and S / C , the ratio of blades pitch to chord length. It is calculated as the sum of a reference value, $i_{SR}(\phi_2, \xi)$ corresponding to a blade cascade with $S / C = 0.75$, and a correction term, $\Delta i_s(\phi_2, S / C)$ to adjust for other values of pitch-to-chord ratio:

A correlation for stalling incidence angle proposed by Aungier⁷⁰ from fitting the experimental data of Ainley and Mathieson⁴⁹ is given by the following formulae:

$$\text{When } \phi_2 \geq 50^\circ, \quad i_{SR}(\phi_2, \xi) = i_{s0} + A - B\xi^2 + D\xi^3 + E\xi^4, \quad (\text{A-22})$$

$$\text{where } i_{s0} = 20 - \frac{(\xi + 1)}{0.11}, \quad \text{where } i_{s0} = 20 - \frac{(\xi + 1)}{0.11}, \quad (\text{A-23})$$

$$A = 61.8 - (90^\circ - \phi_2) \times \left[1.6 - \frac{(90^\circ - \phi_2)}{165} \right], \quad (\text{A-24})$$

$$B = 71.9 - (90^\circ - \phi_2) \times 1.69, \quad (\text{A-25})$$

$$D = 7.8 - (90^\circ - \phi_2) \times \left[0.28 - \frac{(90^\circ - \phi_2)}{320} \right], \quad (\text{A-26})$$

$$E = 14.2 - (90^\circ - \phi_2) \times \left[0.16 + \frac{(90^\circ - \phi_2)}{160} \right], \quad (\text{A-27})$$

$$\text{When } \phi_2 < 50^\circ \quad i_{SR}(\phi_2, \xi) = |i_{SR}(50^\circ, \xi) - i_{So}| \times \frac{(55 - 90 + \phi_2)}{15}. \quad (\text{A-28})$$

Figure A-6 shows the stalling incidence angle for $S/C = 0.75$, as a function of ξ and ϕ_2 ,

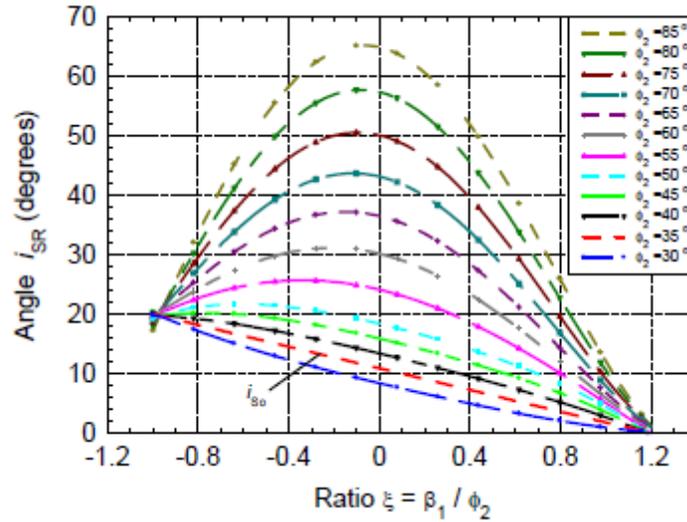


Fig. A-6. Stalling incidence angle for $S/C=0.75$.⁷⁰

The correlation by Aungier⁷⁰ of the correction term, $\Delta i_S(\phi_2, S/C)$, is given by the following equations.

$$\text{When } S/C < 0.8, \quad \Delta i_S = -38X - 53.5X^2 - 29X^3, \quad (\text{A-29})$$

where $X = S/C - 0.75$.

$$\text{When } S/C \geq 0.8, \quad \Delta i_S = -2.0374 - (S/C - 0.8) \times \left[69.58 - \left| \frac{90^\circ - \phi_2}{14.48} \right|^{3.1} \right]. \quad (\text{A-30})$$

DRAFT

APPENDIX B: PRESSURE LOSS COEFFICIENT IN COMPRESSOR BLADES*

In this appendix, the factors for the pressure loss factor of a compressor are evaluated[†]. All parameters (such as Reynolds and Mach numbers) are evaluated using the relative gas flow velocities, unless otherwise specified.

The total pressure loss coefficient in Sect. 5.11.3 is the sum of coefficients for profile losses and tip clearance (leakage) losses:

$$Y = K_{inc} \times (Y_p + Y_{TC}) . \quad (\text{B-1})$$

The secondary losses and end-wall losses are not accounted for in this work for the axial compressor cascades. Horlock and Denton⁴⁵ report that, in the 1950s, investigators like W. R. Hawthorne and L. H. Smith made substantial progress in understanding fluid mechanics of secondary flow in axial compressors, but that attempts to integrate this work into design methods were not very successful. The challenges of modeling secondary and clearance losses were dominant then, and indeed remain so to this day.⁴⁵ In compressors, the classical secondary flow is not as strong as in axial turbines, because the gas turning angle is much smaller in the former. A small gas turning angle is used in compressors to avoid separation of the boundary layer in a positive pressure gradient field.

The profile loss coefficient, Y_p , is determined using the approach of Koch and Smith⁴⁷. Their model for Y_p , an improvement to that proposed by Lieblein⁴⁸, is still regarded as one of the most comprehensive.^{71, 72} It accounts for the actual momentum thickness and trailing edge shape factor of the fully turbulent boundary layer, and for the effects of flow area contraction, Reynolds number, and Mach number on these parameters. Lieblein⁴⁸ had shown that the losses around the blade profile appear as a boundary-layer momentum thickness, θ_{TE} , at the trailing edge, and in the wake, θ_2 , ($\theta_2 > \theta_{TE}$ in highly loaded blades because there is a mixing loss as the suction-surface and pressure-surface boundary layers join to form the wake). Lieblein⁴⁸ also showed that as the aerodynamic loading on a compressor blade increased, the diffusion on the suction surface increased, but that on the pressure surface stayed approximately constant. This prompted this investigator to define an “equivalent diffusion ratio” D_{eq} , as:

$$D_{eq} = \frac{\text{Peak relative velocity on the suction surface}}{\text{Outlet relative velocity, } W_2} > 1, \quad (\text{B-2})$$

and to propose a correlation for this ratio, as a function of blade solidity and inlet and outlet flow angles ϕ_1 and ϕ_2 . Koch and Smith⁴⁷ introduced additional factors correlating the airfoil maximum thickness ratio,

*This section is taken nearly verbatim from Rodriguez.³⁹ The purpose of including it is to provide the engineering design information used in the compressor model.

[†]The Rodriguez document³⁹ does not define a formula for the tip clearance loss factor, Y_{TC} . Presumably, the formula for turbines may be used.

t_{\max}/C , and the streamtube contraction ratio, A_2/A_1 . These authors also used cascade data with boundary layers of higher turbulence levels than those of Lieblein, more representative of the conditions encountered in a modern compressor. Based on their work, Koch and Smith⁴⁷ correlated the equivalent diffusion ratio as:

$$D_{eq} = \frac{W_1}{W_2} \times \left[1 + K_3 \frac{t_{\max}}{C} + K_4 \Gamma^* \right] \times \sqrt{\left(\sin \phi_1 = K_1 \frac{C}{S} \Gamma^* \right)^2 + \left(\frac{\cos \phi_1}{A_{throat}^* \times \rho_{throat} / \rho_1} \right)^2}, \quad (\text{B-3})$$

where the contraction ratio is given by:

$$A_{throat}^* = \left[1.0 - \frac{K_2 \frac{C}{S} \left(\frac{t_{\max}}{A_1} \right)}{\cos(0.5(\phi_1 + \phi_2))} \right] \frac{A_{throat}}{A_1}. \quad (\text{B-4a})$$

The cascade throat area is assumed to occur at one-third of the axial chord:

$$A_{throat} = A_1 - \frac{1}{3}(A_1 - A_2). \quad (\text{B-4b})$$

The gas density at the throat is calculated as:

$$\frac{\rho_{throat}}{\rho_1} = 1 - \frac{\text{Ma}_{x_1}^2}{1 - \text{Ma}_{x_1}^2} \left(1 - A_{throat}^* - K_1 \frac{\tan \phi_1 C}{\cos \phi_1 S} \Gamma^* \right), \quad (\text{B-4c})$$

and the square of the axial Mach number at the inlet as:

$$\text{Ma}_{x_1}^2 = \frac{W_{x_1}^2}{\gamma RT_1} = \frac{(W_1 \cos \phi_1)^2}{\gamma RT_1}. \quad (\text{B-4d})$$

Koch and Smith⁴⁷ obtained the values of the constants in these equations from their experimental data: $K_1 = 0.2445$, $K_2 = 0.4458$, $K_3 = 0.7688$, and $K_4 = 0.6024$. The dimensionless blade circulation parameter in Equations (B-3) and (B-4c) is given by:

$$\Gamma^* = \frac{r_{1m}V_{\theta 1} - r_{2m}V_{\theta 2}}{\left(\frac{r_{1m} + r_{2m}}{2}\right)\frac{C}{S} \times W_1} = \frac{r_{1m}V_1 \sin \alpha_1 + r_{2m}V_2 \sin \alpha_2}{\left(\frac{r_{1m} + r_{2m}}{2}\right)\frac{C}{S} \times W_1}. \quad (\text{B-5})$$

Note that the absolute gas velocities are used in the numerator of Eq. (B-5), not the relative velocities.

Based on Koch and Smith's experimental data at $Re_1 = 106$, the boundary-layer momentum thickness at the blade outlet is correlated in this work as (Fig. B-1):

$$\frac{\theta_2^o}{C} = [0.072 \times D_{eq} - 0.0032] \times [1.0 + 0.2234 \times (D_{eq} - 1.0)^6]. \quad (\text{B-6})$$

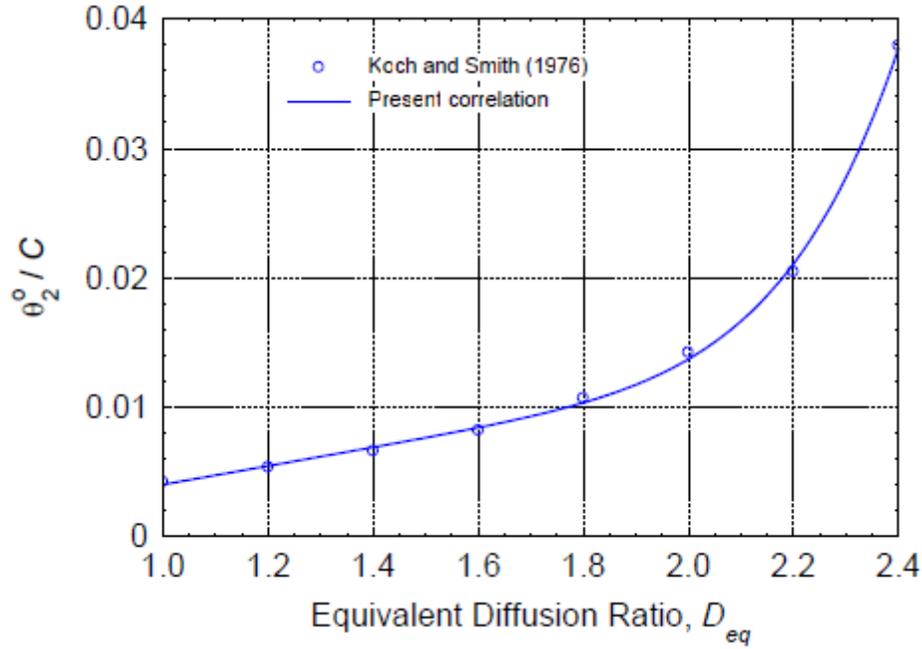


Fig. B-1. Boundary layer momentum thickness at blade outlet, $Re_1=10^{6.47}$

$$H_{TE}^o = \frac{\delta_{TE}^*}{\theta_2^o} = 1.231 + D_{eq}^3 \times (0.0476 + 0.00207 \times D_{eq}^6). \quad (\text{B-7})$$

The values of θ_2^o and H_{TE}^o are obtained for the following nominal conditions:

- no contraction of the flow annulus height, h ;

- b. an inlet Reynolds number of $Re_1 = \rho_1 W_1 C / \mu_1 = 10^6$; and
- c. hydraulically smooth blades.

Koch and Smith⁴⁷ gave correction factors for conditions other than nominal. For the boundary-layer momentum thickness, they proposed:

$$\frac{\theta_2}{C} = \left(\frac{\theta_2^o}{C} \right) \times \zeta_M \times \zeta_H \times \zeta_{Re} \quad (\text{B-8a})$$

The correction factor for inlet Mach number (Fig. B-2) is correlated as:

$$\zeta_M = 1.0 + (0.117569 - 0.169832 \times D_{eq}) \times Ma_1^n \quad (\text{B-8b})$$

with an exponent:

$$n = 2.8532 + D_{eq} (-0.977474 + 0.194771 \times D_{eq}) \quad (\text{B-8c})$$

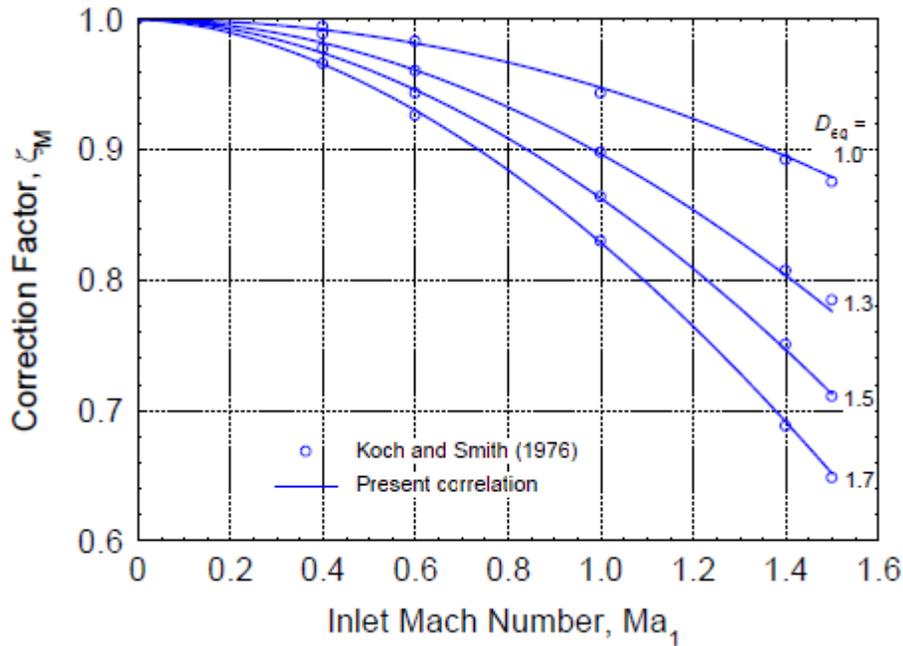


Fig. B-2. Correction factor for effect of Mach number on boundary-layer momentum thickness.⁴⁷

The correction factor for flow area contraction (Fig. B-3) is a linear function given by:

$$\zeta_H = 0.53 \frac{H_1}{H_2} + 0.47, \quad (\text{B-8d})$$

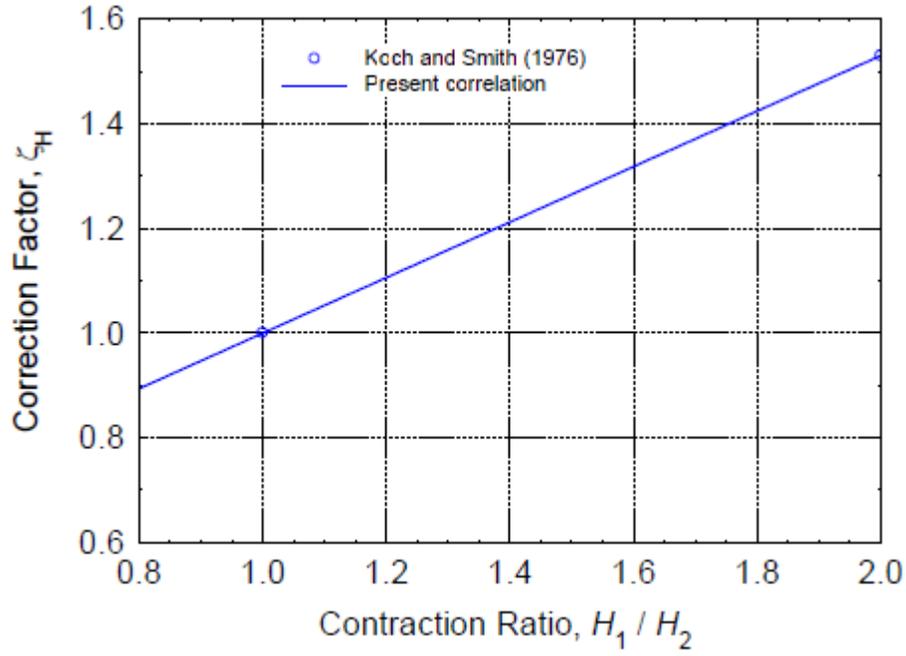


Fig. B-3. Correction factor for effect of flow area contraction on boundary layer momentum thickness.⁴⁷

The correction factor for inlet Reynolds number is given by:

$$\zeta_{\text{Re}} = \begin{cases} \left(\frac{10^6}{\text{Re}_1} \right)^{0.166}, & \text{Re}_1 \geq 2 \times 10^5, \\ 1.30626 \times \left(\frac{2 \times 10^5}{\text{Re}_1} \right)^{0.5}, & \text{Re}_1 < 2 \times 10^5. \end{cases} \quad (\text{B-8e})$$

Similarly, Koch and Smith⁴⁷ corrected the trailing edge boundary-layer shape factor as:

$$H_{TE} = H_{TE}^o \times \zeta_M \times \zeta_H \times \zeta_{\text{Re}}. \quad (\text{B-9a})$$

The correction factor for inlet Mach number (Fig. B-2) is given by:

$$\zeta_M = 1.0 + \left[1.07247 + D_{eq} \times (-0.86098 + 0.180425 \times D_{eq}) \right] \times \text{Ma}_1^{1.8} . \quad (\text{B-9b})$$

The correction factor for the flow area contraction (Fig. B-3) is calculated as:

$$\zeta_H = 1.0 + \left(\frac{H_1}{H_2} - 1.0 \right) \times (0.0026 \times D_{eq}^8 - 0.024) , \quad (\text{B-9c})$$

and the correction factor for inlet Reynolds number is given by:

$$\zeta_{\text{Re}} = \left(\frac{10^6}{\text{Re}_1} \right)^{0.06} . \quad (\text{B-9d})$$

The values of θ_2 and H_{TE} , obtained from Eqs. (B-8a) and (B-9a) for each blade row, can be used in the following relation, due to Lieblein⁴⁸, to obtain the final result for the blade-profile total pressure loss coefficient:

$$K_p = \frac{\Delta \hat{P}_{loss}}{\rho_1 \frac{W_1^2}{2}} = 2 \left(\frac{\theta_2}{S \cos \phi_2} \right) \times \left(\frac{\cos \phi_1}{\cos \phi_2} \right)^2 \times \left(\frac{2H_{TE}}{3H_{TE} - 1} \right) \times \left[1 - \left(\frac{\theta_2}{C} \right) \frac{C}{S} \frac{H_{TE}}{S \cos \phi_2} \right]^{-3} . \quad (\text{B-10})$$

The correction factor, K_{inc} , in Eq. (B-1) is given by

$$\begin{aligned} \text{When } \xi < -2, & \quad K_{inc} = -4\xi - 3 \\ \text{When } -2 \leq \xi \leq 1, & \quad K_{inc} = 1 + \xi^2 \\ \text{When } 1 < \xi, & \quad K_{inc} = 2\xi \end{aligned} . \quad (\text{B-11})$$

Figure B-4 shows the correction factor, K_{inc} , as a function of the dimensionless parameter, ξ .

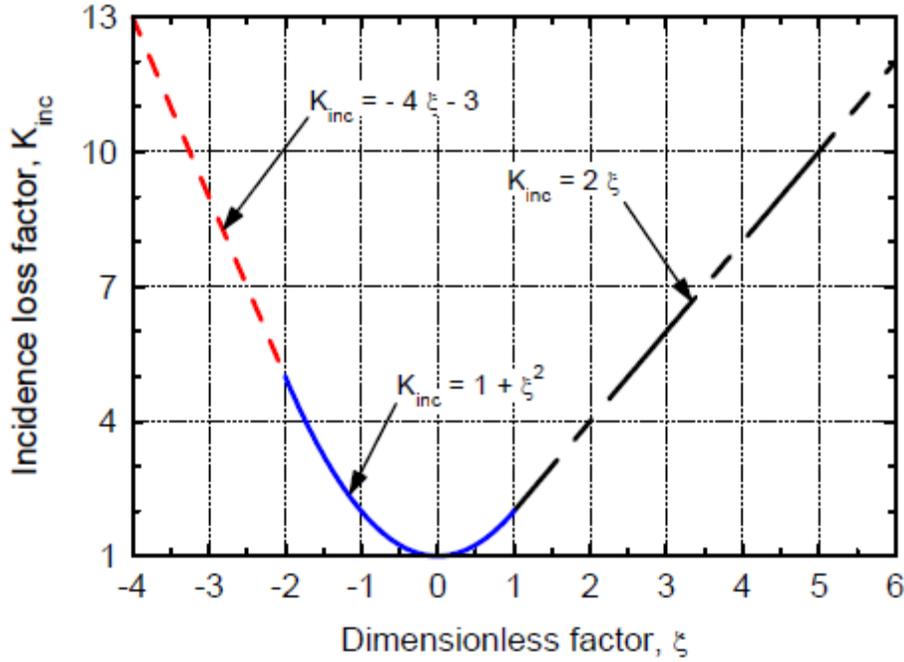


Fig. B-4. Off-design incidence correction factor for compressor blades.⁴⁹

An upper limit of $K_{inc} = 20$ is required in the model. The parameter ξ is a function of the incidence angle, $i = \phi_1 - \beta_1$, optimum angle of attack i^* , and positive (i_s) and negative (i_c) stall incidence angles, as:

$$\begin{aligned} \text{When } i \geq i^*, \quad \xi &= -\frac{i - i^*}{i_s - i^*} \geq 0; \\ \text{When } i < i^*, \quad \xi &= \frac{i - i^*}{i^* - i_c} < 0. \end{aligned} \quad (2.1-1)$$

The incidence loss factor at the positive and negative stall incidence angles is defined such that the cascade losses are twice those at optimum design conditions (i.e., at $i = i_s$ or $i = i_c$), then $K_{inc} = 2.0$.

The optimum design angle of attack, i^* , is a function of the blades and cascade geometry⁴⁹:

$$i^* = \Phi - \beta_1 + \left[3.6K_t - 0.3532\zeta \times \left(\frac{Z}{C} \right)^{0.25} \right] \times \left(\frac{C}{S} \right)^{0.65 - 0.002\zeta} \quad (2.1-2)$$

where Φ is the blade stagger angle ($^\circ$) and $\zeta = |\beta_1 - \beta_2|$ is the absolute camber angle ($W_{10} = V_{10} - U_1 = V_1 \sin \alpha_1 - U_1$).

The maximum blade thickness correction factor is given by:

$$Y_{TC} = Y_{tip} + Y_{gap} \quad (2.1-3)$$

where

$$Y_{tip} = 1.4K_E \frac{C}{S} \times \frac{\tau}{H} \times \frac{\cos^2 \phi_2}{\cos^2 \phi_m} \times C_L^{1.5} \quad (B.4)$$

and the gap losses, contributing a smaller amount to the overall end loss, are given by:

$$Y_{gap} = 0.0049K_G \frac{C}{S} \times \frac{C}{H} \times \frac{\sqrt{C_L}}{\cos \phi_m} \quad (B.5)$$

For midloaded blades, $K_E = 0.5$ and $K_G = 1.0$. For front or aft-loaded blades, $K_E = 0.566$ and $K_G = 0.943$ ⁶⁸

DRAFT

Letter Report

TASK 4—ADVANCED CONTROL AND PROTECTION SYSTEM DESIGN METHODS

T. L. Wilson, Jr., R. A. Kisner, and R. T. Wood
Oak Ridge National Laboratory

February 2012

Project JCN N6177

Technical Monitor: Y. Yang, NRC RES
Principal Investigator: T. L. Wilson, Jr., ORNL

Prepared for the
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

	Page
LIST OF FIGURES	v
LIST OF TABLES	v
1. INTRODUCTION	1
1.1 Project Overview	1
1.2 Task Objectives.....	2
1.3 Task Context	2
1.4 Organization of Report.....	3
2. MODERN CONTROL METHODS	5
2.1 Continuous Control Methods	5
2.1.1 Classical control	5
2.1.2 Linear matrix optimal control	6
2.1.3 Model predictive control	6
2.1.4 Nonlinear control	6
2.1.5 Intelligent control	7
2.1.6 Adaptive control.....	7
2.1.7 Genetic algorithms	8
2.1.8 Multimode control.....	8
2.1.9 Hierarchical supervisory control	8
2.1.10 Resilient control	9
2.2 Discrete Control Methods	9
2.2.1 Expert systems	9
2.2.2 Intelligent agent-based control	10
2.2.3 Nonmathematical flow methods.....	10
2.2.4 Formal methods.....	11
2.2.5 Object-oriented control	11
2.3 Hybrid Control Methods	11
3. NGNP PROTECTION STRATEGY	13
3.1 Design Basis Events.....	13
3.1.1 Anticipated operational occurrences	14
3.1.2 Accidents.....	16
3.2 Plant protection system functions	19
3.2.1 Reactivity control	20
3.2.2 Engineered safety features	20
3.2.3 Shutdown cooling system (possibly investment protection rather than ESF).....	21
3.2.4 Reactor cavity cooling system (RCCS).....	21
3.2.5 Containment/confinement structure	21
3.2.6 Moisture removal	22

3.3	Instrumentation and controls for protection system functions	22
3.3.1	Reactor scram logic	23
3.3.2	RCCS.....	23
3.3.3	Circulator trip logic	23
3.3.4	Circulator start inhibit logic	24
3.3.5	Rod withdrawal prohibition logic	24
3.3.6	Reserve shutdown system and safety shutdown cooling system logic.....	24
3.3.7	Steam/water dump.....	24
3.3.8	Steam generator isolation	24
3.3.9	Confinement vessel pressure and filtration flow logic	25
4.	NGNP CONTROL STRATEGY	27
4.1	Normal Operating Conditions	27
4.1.1	Load follow	27
4.1.2	Maximum ramp	27
4.1.3	Step change	28
4.2	Operational Controls	28
4.2.1	Startup and shutdown	29
4.2.2	Normal operation	29
5.	KEY CONTROL AND PROTECTION DESIGN METHOD ISSUES FOR NGNP	35
5.1	Issues in Protection Systems	35
5.2	Issues in Control Systems	35
5.2.1	Advanced control design methods	35
5.2.2	Support system controls	36
5.3	System Classification	36
6.	REFERENCES	39

LIST OF FIGURES

Figure		Page
1	Two-level cascade controller with demand output.....	30
2	Two level control with increase/decrease output.....	31

LIST OF TABLES

Table		Page
1	Comparison of traditional computer programming with intelligent agents.....	10
2	Cascade control schemes for three HTGRs	33

TASK 4—ADVANCED CONTROL AND PROTECTION SYSTEM DESIGN METHODS

LETTER REPORT

T. L. Wilson, Jr., R. A. Kisner, and R. T. Wood
Oak Ridge National Laboratory

February 2012

1. INTRODUCTION

1.1 Project Overview

The objective of the project designated as Job Control Number (JCN) N6177 is to support the U.S. Nuclear Regulatory Commission (NRC) in identifying and evaluating the regulatory implications concerning the control and protection systems proposed for use in the U.S. Department of Energy's (DOE's) Next Generation Nuclear Plant (NGNP). The NGNP, using gas-cooled reactor technology, will provide the basis for the commercial industry to manage the heat for energy production and industrial processing including hydrogen production. The high temperature gas-cooled reactor (HTGR) can provide heat for industrial process at much higher temperatures than conventional light-water reactors, from 700 to 950°C. (Note that for the upper range of these operating temperatures the HTGR is sometimes referred to as the Very High Temperature Reactor or VHTR. In this project, the gas-cooled reactor design for the NGNP is referred to as the VHTR even though DOE's current plans focus on the lower end of the above-noted temperature range for ultimate deployment of NGNP.)

The JCN N6177 project involves five tasks, which are titled:

- Task 1. Control and Protection Systems in VHTRs for Process Heat Applications
- Task 2. Highly Automated Control Room Design
- Task 3. Models for Control and Protection System Designs
- Task 4. Advanced Control and Protection System Design Methods
- Task 5. Develop Technical Guidance and Acceptance Criteria for Safety-Related Protection and Control Systems Designs

The overall objective of this research is to review potential technologies likely to be employed for the control and protection system design for the VHTR for process heat applications including possibly hydrogen production. The investigation also addresses modeling methods and plant models, including multimodular models, as well as the level of automation that can be achieved and the degree of integration in control room designs that may result. In addition, this research examines such design aspects and issues as prediction of the state and effect of control systems actions, overall resilience of the control and protection systems designs, and fault detection capability. The culminating activity, to the extent possible based on the maturity of the VHTR design and particular process heat application, is to assist NRC in developing technical guidance and acceptance criteria for these safety-related protection and control systems designs for the VHTR.

1.2 Task Objectives

The overall objective of Task 4 is to investigate advanced control and protection methodologies that may be employed in the VHTR. This task uses the background information on gas reactors collected in Task 1 to anticipate the topics of protection and control that may come under review. The task seeks specifically to identify and investigate possible new topics or issues for review that are not common with previously licensed plants.

This task is closely related to both Task 1 and Task 2. Task 1 gathered background information on previously designed gas-cooled reactors utilizing graphite moderator and ceramic fuel. The Task 1 report (Wilson et al.¹) extracted the control and protection features, issues, and experience from the surveyed literature. Most of the designs reviewed in Task 1 also were built and operated and provide operating information on control and protection. Task 2 reviewed the potential impacts of a highly automated control room (Wood et al.²). Task 2 leveraged findings from another research task of the same name (JCN N6350, *Guidelines for the Design of Highly Integrated Control Rooms*) in which advances in the automation were reviewed for potential impacts on licensing of the new power plants currently being licensed. Task 2 applied these insights specifically to the NGNP design.

This research examines the larger role played by the control and protection system through the use of enhanced automation, potential for propagation of disturbances through integrated functionality, and greater reliance on control functions to respond to off-normal conditions in the plant. The use of advanced control design techniques expands the role for automatic functions of the control and protection systems to address prediction of the state and effect of control systems actions, overall robustness of the control and protection systems designs, and fault detection capability.

1.3 Task Context

The stated objective of Task 4 in the project plan is to investigate control and protection strategies that may be important for a VHTR used for hydrogen production. As the project progressed, it became clear that the original goal of preparing for hydrogen production was no longer the most likely primary application for the NGNP. The objective has shifted toward what seems more likely at this point, that is, a VHTR plant that is coupled through a steam generator to a conventional steam turbine/electrical generator. In comparison to a more radical hydrogen production plant, the steam generator driven electrical plant is an incremental step in gas-cooled reactor design development. This increment provides experience with the gas-cooled primary and ceramic core coupled to a conventional steam generator and reduces the technical challenges in developing high temperature materials that would be necessary to produce hydrogen. Alternate plant configurations still being considered involve a VHTR driving a general process heat plant (not necessarily a hydrogen production plant) or a combined cycle with an electrical plant and a process heat plant. The types of process heat applications include oil refining, oil recovery from shale or tar deposits, and process heat for chemical plants. Issues and requirements for separation and decoupling the nuclear island and the process heat plant and their respective safety systems are considered in broad terms.

The most probable initial implementation of the NGNP is a single, stand-alone unit for demonstration and proof of principle. Following the standalone demonstration unit, multimodular configurations are considered to be the next step in the design's evolution to commercial viability. The Task 2 report addresses operational considerations related to multiple units. However, control issues, such as the propagation of disturbances between multiple units, must be addressed by the control design methods employed for NGNP.

At this stage of VHTR development, the investigation under Task 4 is necessarily based on a hypothetical design because no actual design is either in existence or proposed in any detail. Concepts and directions of development are apparent, but a great deal of the design is, at present, unspecified. This letter report is

used to collect the unique properties of VHTRs that affect the designs and must be understood by licensing reviewers emphasizing differences with respect to conventional plants. The emphasis in this report is in applicability and interpretation in light of likely VHTR designs that may be proposed in the future. This letter report, along with the companion reports from the other tasks under this project, can serve as a reference for NRC reviewers.

1.4 Organization of Report

The Task 4 report covers control and protection strategies for the NGNP. The report is focused primarily on the baseline design. In the absence of a proposed design, Section 2 of the report covers modern control methods that may be used and discusses the general attributes of those methods and, to the extent possible, specific features that are useful for the NGNP controls. Section 3 covers the protection system for the baseline NGNP. It addresses the design basis events, safety functions and I&C that may be used to implement the safety functions. Section 4 reviews the control systems that are required for the baseline and general properties of those systems. Section 5 identifies issues in the control and protection systems for NGNP that may be different from previously licensed reactors.

2. MODERN CONTROL METHODS

In the nuclear power industry, single-input, single-output (SISO) classical control has been the primary control design method applied to individual control loops. Multivariate control, such as three element controllers for U-tube steam generators of pressurized-water reactors (PWRs), has been employed in some cases. In very limited instances, an integrated control strategy has been devised to coordinate the action of individual control loops based on an overall control goal. Modern control methods can enable approaches to plant control that invoke more extensive automation capabilities to provide enhanced fault tolerance and result in increased plant operational efficiency.

The application of most advanced techniques to nuclear power control system design has primarily been through simulation as part of research by universities and national laboratories. Some of the techniques employed in controls application research for both power and research reactors include adaptive robust control for the Experimental Breeder Reactor II (EBR-II), fuzzy logic control for power transitions, H-infinity control and genetic algorithm-based control for steam generators, neural network control for power distribution in a reactor core, and supervisory control for multi-modular reactors. A useful compendium of findings from such research activities is found in the proceedings of a series of Topical Meetings on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies sponsored by the American Nuclear Society.³⁻⁹

While design details for the control systems of the NGNP have not been developed, DOE program documentation indicates that the use of advanced control capabilities is being considered.¹⁰ In the Task 2 report, Wood et al.² describe automation technologies and discuss the impact of and associated issues with a highly integrated control room design for NGNP. In particular, the report describes resilient control strategies providing robust fault tolerance and anticipatory event management as well as autonomous control approaches based on integrated supervisory control with embedded diagnostic and decision-making capabilities. These automation technologies embody extensive usage of modern control design methods. This chapter describes key modern control design methods to provide a basis for discussing the NGNP approach to plant control and protection.

2.1 Continuous Control Methods

Continuous systems, which are characterized by differential or partial differential equations, are controlled through feedback from proportionally measuring sensors to achieve an output setpoint value. Continuous feedback control is a simple servo or regulator since the output value is automatically maintained to a setpoint without constant human intervention. As an example, maintaining core outlet temperature to a specific setpoint is a continuous control task. The greatest body of control theory literature and tools has been developed for continuous system control.

2.1.1 Classical control

Classical or proportional-integral-derivative (PID) control compares the output of a process with a setpoint to generate an error signal from which an actuator signal is produced to control the process. The method may be used in combination with feedback and feed-forward configurations. Part of the error signal may be augmented by mathematical derivative or integral action to improve performance; hence the integral and derivative parts of the name. PID is almost always used in SISO control, that is, a single sensor sends a signal to a controller that results in action on a single actuator. This form of control works well in many processes. However, performance and stability suffer for processes that are inherently multivariable, nonlinear, or exhibit large parameter swings or structural changes. Tuning PID controllers is based primarily on rule of thumb methods rather than a mathematically optimized calculation of gain.

2.1.2 Linear matrix optimal control

The linear matrix approach to control, which is based on linear state-space equations, has the benefit of many available mathematical tools for analysis, synthesis, and simulation. One of the tool sets allows the optimization of performance parameters by minimizing or maximizing objective performance criteria (i.e., optimal control). Another tool permits the application of robust methods, which lowers the potential of instability due to noise or uncertainty in plant parameters. Linear matrix methods include Linear Quadratic Gaussian (LQG), H-infinity, and Linear Quadratic Gaussian with Loop Transfer Recovery (LQG/LTR). A definite benefit of matrix-based representation is the inherent ability to handle multivariate systems. The weakness, however, with linear methods is the limited dynamic range over which performance is guaranteed. The common approach to design is to linearize the nonlinear system around a nominal operating point, which limits valid operation to a more or less small neighborhood around the operating point. Changes in plant parameters directly influence their performance, which can necessitate the need for adaptive control as an adjunct to linear matrix control. In many cases, performance is sacrificed for robustness. Linear matrix methods do not permit easy field adjustment by plant operations personnel compared with classic PID controls because of multivariate inputs and outputs and the complex mathematical gain calculations required.

2.1.3 Model predictive control

Model predictive control (MPC) is one of the predominant optimal control methods, with its ease of understanding and effective performance leading to increasingly extensive usage for industrial applications. The MPC method¹¹ involves multivariate control in which an optimum control action is calculated based on current process measurements, a dynamic model of the plant/process, the history of prior control actions, and an optimization cost function into the future over a receding prediction horizon.

The MPC method starts with the state space form of a plant model that is then algebraically manipulated to cast the equations into the predictive form in which the state variable is eliminated. The predictive form of the equations depends on the current state of the system (an initial condition) and all future inputs, but not explicitly on the predicted states. For a given set of present and future control actions, the future behavior of the state variables are predicted over a prediction horizon while present and future control actions are computed to minimize the quadratic objective function. Out of the group of future control actions that are calculated, only the first control action is implemented. The predictive feature of the controller has an anticipatory effect that is reflected in the current control action. These calculations are repeated in the next time step by appending the next measurement to the data set. The progressively updated measurement sets compensate for unmeasured disturbances and model inaccuracies, both of which result in the measured system output being different from that predicted by the model. The MPC requires the on-line solution of an optimization problem to compute optimal control inputs over the time horizon. The MPC iteratively calculates a sequence of future control signals by minimizing a multistage cost function defined over a prediction horizon.

The advantage of the method for the industrial applications is the capability to account for constraints imposed on the control action and the state variables through limits and targets associated with the cost function minimization. This feature, plus the provision of feedforward and feedback elements in a unified but relatively simple mathematical structure, enables MPC-based control designs to address fast actuation demands, large time delays, and high-order dynamics.

2.1.4 Nonlinear control

Nonlinear control refers to a wide range of control methods that contain nonlinear terms to represent for plant dynamics more accurately. Unlike linear matrix control which can be rigorously solved and shown to be stable, the nonlinear control field is broad and unstructured because of the lack of sufficiently

general proofs and design algorithms. Topics that pertain to nonlinear control include chaos (theory) control, Lyapunov methods, describing functions compensation for dead zone, higher-order effects, and step/jump discontinuities, synchronization, and heterodyning. Stability is not as mathematically simple to predict with nonlinear control compared with linear systems. Simulation is regarded as the primary testing method.

One of the more useful forms of nonlinear control is the scheme of Tao and Kokotović for representing the nonlinearity as a set of piecewise linear functions.¹² The scheme deals with each linear piece in much the same way as linear controls and then handles the transitions across region boundaries. The problems of system identification of the linear regions and adaptive control have been solved as part of the system.

2.1.5 Intelligent control

The methods that are often classified with intelligent control are based on analogies to biological and cognitive models of control and behavior. Examples are expert systems, fuzzy systems, and neural networks, which are discussed below. (Expert systems are discussed under discrete-event control.)

2.1.5.1 Fuzzy logic control

Fuzzy logic is a multivalued logic that allows intermediate values to be defined between conventional evaluations like *yes/no*, *true/false*, *black/white*, etc. Notions like *rather warm* or *pretty cold* can be converted into mathematical expressions that can be processed by computers. In this way, an attempt is made to apply a more human-like way of thinking in the programming of computers. Values of variables are not restricted to a single set but may have degrees of membership across multiple sets. Ultimately, internal fuzzy variables must be made crisp values to control the outside world. This step is called defuzzification. An example defuzzifier is the *Mamdani* controller, which is based on calculating the centroid of fuzzy outputs. Fuzzy control is suited for very complex processes, when there is no simple mathematical model, highly nonlinear processes, and if the processing of (linguistically formulated) expert knowledge is to be performed. Fuzzy control is not recommended if conventional control theory yields a satisfactory result, and an easily solvable and adequate mathematical model already exists. Fuzzy logic as a discipline originated in 1965 by Lotfi A. Zadeh, professor for computer science at the University of California in Berkeley.

2.1.5.2 Neural network control

In its simplest form, artificial neural network (ANN) control, which is loosely modeled after human neurons, maps multiple input values to outputs that become signals to actuator devices. At the heart of the network are layers of cross-connections between input and output ports. The weighting values and activation threshold function at each connection determine the function of the network that is somewhat analogous to the neuron model. The mappings (i.e., the connections and weighting values) are learned through a series of training sessions, which may be supervised or unsupervised, and deterministic or stochastic. A network can have feedforward and feedback connections internally. The function that ANNs perform is distributed across its plexus of connections. This distribution offers tolerance for error and noise at the input. Neural networks are useful for vector functions. Two issues always arise in certain applications: (1) ANNs by their nature cannot be examined to determine their functional properties as one might analyze the gain coefficients of a PID controller and (2) ANNs will always give seemingly plausible results even when operation has extrapolated beyond the range of all training.

2.1.6 Adaptive control

Direct and indirect model-based controls are used to accomplish adaptive control, in which the control system adjusts to changing characteristics of the controlled plant to maintain satisfactory stability and performance. Adaptive control methods are very often combined with other control types to permit stable

performance over wide ranges and conditions. In all instances some form of plant model is needed to permit adaptation. Model-based control, which contains dynamic models representing the system being controlled, is based on differential equations derived either from first principles or through system identification techniques. In a direct model-based control scheme, the mathematical model simulates the real process in faster-than-real time. Thus the behavior of a variety of control actions can be simulated, analyzed, and an optimum path chosen. The direct implementation is prohibitively computer intensive for any sufficiently complex system, which leads to indirect model based methods.

The indirect methods use (simplified) mathematical models embedded in the control system to permit adaptation of control gains and coefficients. Examples include self-tuning, which has become popular in single channel PID controllers. A more complex implementation is inverse control, which incorporates an inverse model of the plant or component to be controlled that tames its nonlinearities and dynamics. Convergence becomes an issue in model tuning and adaptation.

2.1.7 Genetic algorithms

Genetic algorithms are used for search and optimization functions making them suited for certain types of control systems. Genetic algorithms are unique systems based on the supposed functioning of living organisms. The method of application differs from classical optimization algorithms in the following ways:

1. use of the encoding of the parameters, not the parameters themselves;
2. work on a population of points, not a unique individual;
3. use the only values of the function to optimize not their derived function or other auxiliary knowledge; and
4. use probabilistic transition functions not determinist ones.

The functioning of such an algorithm does not guarantee success in finding an optimum. In a stochastic system for example, the genetic pool may be too far from the solution. Also, a too rapid convergence may halt the process of evolution. Nevertheless, these algorithms have proven to be efficient in applications as diverse as the stock market forecasting, production scheduling, or programming of automotive industry assembly robots.

2.1.8 Multimode control

Combinations of differing continuous signal control methods can yield useful results for certain hard-to-control processes. The combinations may range from simple to complex. The ability to simultaneously achieve desired performance and stability is improved by wisely applying several control methodologies. Although specifics depend on the system to be controlled, the overall scheme is to allow several carefully chosen control algorithms (usually based on differing methods, e.g., neural network, linear feedback control, and a model-based algorithm) to process in parallel then choose command signals from one to operate plant actuators. Variations in output command selection include pre-designation of specific regimes or conditions over which certain controllers capture control and mixing of all command signals by yet another controller (e.g., fuzzy controller or a command validation algorithm). Permitting adaptation of all the controllers over time enhances the concept. Additionally, sliding mode control, which is a variable structure control, is an often-used form of multimode control.

2.1.9 Hierarchical supervisory control

In most large-scale, loosely-coupled systems, the entire system is too large to be solved as a single multivariate system. Instead, the control is decentralized into subsystems that are internally closely

coupled, but loosely coupled to one another. The subsystems must be coordinated to achieve system-wide performance. Hierarchical supervisory control, whose purpose is to achieve total plant coordination, permits individual decentralized process control by local controllers while exercising top-down coordination across multiple process controllers. The coordination achieves an optimization of materials and energy flow by adjusting local controller setpoints and other parameters. Coordination also involves switching of controller operational modes (e.g., during maintenance cycles). Automated start up and shutdown as well as system-wide diagnostics are possible with supervisory control. Often hierarchical control involves both continuous and discrete-mode control methods (see hybrid control below).

2.1.10 Resilient control

The concept of resiliency has been developed through control theory research to address issues such as disturbances, failure events, errors, incorrect human operation, and cyber attacks.¹³ A resilient control system is defined as “one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected or malicious nature.”¹⁴ In this sense, state awareness involves knowledge of conditions and parameters relevant to control decisions, including an understanding of the status of the process being controlled and the control system itself. Essentially, a resilient control system constitutes a whole-plant, supervisory control system with extended capabilities. Key features include anticipation of failures or disturbances followed by adaptation to mitigate the potential consequences as well as perception of events and conditions followed by responsive action to ensure safety, stability, and performance. The approach to automation enabled by resilient control is discussed in more detail by Wood, et al.²

2.2 Discrete Control Methods

Discrete event systems are characterized by a finite collection of specific, distinct states and the transitions between them. These systems are controlled by applying logic through combinational and sequential rules. These are not proportional systems (c.f., continuous control). Often, the control of these systems is left to schemes based on heuristic rules inferred from practical plant operation. Industrial plants regularly use programmable logic controllers (PLCs) to achieve event control. These commercially available controllers, which are programmed in ladder logic, offer limited intelligence and do not integrate well with complex continuous control algorithms. Start-up sequencing of simple equipment that invokes discrete (binary) steps is well accomplished by PLCs; however, complex machinery, which may have the possibility of multiple start-up paths depending on internal and external conditions, go beyond the fixed programming of PLCs.

2.2.1 Expert systems

The primary purpose of expert systems is to capture the human capability of diagnosis and control for particularly difficult or specialized tasks. If-then-else rules are the building blocks of expert systems. These rules permit conditional decision making in which the outcome decision is based on the logical condition of input variables. The strategy is to make a rule-based system flexible enough to cope with the many degrees of freedom that arise in large complex systems but manageable to design and test. By subdividing the system into smaller subsystems, the development workload can be shared and performed in parallel; nevertheless, the human effort to design large-scale expert systems is large.

2.2.1.1 State-based control

State-based control is a more complex application of *if-then-else* rules in which the states of the system being controlled are the basis for the structure of the rules. The transition between states is initiated by multiple conditions, which in turn initiate specific actions that drive the system to the desired state. This

method may take advantage of graphically oriented display. It is also suited to mathematical formalization. Timing and sequence are handled well with these model types.

2.2.1.2 Data-based control

Data-based control emphasizes internal and external activities. The flow of data and communications is well modeled with this method. However, timing and sequence is not handled as well with this method. State and data control methods may be combined.

2.2.2 Intelligent agent-based control

Intelligent agent-based control is a growing area of research. Several potential advantages are evident including the “mobility” property: agents can move about in a system to apply their specialty as needed. The literature indicates that intelligent agents have been growing in their use in computer science over the last decade. Intelligent agents have several applications related to control systems: (1) as a carrier and implementer of control algorithms, (2) as a method of communicating adaptation parameters, and (3) as a means of designing the control system both during the original plant design and as a means of upgrading throughout the plant’s lifetime.

Related to the third application above, great possibilities exist for using agent capabilities to capture control system design requirements and create a structure for linking their relationships into a control system. Multiple agents can be assigned to look for and capture according to specific requirement categories. Other agents can scan for inconsistencies and errors as the process evolves. Still other agents can compile resource requirements for the subsequent design steps.

All software agents are programs, but not all programs are agents. The salient differences between traditional computer programs and intelligent agents are compared in Table 1. There are activities for which intelligent agents offer potential advantages, e.g., activities that require teaming and may cross several computer platforms. Agents are adaptive and autonomous, which may be advantageous for some applications; however, more traditional (static) programming may be appropriate for some precision calculations.

Table 1. Comparison of traditional computer programming with intelligent agents

Traditional computer program	Intelligent agent
Static	Dynamic
Direct manipulation: user initiates every action.	Indirect manipulation—autonomous. Actions may be initiated by either the user or the agent system.
Noninteractive. Dialogs are fully scripted.	Interacts with user and with other agents.
Never changes, unless changed by a human or an error in the program.	Adapts, learns.
Runs one time, and then stops to be run again when called.	Persistent. Continues to run over time.
Predictable—does what you tell it to, even if you didn’t mean what you said.	Interprets what you mean, not what you say. In the best of circumstances, actions are based on rules, but they may change over time, or in reaction to different circumstances.
Follows instructions.	May initiate actions as well as respond to instructions.
Stays in one place.	May be mobile, traveling to other servers.

2.2.3 Nonmathematical flow methods

Multilevel flow models (MFM)¹⁵ are graphical models of goals and functions of technical systems. Morten Lind invented MFM at the Technical University of Denmark and several new algorithms and

implementations have been contributed by the group headed by Jan Eric Larsson at Lund Institute of Technology. MFM has several properties which permits knowledge engineering without mathematical models as used in classical and modern control theory and without rule bases used in standard expert systems. MFM allows diagnostic algorithms to be run in real-time without high processor overhead.

2.2.4 Formal methods

Formal methods apply to a broad range of techniques that employ mathematically precise operators to represent states, modes, and actions. The recent emphasis on formal methods has been on automated control system design. An international collaborative effort was mounted in 1996 to apply formal specification methods to generating a steam boiler control system from a specification document. The effort by Abrial et al. produced 33 solution methods from numerous students based on numerous formal languages and constructs.¹⁶ The conclusion is that there are several viable ways to apply formal methods to capture and design the controller. Since the publication of Abrial's results, others have continued the spirit with continued improvement. For example, Petre et al. have examined combining formal and informal design methods to permit better integration with software practice.¹⁷

2.2.5 Object-oriented control

Object-oriented control takes advantage of information hiding and inheritance properties for efficient programming. The objective is to make the design task less labor intensive, more amenable to analysis and testing, and flexible for modification. For the most part, object-oriented control methods are an extension of object oriented computer-programming methods (e.g., C++).

2.3 Hybrid Control Methods

Continuous servo control systems operating alone experience difficulty achieving their objectives in the face of changing dynamics, such as radical swings in subsystem parameters, component failures, or changes in equipment interconnectivity. In addition, some components have, by their nature, finite states and therefore are not controllable by traditional continuous-time methods. Hybrid control is the combination of continuous and discrete-event control to achieve automatic control over a wide range of system conditions, configurations, and desired outputs. At its simplest level, a hybrid controller can be envisioned as a switching mechanism between a collection of continuous controllers. In more complex implementations, the hybrid controller can include a capability to select modes and states of multiple subsystems to effect a coordinated movement to target goals even with malfunctioning equipment. Diagnostics play an integral role in advanced hybrid control to accommodate faults and failures.

Combining continuous and discrete control techniques often leads to a hierarchical structure with continuous controllers carrying out the tasks of regulation and tracking at lower levels while discrete-event controllers supervise their operation and make more abstract, strategic decisions. For the most part, the continuous parts and discrete-event parts are designed independently and then combined. Discrete-event activities dominate at the coordination and decision-making levels, which exist higher up the hierarchy.

For small-scale systems, the design task of the logic (discrete) component can become complex. The extension to large-scale systems is difficult to scale. Many subsystems contain multiple control types so that discrete and continuous controls must work together at the equipment level. To control a flow loop for example may require continuous control of pump speed but also requires discrete control over electrical power to motors, oil lift pumps, and valve positioners. (See ORNL/TM-9500 for a more in-depth description of the automation of discrete and continuous control.¹⁸)

3. NGNP PROTECTION STRATEGY

The protection strategy of a nuclear power plant is the set of designed responses to postulated disturbances in process variables and postulated equipment failures or malfunctions that protect the plant from damage and prevent release of radioactive materials from the fuel. The set of disturbances and failures on which the strategy is based are called the design basis events. The design basis events are “postulated events used in the design to establish the acceptable performance requirements for structures systems and components.”¹⁹ The events are broken into two categories, anticipated operational occurrences (AOOs) and accidents.²⁰ The anticipated operational occurrences are defined as “those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit.”²¹ This set of events is generally considered to have a frequency of occurrence greater than 10^{-2} events per plant year. Accidents are occurrences that are postulated but are not expected to occur. Accidents are considered to be “an event on the order of magnitude of 10^{-7} events per plant year or greater and potential consequences serious enough to affect the safety of the plant to the extent that the guidelines in 10 CFR Part 100 could be exceeded.”²⁰ The accidents may be subdivided into design basis accidents and special events (sometimes called beyond design basis accidents). The event probability of special events, which is very low and would normally not be deemed credible, may potentially result in consequences so severe that mitigation is deemed necessary. For LWRs, the anticipated transient without scram is in the special event or beyond design basis category. The selection and analysis of design basis events forms a significant role in setting the protection strategy of any plant. The protection strategy is created as a response to the design basis events as a way to protect against adverse consequences and thus has a central role in the protection design process. Once the safety strategy is conceived and demonstrated by safety analysis to protect the plant and public, the strategy must be implemented in the software and hardware of the safety system’s I&C design. The licensing test for the I&C system is to show the actual system to perform as well or better than the protection strategy used the safety analysis with its conservative assumptions.

The following section lists and discusses the set of design basis event that are likely to be considered for the baseline NGNP. The list provides a basis for discussing necessary protection functions for the NGNP and to draw contrasts with LWR protection strategies. Most of these events are also reported in the Task 3 letter report.²² The strategy assumes that the design is the baseline NGNP with a single reactor driving a single steam generator and single turbine generator.

3.1 Design Basis Events

The design basis accidents are the set of postulated accidents that a nuclear facility must be designed and built to withstand without loss of the systems, structures, and components necessary to ensure public health and safety. The most severe and limiting events are chosen so that all other accidents are encompassed by the results of the design basis events. A number of different initiating events may result in the same sequence of plant responses and are grouped together as a single design basis event. The selection of the events which compose this set is the subject of considerable study. Over time and experience, a consensus has emerged among regulators and designers for the set of design basis events for LWRs. The design basis accidents for gas-cooled reactors are not nearly as settled. The following types of transients are certainly part of the list and are generally covered in all gas reactor licensing submittals. The following discussion is for gas-cooled reactors in general. Where it is possible, the discussions address the features expected in the baseline NGNP. The descriptions and terminology are based on the Next Generation Nuclear Identification and Ranking Tables (PIRTS) Vol 2.²³

3.1.1 Anticipated operational occurrences

3.1.1.1 Turbine trip

Turbine trip transients are a common operational event. The initiation can occur because of external grid disturbances or internal events in the secondary plant. In conventional LWR plants and probably in the baseline NGNP, a turbine trip is not a safety function. However, with the single reactor and heat load configuration in the base NGNP, the turbine trip would probably generate an anticipatory reactor trip signal (ARTS). The ARTS is an input to the reactor protection system and would cause a reactor trip and circulator trip. For plants with multiple heat loads, the turbine trip might not result in a reactor trip but in a rapid change in power level and redistribution of the load. The signals generating a turbine trip typically consist of

- low bearing oil pressure;
- low electrohydraulic fluid pressure (i.e., loss of motive force for turbine governor valves);
- high condenser back pressure (i.e., loss of condenser cooling water);
- turbine overspeed;
- turbine bearing wear;
- loss generator (generator trip); and
- remote trip from an external system.

A turbine trip also trips the generator (if it is not already tripped) and results in actuation of fast-acting turbine stop valves stop the driving flow to the turbine and to protect the turbine from overspeed damage. The gas-cooled reactor core requires less rapid response to protect the core than a LWR. Even if the ARTS trip fails to act, the HTGR core can sustain the post-event heat up on loss of load. Most HTGR designs have sufficient thermal margin between the operating maximum temperature in the core and the temperature at which fuel damage could occur such that the temperature rise in the fuel can safely shut down the nuclear reaction following the turbine trip event even if the rods fail to insert (an anticipated transient without scram event).

Protection of heat exchanger surfaces from hot gas is also a concern post-accident. The rise in gas temperature following a turbine trip may be sufficiently high that some heat exchange material's temperature limits may be exceeded. The control concern is that primary and secondary flows must be accurately controlled to protect the heat exchanger from damage. To protect the heat exchangers, the helium circulators on the primary coolant loop may require a safety-related trip function.

3.1.1.2 Load rejection

In this transient, the generator breakers to the grid open reducing the load to the station load. The event requires a prompt turbine response to protect the turbine from overspeed. Some designs may respond to this event as a rapid runback to station load. In the runback scenario, no safety systems actuate; operational controls run reactor power back to a low electrical power equal to the needs of the site. More commonly, load rejection event trips the turbine and the sequence of events is the same as any turbine trip above. It is not known whether the baseline NGNP will employ runback or trip strategies.

3.1.1.3 Loss of heat sink

The loss of normal heat sink means the loss of flow or coolant on the secondary side of the normal heat removal heat exchanger. For a plant with a steam generator, the loss of flow would most frequently be caused by a loss of feedwater due to inadvertent feedwater valve closure or loss of the feedwater pumps. Loss of coolant can result from a secondary system pipe break or failure of a relief valve in the open

position. Ultimately, the transient results in a heat up of the reactor system and a need to establish an alternate heat removal through nonsafety shutdown cooling system or the safety-related passive heat removal capability of the RCCS. One of the safety concerns in a loss of secondary coolant is that the initial response of the steam generator can be different than the final response depending upon the break location. A break in the secondary coolant pressure boundary downstream of the heat exchanger would result in a temporary increase in flow of the coolant through the cold side until the inventory of secondary coolant begins to be exhausted and the density and pressure drop. The increase in flow results in an overcooling event which is then followed by an undercooling event. A break occurring upstream of the heat exchanger results in an immediate reduction in flow and reduction in heat removal. Thus, in one instance the initial indications of temperature and pressure on the primary indicate the wrong direction that the reactor should respond, whereas, the other is the right direction.

The initial overcooling for breaks downstream of the steam generator results a positive reactivity insertion and power rise because of the strong negative temperature coefficient of the core. A safety function to trip the circulator is necessary to protect the fuel on detection of the steam line break.

Because of the expected high frequency of events in this category and the requirement for establishing alternate heat removal, this sequence is frequently one of the main contributors to the core damage frequency in probabilistic risk assessments.

3.1.1.4 Control system failures

Failures in the nonsafety control system are considered AOOs. The protection strategy and safety system implementation must show that the safety function is not compromised by any I&C system failure and any consequential effects of that failure. The analysis of the design must show the ability of the sensors to accurately portray the plant status to the operator so that correct diagnosis of the failure is made and correct actions are taken. The range of transients to be considered include failure of inputs and outputs to high, low, and as-is signal values. Module level failures representing stalled processors or communications, failed power supplies and any consequential effects must all be considered. All possible command failures need to be considered. Since highly automated plants such as the NGNP have a very large number of potential commands that the system could issue, the analysis of the NGNP due to I&C system failures may be significantly more complex than conventional LWR with lower levels of automation.

It is very likely that the I&C system will be dual or triple redundant. Particular attention is necessary to identify any points of signal selection or redundant power supply failure that are vulnerable to single failure.

A resilient control or trip avoidance system may be included on the NGNP plant as a layer of control between the operational control and protection. The normal operating controls act to pull the plant toward the operating point. The trip avoidance strategy is to drive the plant away from edge of the trip envelop. The additional layer of control adds to the complexity of response and greater potential for unforeseen adverse interactions with the normal control and protection systems. Interactions between normal and resilient (such as integral windup and estimator mismatch) must be designed into the logic that transfers control between the two layers. Also, the resulting overall control strategy is in effect a nonlinear control scheme. It is very difficult to show formally that instabilities do not exist in nonlinear system. Instead, the operability must be shown with less convincing simulated test suites, over a range of operational conditions. Adequate testing of the controls depends on a high fidelity, validated simulation model. Acceptance testing of the control design should be performed with hardware-in-the loop to exercise the actual hardware with realistic plant process feedbacks, not open loop testing of the hardware.

3.1.2 Accidents

3.1.2.1 Pressurized loss of forced circulation (P-LOFC)

Pressurized loss of forced circulation (P-LOFC) is an event during power operation in which the primary helium flow stops but the pressure boundary remains intact and the primary system remains pressurized. P-LOFCs may result from a variety of initiating events or event sequences. Most commonly, it is the loss of circulator. This is an accident that the NGNP is inherently, well-designed to handle. In fact, the primary helium flow is intentionally stopped by the reactor protection system on shutdown of the reactor to avoid rapid overcooling. The subsequent heat up serves to shut down the nuclear reaction through the negative temperature coefficient even if rods are not inserted (either by accident or by design).

Two major safety concerns can be considered for P-LOFCs. The first concern is over temperature of the fuel. However, this should be a relatively straightforward for the NGNP. The power density in the core and the reactor cavity cooling system (RCCS) are designed so that the heat up of the core with pumps off is not damaging to the ceramic-coated fuel particles. With full pressure and density of the coolant, natural convection provides adequate heat removal from the fuel to the reactor vessel walls and the RCCS is design with adequate capacity to cool the reactor vessel. Thus, following the decrease in flow, the core temperature stabilizes at a level higher than normal operating temperature but within the thermal limits of the ceramic coated fuel pellets and moderator. Because of the natural circulation, the maximum core temperatures occur near the top of the core. Maximum temperatures for P-LOFC are significantly lower than for depressurized loss of flow events which do not have significant heat removal by natural recirculation.

The second safety concern is the heat-up of the primary system pressure boundary and critical components during P-LOFC conditions. Some important metallic structures, such as control rod sleeves, core barrel and reactor pressure vessel, and eventually their support structures, experience elevated temperatures as the core heats up and natural circulation with the reactor vessel carries that heat to the top of the reactor vessel. These temperature excursions and period of time at high temperatures should be taken into account in determining the structural integrity of these components and code limits. The upper vessel temperatures are more limiting in the protection strategy than the fuel temperatures. The LWRs are always more limited by fuel temperatures. The NGNP has different and somewhat lesser vulnerabilities that require a change of focus in what is important in safety review and licensing.

A variation on the P-LOFC which may lead to severe consequences is an inadvertent restart of helium circulators which can lead to excessive temperature in metallic structures and components and heat exchanger surfaces. The potential for damage by hot helium from the post shutdown reactor is a significant concern. Safety interlocks based on high core temperature are needed in the NGNP to prevent inadvertent startup of the circulators.

For some designs the high temperatures in the upper vessel are a concern for control rod cladding. For this reason, the rods may be withheld from the core following a turbine trip. The nuclear reaction is shut down by the negative reactivity due to the core temperature increase. The reflector and core region rods can safely be inserted after decay heat decreases and temperature drops. This approach protects the rods from unnecessary thermal fatigue.

3.1.2.2 Depressurized loss of forced circulation (D-LOFC)

A depressurization accident is an event that results in partial or complete loss of helium inventory. Depressurization events can be the result of failures of the primary pressure boundary or the opening of primary system safety valves with failure to reclose. The loss of coolant causes a reduction in density and mass flow rate for forced convective cooling even if the circulators are not tripped. The D-LOFC is the NGNP equivalent of a loss of coolant accident in LWRs. (Circulators are usually tripped in D-LOFC to slow air ingress from reaching the core.)

The major consequence of D-LOFC accidents is the core heat-up and potential radioactivity release into the confinement building. Unlike the P-LOFC conditions, natural convection cooling in the core is negligible because of the reduced coolant density. The D-LOFC must rely on conduction and radiative cooling to the vessel walls and the reactor vessel cavity cooling system. The maximum core temperature is considerably higher for the D-LOFC than the P-LOFC. The design limitations on the core and fuel design ensure that the core can survive a D-LOFC without significant fuel damage even in the event of failure of the rods to insert. The design objective for heat removal systems (RCCS) for NGNP is to limit the core design such that the fuel is passively safe in the event of a D-LOFC.

For the long-term D-LOFC, maximum fuel temperatures typically reach peak values in a few days and are located near the middle or beltline of the core. Temperatures then begin a long, slow decrease as decay heat diminishes. Because of the reduced coolant density, natural convection cooling does not carry core heat upward to the upper head. Consequently, upper head temperatures are not usually the limiting factor as they are for P-LOFC.

Typically, the design power level of a gas reactor is based on a conservative calculation of maximum fuel temperature in a D-LOFC accident. As in the P-LOFC, the heat-up of metallic structures and subsequent impact on material integrity must also be taken into account in determining protection. Since the event includes a loss of coolant, protective measures to limit radioactive release from confinement are necessary also.

Depending on the location of the depressurization process, the reactor core could experience an initial cooling due to a rapid discharge of helium and increased coolant flow through the core. The cooling would have a positive reactivity effect. Typically, the overpower event would be terminated by a scram on high neutron flux.

The protective actions required for D-LOFC include the reactor scram, circulator trip, confinement pressure control, confinement filtration control. Investment protection is a major issue. Because of high temperature in the reactor cavity, significant electrical equipment losses can occur if component cooling and service water cannot be maintained. Secondary plant shutdown is part of the investment protection scheme.

3.1.2.3 Anticipated transient without scram (ATWS)

Normally, the initiating event for an ATWS event sequence is an anticipated operational occurrence followed by a failure of the reactor trip system to shut down the reactor. In ATWS events in conventional LWR plants, there is a very high probability of core damage. The AOO in combination with a highly unlikely failure of the rod trip a mechanism is a very low probability event and is thus considered a beyond design basis event and is not part of the safety analysis of the plant. However, the potential consequences of the event are so severe that the risk of the event must be considered in the plant probabilistic risk assessment (PRA) and if necessary mitigation strategies must be put into place. The PRA of the ATWS events must show that the core damage frequency is less than 10^{-4} events per reactor year. In LWRs, a feedwater trip with failure of the reactor trip mechanism is frequently the highest probability event in the core damage frequency estimate for the beyond design basis analysis.

In light water reactors, the consequences from loss of feedwater with ATWS are expected to include core damage and radiation release. In contrast, the same AOO in gas-cooled reactor, (LOFW with ATWS) presents very low likelihood for core damage. As discussed in the P-LOFC, the HTGR inherently possesses a large margin between operating temperatures and temperature at which damage occurs, strong negative reactivity coefficients of temperature, and large thermal capacity of the moderator and reflector. The inherent thermal feedback for shutdown protects the core under all AOO events. In the analysis of an ATWS events in an HTGR, all control and safety rod positions are assumed fixed and no rods drop and no secondary shutdown mechanism operates in response to scram signals. Other protective actions, such as tripping the primary circulators and core heat removal via the reactor cavity cooling system (RCCS)

and shutdown cooling, are assumed successful. Unless accompanied by another (low probability accident such as D-LOFC) ATWS events do not have serious consequences. The I&C provisions for ATWS events are not decided for the NGNP. Certain nonsafety equipment, such as the shutdown cooling system and the secondary shutdown system, may have high risk significance and require licensing review as risk significant nonsafety equipment.²⁴

3.1.2.4 Air ingress

Air ingress into the primary system is a safety concern because of the damage it could cause by oxidizing graphite structures and components in the vessel and by oxidation damage to the ceramic coated fuel particles (TRISO particles) leading to the release of fission byproducts from the fuel. At the temperatures that would be seen in the core following failure of the pressure boundary (D-LOFC), a significant oxidation would be possible. The extent of the air ingress flow rates and the oxygen content of the available air are dependent on a wide variety of possible reactor and reactor cavity design features, initiating event factors, and subsequent accident progression scenarios. These accidents are typically categorized as very low probability events—special events in the terminology of safety analysis (or beyond design basis accidents BDBA).

An air ingress event caused by a primary system break starting from nominal operating conditions is usually assumed to follow complete depressurization in a long-term D-LOFC accident. Depressurization to atmospheric pressure is a prerequisite for atmospheric air to enter the primary system. Air ingress during a normal shutdown is not considered since reactor internal temperatures are below the levels where significant graphite degradation would occur.

During D-LOFC, vessel or other primary system breaches would likely result in blowdown of the helium inventory into the reactor or power conversion unit (PCU) cavity, resulting in displacement of air therein. The resulting atmosphere for the duration of the potential ingress event would depend greatly on whether or not the confinement system is designed to release the initial discharge of the gas to the atmosphere.

Ingress flow rates are usually limited to relatively low values due to the high core flow resistance and resistances in other parts of the flow paths. There is considerable uncertainty in the mechanisms of ingress. Many calculations assume purely molecular diffusion which is the slowest ingress. Other studies have shown that convection-assisted diffusion occurs in vertical pipe breaks (cold flow in at the bottom of the break, hot flow out at the top of the same opening.)

Actions by a protection system are to promptly insert rods to shut down the reaction and to cool the core as quickly as possible below the temperature at which the air graphite reaction takes place. Since the accident is considered beyond design basis, the appropriate analysis is a probabilistic risk assessment for core damage frequency. In the probabilistic risk assessment, the nonsafety cooling systems can be considered in to contribute to risk reduction for core damage frequency. So cooling by the shutdown cooling system and by the steam generator may be considered part of the accident response. The risk significance of systems affects the level of review given by the license review and subsequent in-plant inspections.

3.1.2.5 Steam/water ingress

Steam/water ingress into an HTGR core can result from steam generator tube leaks in the steam generator. The steam generator pressure is much higher pressure than that of the primary helium; thus, at the initiation of a tube leak, significant water can enter the primary. Once in the primary, water can propagate to the core by forced convection until circulators are stopped and by diffusion thereafter. Water ingress events can involve complex interactions between neutronics, thermo-fluids, chemical reactions that erode fuel and graphite, and radioactivity releases. Metal and graphite surfaces that have operated at high temperature have all protective oxide coatings removed and are very sensitive to water reaction at normal operating temperature. Water ingress at Fort St. Vrain led to stuck rod and stuck secondary

shutdown system due to water effects on the release mechanisms. The safety significance of the safety system failures resulting from steam/water ingress at Fort St. Vrain should not be underestimated. A single failure has the potential for inhibiting two independent reactor shutdown mechanisms. (At Fort St. Vrain, the failures did not occur concurrently.) NGNP has similar rods and secondary shutdown boron spheres as Fort St. Vrain. The rod and boron sphere release mechanisms however are different. Also, the ingress mechanism at Fort St. Vrain was the water driven turbine on the helium circulators used for startup and not a steam generator tube leak.²⁵

The protective functions in the event of steam water ingress are to shut down the reactor promptly, isolate the steam generator and dump the water and steam to a dump tank, depressurize the secondary, and trip the helium circulators. Moisture removal from the primary coolant using the helium purification system may be required to reduce the concentration of steam in the primary and limit the mass available for reaction. The moisture removal function may need to be a safety related function. Cooling the graphite and structural metal reduces the reaction rate so the initiation of the shutdown cooling system would be advantageous to reducing fuel reaction and erosion. Prompt insertion of rods counters the positive reactivity of water in the core, reduces possibility of stuck rod events due to erosion, and permits rapid cooling of the core to reduce chemical reaction rates without the potential for re-criticality.

3.2 Plant protection system functions

The instrumentation and controls in the plant protection system consists of the components required to detect and initiate automatic corrective actions upon onset of an unsafe condition. These actions are directed toward reducing plant power and shutting down reactor plant equipment and allowing passive systems to maintain the reactor in a safe configuration that does not result in fuel damage or the release of radioactive materials to the atmosphere. The major automatic functions of the baseline NGNP plant protection system (which is based on the MHTGR design²⁶ with modifications for NGNP) are expected to be:

- reactor scram,
- secondary isolation
- steam generator isolation and dump system
- circulator trip,
- rod withdrawal prohibit
- confinement pressure control,
- confinement filtration control, and
- moisture removal function of the helium purification system.

The protection system functions are expected to be organized into three categories:

- reactor protection system (RPS),
- engineered safety features (ESF), and
- investment protection systems (IPS).

The reactor protection system (RPS) shuts down the nuclear reaction in response to upsets. Engineered safety features (ESF) mitigate the consequences of design basis or loss-of-coolant accidents. The RPS and ESF are traditional subdivisions of the protection system. In modern digital protection systems, I&C for RPS and ESF may be merely functional divisions within a single digital system rather than two physically separate systems.

The investment protection category of protection system is a new concept for licensing which was introduced by the MHTGR preconceptual design report and which was discussed in Task 1 report.¹ The passive cooling of the RCCS is sufficient to protect the fuel in a depressurization event; however, other equipment important to investment and operation may be vulnerable at the temperatures that may exist in

the reactor and confinement cavity when only the inherent passive cooling is available. Active components such as pumps, valves, motors, control rod drives, and instrumentation are in fact likely to be damaged by the high temperatures reached when the plant is involved in a D-LOFC event unless active cooling systems are operational. The class of support function which would cool the active components is called “investment protection” by General Atomics in their pre-conceptual MHTGR design report.³⁰ As presented by General Atomics, the concept of “investment protection” is an intermediate safety class between safety-related and nonsafety-related. When the MHTGR pre-conceptual design was reviewed by the NRC, one of the unresolved issues was the concept of “investment protection” rather than “safety-related” as the designation for equipment analogous to LWR systems which are safety related. Because the issue is unresolved, no distinction is made between the safety related functions (RPS and ESF) and investment protection in this report.

The plant protection system is utilized upon occurrence of the following.

- Equipment failures which require corrective action beyond the capability of the plant control system.
- Failure of the plant control system causing an abnormal condition.
- Incorrect operation which result in a potentially unsafe condition.

The protective functions required of the plant protection system are related to conditions which might lead to:

- loss of core cooling,
- power increase not matched by core cooling,
- confinement/containment pressure rise, and
- core or major equipment damage.

By regulation,¹⁹ the plant protection system must achieve high reliability and perform its function in the presence of any single failure and consequential effects. Standard design practice uses redundancy and coincidence logic to achieve the required operation. The system uses channel independence to guard against the effects of plausible single events, such as fires, shearing or blocking of process connections, environmental effects, seismic events, and module removal.

3.2.1 Reactivity control

The NGNP is expected to use rods as the primary reactivity control mechanism. Rod groups may be segregated by groups by the core region. The outer reflector region is cooler than core region. Outer control rods located in the reflector are used to control power and to shut down from high power to protect them from excessive temperature. Rods in the central fuel region would be safety rods which are inserted in bores in the fuel block for cold shutdown. Both control and safety rods are fabricated from natural boron in annular graphite compacts. Metal cladding is provided for structural support.

The reserve shutdown system provides a second independent shutdown mechanism if needed. The reserve shutdown system operates by releasing boronated graphite spheres stored in hoppers above the core into channels bored in the graphite moderator in the central fuel region of the core.

3.2.2 Engineered safety features

The engineered safety features (ESF) provide cooling to the core when the normal heat removal systems are unavailable, containment/confinement systems which isolate and/or filter gases from primary, and steam generator isolation systems.

3.2.3 Shutdown cooling system (possibly investment protection rather than ESF)

The shutdown cooling system (SCS) in the NGNP design provides normal temperature control and decay heat removal when the reactor is shutdown. The system consists of a gas-to-water counter-flow heat exchanger located in the lower plenum region of the reactor vessel to remove heat from the helium coolant and a water-to-air heat exchanger to dump the heat to the atmosphere. The forced circulation of the shutdown loop is provided by an electrically driven pump. The helium in the reactor vessel is circulated by the SCS circulator.

3.2.4 Reactor cavity cooling system (RCCS)

The safety-related reactor cavity cooling system (RCCS) removes heat continuously and passively from the reactor vessel walls. The vessel wall is uninsulated and transfers heat to the reactor cavity via natural convection and thermal radiation. The reactor cavity transfers heat to cooling panels and then to the environs through natural convection of either air or water. The cooling panels separate the outside air from the air in the reactor cavity to minimize release of radioactive air that has been activated by flow through the reactor cavity. The cooling panels also serve to protect the cavity walls from overheating during normal operation.

The RCCS is a completely passive system with the capacity to remove all decay heat from the core, whether the core remains pressurized or not. The system is redundant but not diverse. Redundant inlet/outlet flow paths ensure adequate air flow to the heat panels. Heat rejection can also be accomplished to the ground surrounding the underground concrete reactor building. The RCCS has no valves or active components. In comparison to conventional light-water reactor emergency cooling system, the RCCS is a particularly noteworthy system because the safety system is always “on.” It does not have to detect a loss of cooling and initiate the emergency cooling function. There is just one alignment and one operating mode. Air or water flow through the RCCS and heat rejection is simply a function of the reactor vessel temperature and the outside air temperature. The heat transport design of the cavity ensures that the system can remove the maximum decay heat from the reactor vessel without the vessel, internal structure or core exceeding thermal limits. The RCCS is the ultimate heat sink in the reactor designs credited in plant safety analysis. A passive system is only possible because of the capability of the fuel particles to withstand very high temperature without damage or radiation release in excess of allowable limits.

3.2.5 Containment/confinement structure

Historically, most HTGRs have a containment vessel that is designed to retain helium released from the reactor in the event of a primary loss of pressure accident. The containment structure consists of a reactor containment vessel (CV), service area (SA), and an emergency air purification system, which reduce the release of fission products to the environment during postulated accidents. The proposals for the NGNP have included a confinement rather than containment concept. The strategy was originally presented by Dilling for the MHTGR²⁷ and also proposed for the PBMR design.²⁸ The confinement structure is designed to retain released gas from the reactor briefly to cool and filter it. Because of the design and reliability of the fuel particles, the coolant gas in normal operation is not highly contaminated and can then be released to atmosphere. The argument for release rather than containment is that, after a depressurization accident, a containment vessel pressurized with the helium is more hazardous than the release of the gas to atmosphere. Moreover, early release of the gas in the confinement is argued to be safer than later when accident evolution may have led to fuel damage. The confinement strategy usually involves filtration. The filtration may require a bypass early in depressurization events because the high temperature of the exhausted helium may damage the filters rendering them ineffective later when the release of contamination is more likely.

The confinement strategy may require active safety-related controls systems for both pressure and filtration. This is one area in which the I&C for a safety systems for the NGNP may be more complex than an analogous containment building in an LWR.

3.2.6 Moisture removal

The helium purification of system is a normal operating process that maintains high purity helium. In water ingress events, the system may also perform a safety function to remove water before reaction can take place. In normal operation, small amounts of air and moisture enter the primary system through the addition of fresh fuel elements, small leaks in the cooling facilities, experimental ports, and through the course of maintenance and repair work to components of the primary circuit. The helium purification system continuously extracts a fraction of the flow to remove impurities from the coolant. In accident conditions, the system, or a portion of the system operates to remove water from water ingress events. The process requires instrumentation and controls to initiate any special operation due to accident conditions. It also requires process controls for flow, temperature, and pressure controls for the purification process.

3.3 Instrumentation and controls for protection system functions

NGNP safety systems are likely to be similar in structure and hierarchy to existing digital safety system controls because simplicity and reliability require it. Innovation and complexity are not advantages. It is to be expected that the logic in the safety system consists of an envelope of operating conditions within which the plant is assured by safety analysis to be protected. Unsafe conditions and equipment failures will be detected by measured parameters reaching a trip setpoint at the edge of the envelope. The trip logic will seal in and a safety function or set of safety functions will be initiated to drive the plant to a safe shutdown state. The safety analysis is used to show that all credible events are detected by the envelope and comparator logic and that safety functions can safely mitigate the event.

While the envelope concept of a protection system is expected to be the same as a traditional plant, there may be some new features not present in existing plants. Task 2 reports on resilient control and trip avoidance measures. These features are intended to improve safety and increase plant availability. The resilient controls would act inside the traditional safety envelope. For example, the control system may employ trip avoidance strategies to reduce the demands on the protection system. Using resilient control techniques, the controls system may automatically diagnose equipment degradation or failures and reconfigure the operating controls to adapt to the degraded conditions. The “resilience” is to maintain the reactor in safe operating condition without exercising the protection system, to increase reliability and availability of the plant, and to minimize thermal transients which stress and age the reactor systems. The difficulty is the complexity of the resilient control scheme and the potential for adverse, unforeseen interactions between the resilient control and the protection system. The difficulty is not that unforeseen, adverse interactions between the resilient control and the safety system are likely. In fact, the strategies seem to make that unlikely. However, it is difficult to prove that a complex system has no adverse interactions. This report leaves as an open issue the problems of licensing resilient control and trip avoidance. Since the proposed use of resilient control has not moved to even conceptual design phase, the question cannot be very well evaluated.

The following section provides a discussion of the logic functions that seem likely for the protection of the baseline NGNP. The logic for each safety function is hypothetical but is based on logic presented for other reactors in Task 1. The purpose of presenting hypothetical logic is for discussion of potential problems and licensing differences with respect to LWRs since the actual NGNP protection logic has not yet been designed.

3.3.1 Reactor scram logic

The following plant states are used by the plant protection system to initiate the automatic reactor scram logic:

- manual,
- low main steam line pressure,
- low hot reheat steam pressure,
- high wide range channel rate of neutron flux change,
- high startup count rate (startup only),
- rate of change of startup count rate (startup only),
- neutron flux high,
- high moisture in the primary coolant,
- high reheat steam temperature,
- low primary coolant pressure (only at power),
- high primary coolant pressure,
- plant electrical system power loss,
- high reactor building temperature,
- high reactor building pressure,
- circulator trip, and
- auxiliary scram actions (e.g., turbine trip).

3.3.2 RCCS

The reactor cavity cooling system is the only safety related heat removal system. (The steam generator and the shutdown cooling system are nonsafety heat removal systems.) The RCCS is always on and does not have any logic for initiating the function. The RCCS only requires monitoring of temperatures to ensure normal operations are proceeding.

3.3.3 Circulator trip logic

The NGNP circulator is expected to be a variable speed electrically driven blower. Trip functions to protect against overcooling and against circulating air or moisture in the event of an ingress event.

The plant protection system may use these parameters in circulator trip circuit and provide an input to the reactor protection system:

- manual,
- low circulator speed,
- high circulator speed,
- low feedwater flow,
- low circulator magnetic bearing clearance,
- reactor trip,
- turbine trip,
- circulator penetration pressure high,
- steam leak detection (turbine building pressure, rate of rise),
- steam leak detection (reactor building pressure, rate of rise),
- steam leak detection (turbine building pressure, fixed setpoint), and
- steam leak detection (reactor building pressure, fixed setpoint).

3.3.4 Circulator start inhibit logic

The circulator must be inhibited from starting when core temperature is too high for structural materials downstream of the core.

3.3.5 Rod withdrawal prohibition logic

The rod withdrawal prohibition logic prevents high reactivity insertion in approach to critical during startup or an overpower event during power operation. The NGNP plant protection system uses these parameters in rod withdrawal prohibition:

- low count rate,
- high startup range channel rate of neutron flux change,
- high wide range channel rate of neutron flux change,
- high flux level,
- flux to flow interlocks,
- rod control circuit load, and
- power range failure.

3.3.6 Reserve shutdown system and safety shutdown cooling system logic

The NGNP reserve shutdown system and safe shutdown cooling systems are expected to be manually actuated with no operating bypasses. Instrumentation for operator control information is required. The shutdown system requires monitors of release mechanism position and detection that absorber balls have been released. The shutdown cooling system needs monitoring of the shutdown circulator, temperatures of the helium, temperatures and flows on the shutdown heat removal heat exchanger and pressures. Isolation of the shutdown cooler is an ESF safety function.

3.3.7 Steam/water dump

The steam dump system isolates and drains the steam generator in the event of a tube leak to limit the amount water in the steam generator that could enter the primary. Upon detection of moisture in the primary, the dump system activates emergency feedwater isolation valves and main steam stop/check valves. The dump is accomplished by the rapid opening of two parallel redundant valves relieving water and steam through the feedwater header to the dump tank. To meet redundancy requirements, either valve must be sufficient to drain the steam generator.

3.3.8 Steam generator isolation

Actuation of steam and feedwater block valves are ESF functions required for preventing water and steam entry into the steam generator when a tube leak is detected. The isolation is initiated in response to moisture in the primary.

3.3.9 Confinement vessel pressure and filtration flow logic

The confinement building is a low pressure sealed building. To protect the building from overpressure, the building must release helium to atmosphere. The function is triggered by indications that the primary coolant is entering the confinement.

- High confinement pressure or
- High cavity wall temperature or
- High confinement radioactivity.

Filtration bypass is triggered by

- High confinement pressure with high temperature and low radioactivity in reactor cavity.

4. NGNP CONTROL STRATEGY

While the protection system for the baseline NGNP is likely to be a conventional digital protection system with comparator protection logic, major innovations and advancements are expected for control systems. Highly integrated digital control systems are likely to be used to (1) automate mode changes such as component startup and shutdowns, (2) apply multiple modes and algorithms for regulation and tracking control, and (3) detect faults and disturbances and reconfigure the plant and controls to avoid plant trips without operator action using resilient control. These innovations will make the plants more reliable but at the same time more complex. The main impact is in ensuring that the plant is safe through design and review. The greater the number of actions that are taken automatically then the greater number of opportunities for the action to be unsafe under some unforeseen circumstance. The issue is adequate assurance of the safety of the plant to accommodate unforeseen unsafe actions.

Many aspects of modular HTGR heat transport system controls are quite different from those of LWRs. First, the mean temperature rise of the coolant through the core is $\sim 400^{\circ}\text{C}$, or about a factor of 10 larger than for LWRs, so system temperature gradients are much larger. Since the mean coolant outlet temperature is very high, it is important that it remains constant (high) over the power operating range both to maintain high efficiency and avoid thermal cycling of the high temperature components. The inlet coolant temperature should remain nearly constant as well, in the $300\text{--}400^{\circ}\text{C}$ range, since it is used to maintain moderately low reactor pressure vessel temperatures, cooling the vessel in its path from the entrance up to the top (inlet) plenum. Thus for variations in power (load) from 100 to 20%, the coolant mass flow rate must also change from 100 to about 20%. From low flow to high flow, the thermal response time constants change by about a factor of five as well which complicates a fixed gain control strategy. Another feature of the core coolant is the large spatial variations in outlet temperatures due to uneven heating, in the order of $\sim 100^{\circ}\text{C}$ or more. The resulting mixing problems (including temperature sensor signal fluctuations) can make it very difficult to get valid mean temperature measurements for this important control signal. These properties of the HTGR system mean that control strategies are expected to be considerably different and challenging than LWR controls.

4.1 Normal Operating Conditions

Normal operating conditions are defined as the envelope that covers the reactor power between some nominal low power range limit (e.g., 20%) to 100% with all reactor and plant systems functioning as designed. Major transients in this class are (1) load follow of ramp demand and (2) load follow of step change in demand.

4.1.1 Load follow

The load follow event is an example case of the ability of the reactor and power conversion systems to respond to disturbance in which the load produced by the reactor and supplied to the power conversion system must change in response to a change in demand. The limiting cases are taken from the contractually rated maneuvering capabilities of the plant. The limiting cases are specified in terms of the ramp rate and size of step changes that can be followed within specified time response.

4.1.2 Maximum ramp

The maximum ramp transient conveys the plant from the lowest automatic level to the highest at the maximum ramp rate permitted. Plateaus or hold points required by the operation of the plant may be programmed to occur in the load follow control system. Any system state transitions related to power change may be controlled off the load setpoint. For example, a signal to automatically load the turbine

and shutdown steam bypass to the condenser would be triggered by the load setpoint during the rise to power operation.

4.1.3 Step change

The step change transient involves a step in the demand. Of course the system cannot respond instantly; the step change transient shows that the system can respond stably and within the time warranted by the vendor. From a control analysis, the step change transient reveals a great deal about the control and plant dynamics. Many control tuning procedures are based on the step change test for overshoot damping time and maximum error. Parametric studies may point to specific combinations of operating conditions that are most limiting in the system's ability to respond within the trip envelope.

4.2 Operational Controls

In safety analysis, the operational controls are the first echelon of defense in depth. Because the operating point is within the envelope of safe conditions for the plant, the regulation of the plant to the operating point maintains safe conditions. The control system uses deviations of the plant from its setpoint to restore the plant to the design operating point when disturbances occur. The operational controls use a combination of feedforward and feedback controls to respond quickly and stably to disturbances.

Control schemes involve different modes and functions depending on the plant state. Most of the major equipment systems have four distinct control modes: offline, startup, normal operation and shutdown. The offline and normal operation modes are typically the continuous static states; startup/shutdown modes are transitional between normal operation and offline. In normal operation, the control systems regulate the process using feedback control. The normal operation mode encompasses both steady state and power maneuvering at rated ramp rates for power change. Additional submodes in normal operation may exist for low power, rapid runback, and special plant configurations (e.g., operation on turbine bypass versus normal turbine). Each of the equipment modes may have a special servo control made to address any special requirements of the plant.

The control system of the baseline NGNP is expected to be constructed as a distributed network of different types of digital devices for signal input and output; processing, computations, and logic; communications; and operator interface. All the devices communicate with each other over a digital communications network so that each module on the network has access to all data and commands.

In addition to the regulation of the plant, the same digital control systems perform additional tasks, such as

- providing the operator displays and the operator input interface through touchscreens or trackball,
- diagnostics of the control system and the plant equipment,
- sensor and transmitter calibration,
- historical plant data logging,
- special data logging for accident review, and
- maintenance bypass and logout/tagout functions.

Important functions such as maintaining the ability to control the plant when the control room becomes uninhabitable are also addressed as part of the normal control system review. These auxiliary functions, as a group, are not necessarily unique to NGNP designs and are generally similar to other reactor designs.

Only preliminary control system studies have been reported for the NGNP designs. Consequently, only general and hypothetical comments are made regarding the operational controls.

4.2.1 Startup and shutdown

Startup and shutdown of equipment involves a transition from an offline or standby condition to an operational state, or the reverse transition. The transition usually involves discrete logic to monitor the plant status to detect the point at which transition is required and then the performance of a series of steps to convey the system from one state to the other. The transition functions which were manually performed by an operator at the control panel on current generation plants are likely to be controlled automatically by the NGNP control system. The operator serves to monitor the process. The interface would probably provide for acknowledging the automatic transitions as needed to maintain operational awareness. Operator awareness is part of human factors design and is not covered in this report. The previous HTGR plants constructed in the 1960s, such as Fort St. Vrain and AVR, were largely manually controlled in startup and shutdown. The more advanced plants including MHTGR were designed with automated digital startup and shutdown controls. It is expected that NGNP will be fully automated in startup and shutdown. The startup/shutdown control modes include the operational controls for starting auxiliary systems, such as cooling and lubrication systems; conditioning the equipment for operation, such as, warming components to operating temperatures; and valve and power alignments to bring the equipment online. The startup/shutdown may include a transitional control mode in which one system is started and balanced with other systems already online.

The safety significance of the startup and shutdown control modes is that each control mode constitutes a different set of conditions and responses for the system. Each mode has a different response whose safety must be evaluated for normal conditions, external disturbances, and all types of failures in the plant or the control system.

4.2.2 Normal operation

4.2.2.1 Heat transport system control

The NGNP plant control involves control of a series of heat transfer and energy conversion processes. The reactor produces heat. The flow of helium coolant through the core removes the heat by convection and transports it to a heat steam generator which removes the heat. Steam produced in the steam generator flows to the turbine/generator that converts the thermal energy to electrical power. At steady state, the operational control system regulates the heat transport processes to the design point. The feedback controls adjust for gradual changes in the plant, such as burnup or steam generator fouling, or changes in the temperature of the absolute heat sink. Feedback control is used to regulate temperatures, pressures, and flows within the heat transport system to their setpoints despite variations in the plant.

The control system is also responsible for normal maneuvering from one power level to another or for restoring the plant to equilibrium following major disturbances such as turbine trip or feedwater pump trip. Disturbances usually involve rapid changes in power level. In some control strategies, the power maneuvering involves a feedforward in addition to the feedback to improve dynamic response.

The regulation of the plant to an operating point or tracking a changing setpoint are realm of continuous servo control that is the most familiar problem in control engineering. The main heat transport control problem is a multivariate control problem that could be solved by modern multivariate control such as those described in Section 2. However, the servo control strategy could very easily be similar to conventional LWR and fossil power plants. The conventional control strategy for normal operation and regulation of the heat transport systems involves decentralized control designs. The decentralized control algorithms use single loop controls with proportional-integral or proportional-integral-differential action. In many instances, feedforward inputs for load setpoint are added to the feedback action to improve coordination between the different parts of the heat transport system and to improve the speed of response. In most cases, the conventional control system involves a two-level cascade in which a top level controller computes a setpoint for the lower level controller. The lower level controller in the cascade

forms a second error using another measured variable in its feedback loop. The output from the lower level controller is an actuation signal (increase/decrease) or a position demand.

Figures 1 and 2 show typical two-level, cascade control loops for demand output in the upper figure and increase/decrease output in the lower. The demand output is used by actuators such as valve positioners which require a position demand. The increase/decrease output is used by systems such as rod controls which have increase or decrease inputs. The feedback devices are shown as proportional-integral action but could be any combination of proportional, integral, or differential action.

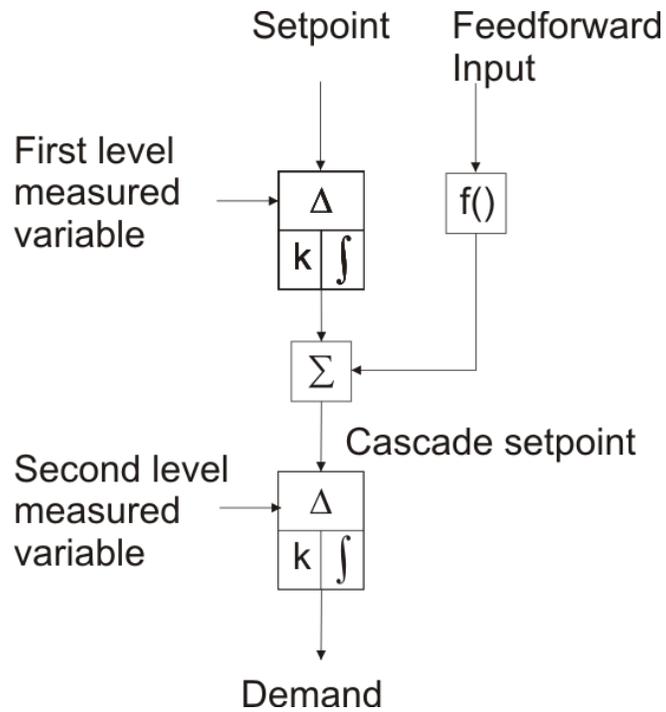


Fig. 1. Two-level cascade controller with demand output.

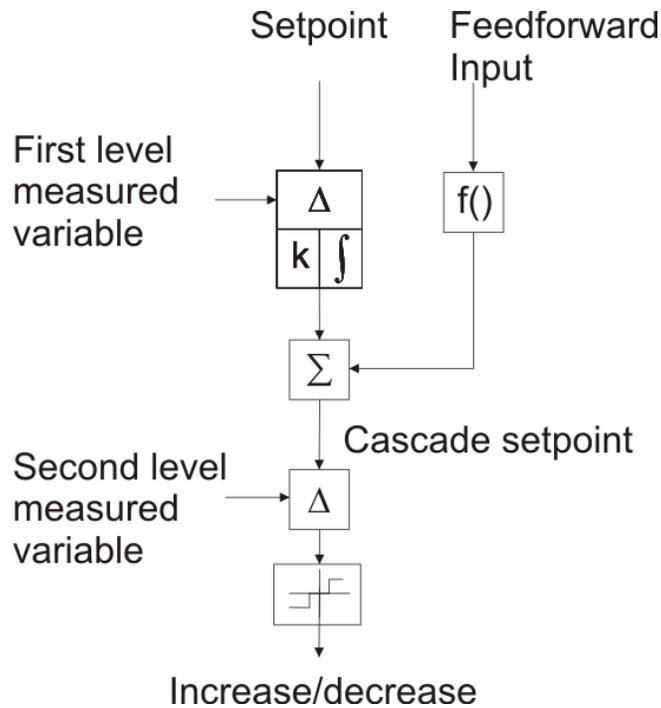


Fig. 2. Two level control with increase/decrease output.

In heat transport systems, the feedforward signal is either a load setpoint from a coordinated load controller or a measured variable that is related to the load, such as feedwater flow. The load signal acts as an exogenous input which causes the heat transport processes in the reactor, circulator, steam generator, and turbine to act in unison in response to the external input. The HTGR's dynamic response has a wide range of time constants. The feedforward component of the control signal helps to keep the different parts of the heat transport system responding together despite the differences in the time constants.

The first level feedback gives the corrective action for deviations due to variations in the process. If integral action is included in the first controller, then the cascade setpoint integrates to a value that yields zero offset in the first level error. Typically, this integral has a low gain for slow, stable approach to steady state and is tuned on the basis of the time constant of the process connecting output demand to the first level measured variable.

The second level feedback error takes advantage of a measured variable that is more directly affected by the actuator to provide rapid positioning. The open loop response from the demand to the second level measured variable is usually quite fast. The control gains can be much larger, which improves the tracking of the final demand to the feedforward signal. For example, the first level measured variable for the rod control could be core outlet helium temperature which has a very slow response. Since it has a large time delay, the control loop on temperature cannot have high gain. The low gain integral action applied the temperature error gradually corrects for effects such as burnup, errors in feedforward signal, and other disturbances so that the reactor stays at the core outlet temperature operating point. The second level measured variable is neutron flux which responds more rapidly. The rod control at the lower level causes the neutron flux to track the load demand in unison with feedwater flow and turbine. The lower level in the cascade provides a fast response to the feedforward input. The combination of slow, stable calibration on the top level and fast adjustment to load setpoints on the lower level give the best combination of speed of response to load change and stability.

Although the cascade structure results in what is actually a multivariate control problem, modern control methods have not typically been applied to determine the gains analytically. Undoubtedly, this is because conventional tuning strategies work very well. The main limitation in operating response is not due to control algorithm issues; rather, it is the speed of actuators (rod drive, valve actuator, etc.) that limit the responsiveness. The rate limits and saturation limits of the actuators would impose constraints on a multivariate controller (or would be considered nonlinearities depending on the method of solution). The complexity of the resulting control system design has simply not been justified. Based on the survey of the literature in Task 1, we learned that control schemes for HTGRs have historically been developed with ad hoc structure and trial and error tuning and were found to be satisfactory. The similarity of the NGNP control problem to previous HTGRs and to conventional fossil power plants gives historical basis to assume that this control design approach would prove to be satisfactory again.

4.2.2.1.1 Steam generator-turbine heat transport controls

The baseline NGNP has a single primary loop with steam generator in the primary loop. Four of the five existing HTGRs surveyed in Task 1 have a steam generator and steam turbine for power conversion. (The fifth, HTTR, has a water cooled heat exchanger that dumps heat to an air cooler without any power conversion.) The design experience with the steam generator designs is directly applicable to the NGNP. The heat transport loop of steam generator plants consists of the reactor, helium circulation system, the steam generator, and the turbine-generator. The heat transport system's inputs and outputs are all closely coupled together so that many different combinations of input-output pairs that give feasible control systems. This fact is borne out by the range of configurations that are found in the survey of existing plants.

Three of steam generator-turbine plants in the survey of existing plants have sufficient detail to compare the overall control scheme for the heat transport plant. The main heat transport loop at normal power operation involves control variables for four main systems: reactor power, feedwater control, electrical power, and circulator flow. The control schemes are compared in Table 2. What is interesting is that substantially the same control problem can be solved in three very different ways for the three reactors reviewed.

Table 2 from Task 1 gives the input and output pairings of measured and controlled variables for each loop in terms of the inputs shown in the general cascade controllers in Figs. 1 and 2. For example, the MHTGR column indicates that the first level process variables are assigned so that the allocated load (for each reactor module) is controlled by the module feedwater flow valve, steam pressure (for a group of reactors in the same power block) is controlled by the turbine throttle valve, and steam temperature is controlled jointly by circulator speed and reactor neutron power. The MHTGR uses the measured feedwater flow setpoint as a feedforward input to coordinate the reactor power and the circulator speed. The input/output pairs and actions are based on the operational descriptions of the control systems. Some uncertainty in the data exists because of vague descriptions in the source documents. Uncertain information is indicated with (?).

Table 2. Cascade control schemes for three HTGRs

Controlled variable	Controller input components	MHTGR	Fort St. Vrain	AVR
Control rods	Feedforward input	FW flow	Steam flow	None
	First level (action)	Steam temperature (PD or PID)	Reheat steam temperature (PI)	Reactor outlet temperature (Manual?)
	Second level (action)	Neutron flux (P)	Neutron flux (P)	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease
Helium circulator motor frequency	Feedforward input	FW Flow	FW flow	None
	First level (action)	Steam temperature (PD)	Main steam temperature (PI)	Electrical load (Manual?)
	Second level (action)	None	None	None
	Output	Speed demand	Speed demand	Speed demand
Feedwater valves	Feedforward input	Module load	Turbine first stage pressure	
	First level error (action)	FW flow (PI)	Steam Pressure (PI?)	Steam temperature (Manual?)
	Second level error (action)	None	FW Flow (PI?)	None
	Output	Valve demand	Valve demand	Valve demand
Turbine throttle valve	Feedforward input	Total load	None	None
	First level error (action)	Steam pressure (P)	Electrical load	Steam pressure (P)
	Second level error (action)	None	None	None
	Output	Increase/decrease	Increase/decrease	Increase/decrease

Action means the type of feedback applied to the error. P-proportional, D-differential, I-integral

4.2.2.2 Direct cycle gas turbine plants

The other type of power conversion proposed for HTGRs is the direct-cycle, gas turbine.²⁹ The most common configuration for the plants is a single shaft design in which the compressor, turbine, and generator are all on the same shaft. The control inputs are considerably different than a steam turbine plant. In normal operation, when the generator is synchronized to the grid, the helium circulator speed is fixed by the grid frequency. Also, the gas turbine is not usually throttled like steam turbines. Lacking circulator speed and turbine throttle valve takes away two degrees of freedom that the steam generator plants utilize. The control inputs for the gas turbine system are the rod position, helium inventory (mass in primary), turbine bypass valve, and the intercooler flow control valve. The turbine bypass valve routes the helium flow around the turbine. It is a fast-acting, but thermodynamically inefficient, means for controlling electrical load. Helium inventory is slow-acting means for controlling electrical load but maintains efficiency at reduced load. Changing density of the helium maintains the same gas velocities and blade versus gas velocity angles so that efficiency is constant with load but involves slow response and pumping losses in removing and restoring the helium to the primary. The flow to the inventory storage system is extracted from the high pressure side of the compressor and return flow is to the low pressure side so that no separate helium pump is needed (except for startup). The rods are used to control reactor outlet temperature, and the intercooler secondary side flow (water cooled usually) is used to control reactor inlet temperature.

4.2.2.3 Helium purification systems

Helium purification systems contain a number of local controls for controlling the flow and temperature of the helium stream. In addition, the normal operation of these systems typically has two submodes: purification and regeneration. Regeneration refreshes the chemical extraction mediums for reuse. Helium purification systems have at least two trains so that one train can be online and processing the helium coolant and the other in regeneration to remove impurities from adsorption beds and ready them for reuse. Automatic controls for both normal purification and regeneration would involve on/off controls to redirect flows and transfer systems from one mode to the other and servo controls to regulate temperatures, flows and chemical concentration in the purification and regeneration modes. Control schemes for the purification plants have not been found in the literature survey.

Moisture removal from the primary system is one of the safety functions required following a water ingress event. The safety function might be a special control mode of the purification system.

4.2.2.4 Cooling systems

Controls for support cooling systems such as vessel cooling system, shutdown cooling system, component cooling system, and various balance of plant heater exchangers require normal controls similar to LWRs. Descriptions of the controls and instrumentation for these systems is not available however in the NGNP literature. The systems are decoupled from the heat transport processes such that decentralized single-input-single-output servo controls can be used to maintain temperatures pressures and flows in the support cooling systems. The NGNP cooling systems would be expected to be similar to cooling systems in conventional plants.

5. KEY CONTROL AND PROTECTION DESIGN METHOD ISSUES FOR NGNP

5.1 Issues in Protection Systems

The inherent safety properties of HTGRs eliminate or significantly reduce the risk of some of the most severe accidents that LWRs must address. However, some new types of active safety systems may require formulation of new requirements and guidance. The most severe accidents for HTGRs involve air and water ingress. Air ingress may rely on measures to reduce or restrict available air in the vicinity of a leak. Mitigation measures, such as foam to stop or slow air ingress, may be required to protect the fuel from erosion by oxygen. Water ingress may require an operable helium purification system to remove moisture in water ingress events. Confinement systems with active controls on either filtered or released helium leaked from the primary system in a depressurization event are also a new type of protection system. An inadvertent restart of a helium circulator following any emergency shutdown when the core is at peak temperature can produce helium temperatures that would damage heat exchangers. An inhibit function to prevent the start of the circulator when the core temperature is high may be needed. Acceptance criteria for these new types systems are not suggested by the existing general design criteria.

5.2 Issues in Control Systems

5.2.1 Advanced control design methods

The NGNP can be expected to make extensive use of digital technology and may employ advanced control design methods to optimize performance. In addition, it will likely have a much higher level of automation than existing plants and may employ modern control methods to provide advanced functions such as trip avoidance strategies to reduce the demands on the protection system. A primary safety-related concern for advanced, highly integrated control systems is the potential that the plant may operate or fail in a way that results in transients that are not bounded by the plant safety analysis. Another key concern is that failure of complex control systems could inhibit the successful execution of required safety functions.

The inherent safety characteristics (e.g., a small operational excess reactivity, large thermal mass of moderator and fuel for slow heatup rates, a large negative temperature coefficient, inert gas coolant, ceramic fuel particle coatings that can withstand very high temperature without releasing fission products, a passive heat removal capability) of the HTGR designs proposed for NGNP may address the first concern by limiting the potential impact of control system inadequacy or failure as a consequence of the plant design. This determination depends on the results of the plant accident and transient analyses and the demonstrated fidelity of those findings.

Regarding the concern about the impact of the control system on the safety system, adherence with the independence requirements of IEEE 603-1991 generally provides the key basis for ensuring that the integrity of safety functions is adequately protected. Given the digital capacity to enable greater interconnection and integration among systems, additional guidance on issues such as communications independence and command prioritization has been provided by NRC through the interim staff guidance for digital I&C. If, as is the case for the ALWR designs, the NGNP automated control room maintains adequate independence between the control and safety systems, then the impact of automation will primarily involve operational control functions so the necessary assurance of adequate safety can be established based on the safety system implementation. Consequently, the assessment of the adherence to safety system requirements, in particular the independence criterion, will be a crucial aspect of any regulatory review for the highly automated control room of the NGNP.

Issues associated with automation in highly integrated control rooms are discussed in detail by Wood et al.² In addition, the impact of unique concepts of operation, such as multiunit control and coupled nuclear and industrial process control, are also presented in the Task 2 report.

5.2.2 Support system controls

The discussion in this report focuses on the protection and control design methods for the reactor and major heat transport systems. Other controls may eventually need to be examined further depending on as of yet unavailable design details. Some control systems in HGTRs may be new or unique and may have greater safety implications than control in traditional LWR power plants. Two such control systems which may need further examination are the magnetic bearing control for the helium circulator and shaft seal controls.

One potential concern regarding the magnetic bearing controller is that a failure of the control device and catcher bearings could cause the displacement of the impeller and motor shaft leading to failure of the pressure boundary in the circulator. The magnetic bearing control design issue has been raised as a part of this review but no details of the magnetic bearing controls and their safety implications in plants which employ them have been found in literature. This event, a control system failure leading directly to a loss of coolant accident is a possible accident with a much higher severity category than other control system failures in licensing reviews.

A related problem is helium shaft seals. The helium circulator motor and shaft are likely to be externally sealed. That is, the motor and impeller are sealed within the helium pressure boundary. However, the main coolant cannot be allowed to circulate freely around the motor and impeller because of dust in the coolant which could damage the circulator components and radioactive contamination deposits which would greatly increase the radiation exposure of workers during maintenance. The helium from the main reactor circuit must be kept out of the internal motor and impeller space by internal seals and a flow of higher pressure clean helium into the space toward the reactor. Because the consequences of failure are severe, control of the seal flow and cooling becomes an issue from a regulatory perspective.

5.3 System Classification

In the preliminary licensing proposal on the MHTGR presented by General Atomics to the NRC,³⁰ a licensing strategy was proposed to take advantage of the inherent safety of the HTGR and reduce the number of systems considered to perform safety-related functions. In this approach, certain functions that protect equipment but are not necessary for satisfying regulatory dose limits in accident analyses are designated as “investment protection systems” rather than “safety-related systems.”

The inherent safety function of HTGRs provides only limited protection of equipment other than the fuel itself. While the fuel is generally protected and radiation release is predicted to be within 10 CFR 100 limits when relying solely on passive response of the reactor system, other equipment important to investment and operation may be vulnerable at the temperatures that may exist in the reactor and confinement cavity when only the inherent passive cooling is available. Active components such as pumps, valves, motors, control rod drives, and instrumentation may in fact be damaged by the high temperatures reached when the plant is involved in a worst case event unless active cooling systems are operational. The class of support function that would cool the active components is what would be designated as investment protection.

The concept of investment protection as an intermediate class between safety-related and nonsafety-related is a licensing approach that has not been previously approved by the NRC. When the MHGTR pre-conceptual design was reviewed by the NRC, one of the unresolved issues was the concept of “investment protection” rather than “safety-related” designation for equipment analogous to LWR systems which are safety grade.

As for every reactor design, the determination of whether I&C functions should be considered as control or protection will depend on the results of transient and accident analyses for NGNP. Clearly, safety functions and their corresponding protective actions must be treated in accordance to safety system design requirements. The remaining control functions are designated according to the safety/nonsafety classification based on the determination of whether, through normal operation, system failure or inadvertent operation, they can affect the performance of critical safety functions. Thus, the treatment of the systems that perform these functions is dependent on analysis of the impact of these systems on the execution of safety functions. If the investment protection system of the NGNP is determined to be a nonsafety system, it still may be required to demonstrate augmented quality, following the guidance of Digital I&C ISG-02. This would be the case if it is allocated a role as a diverse means of performing an equivalent safety function in the event that a CCF disables protection afforded by another echelon of defense.

Nonsafety systems that are relied on for beyond design basis events to reduce core damage frequency below 10^{-4} /reactor year are treated under special requirements called “regulatory treatment of nonsafety systems” or RTNSS.

6. REFERENCES

1. T. L. Wilson, Jr., et al., *Task 1–Control and Protection Systems in VHTRs for Process Heat Applications*, LTR/NRC/RES/2010-001, Oak Ridge National Laboratory, Oak Ridge, TN, September 2010.
2. R. T. Wood et al., *Task 2–Highly Automated Control Room Design for VHTRs*, LTR/NRC/RES/2011-005, Oak Ridge National Laboratory, Oak Ridge, TN, September 2011.
3. *Proceedings of the 1993 ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, American Nuclear Society, Oak Ridge, TN, April 1993.
4. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 96)*, Vols. 1 and 2, American Nuclear Society, Penn State University, PA, May 1996.
5. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2000)*, American Nuclear Society, Washington, DC, November 2000.
6. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2004)*, American Nuclear Society, Columbus, OH, September 2004.
7. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2006)*, American Nuclear Society, Albuquerque, NM, November 2006.
8. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2009)*, American Nuclear Society, Knoxville, TN, April 2009.
9. *Proceedings of the ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2010)*, American Nuclear Society, Las Vegas, NV, November 2010.
10. L. M. Stevens, C. G. Rieger, and W. C. Phoenix, *HTGR Resilient Control System Strategy*, INL/EXT-10-19645, Idaho National Laboratory, Idaho Falls, ID, September 2010.
11. J. M. Maciejowski, *Predictive Control with Constraints*, Prentice-Hall, New York, 2002.
12. Gang Tao and P. V. Kokotović, *Adaptive Control of Systems with Actuator and Sensor Nonlinearities*, John Wiley and Sons, Inc., New York, 1996.
13. S. M. Mitchell and M. S. Mannan, “Designing Resilient Engineered Systems,” *Chemical Engineering Progress*, **102**(4), pp. 39–45 (April 2006).
14. C. G. Rieger, D. I. Gertman, and M. A. McQueen, “Resilient Control Systems: Next Generation Design Research,” pp. 632–636 in *2nd Conference on Human System Interactions*, Catania, Italy, (May 2009).
15. *Knowledge-Based Systems*, **15**(1–2), pp. 103–110, Sp. Iss. Si (January 2002).
16. J. R. Abrial, E. Borger, and H. Langmaack, Eds., *Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control*, Springer-Verlag, 1996.
17. L. Petre, M. Qvist, and K. Sere, *Distributed Object-Based Control Systems*, TUCS Report N. 241, Turku Centre for Computer Science, February 1999.

18. R. A. Kisner and G. V. S. Raju, *Automating Large-Scale Power Plant Systems: A Perspective and Philosophy*, ORNL/TM-9500, Oak Ridge National Laboratory, Oak Ridge, TN, 1984.
19. IEEE Std 603 1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
20. Regulatory Guide 1.206, Rev. 3, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, June 2007.
21. Title 10 of the *Code of Federal Regulations*, Part 50, Appendix A, Office of the Federal Register National Archives and Records Administration, 2011.
22. T. L. Wilson, Jr., et al., *Task 3—Models for Control and Control and Protection Systems Designs in VHTRs*, LTR/NRC/RES/2010-003, Oak Ridge National Laboratory, Oak Ridge, TN, May 2011.
23. S. J. Ball (Panel Chair), *Next Generation Nuclear Plant Phenomenon Identification and Ranking Tables (PIRTs), Volume 2: Accident and Thermal Fluid Analysis PIRTS*, NUREG/CR-6944, Vol. 2, March 2008.
24. SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs (SECY-94-084)," May 22, 1995. (ML003708005)
25. D. A. Copinger and D. L. Moses, *Fort Saint Vrain Gas Cooled Reactor Operational Experience*, NUREG/CR-6839 (ORNL TM-2003/223), Oak Ridge National Laboratory, Oak Ridge, TN, September 2003.
26. Preliminary Safety Information Document for the Standard MHTGR. Volume 1, DOE/HTGR-86-024, December 1, 1986.
27. D. Dilling, T. D. Dunn, and F. A. Silady, *A Vented Low Pressure Containment Strategy for the Modular High Temperature Gas-Cooled Reactor (MHTGR)*, General Atomics Project 7600, GA-A21622, April 1994.
28. A. Koster and D. Lee, "The PBMR Containment System," 2nd *International Topical Meeting on High Temperature Reactor Technology*, Beijing, China, September 22–24, 2004.
29. C. Rodriguez, J. Zgliczynski, and D. Pfremmer, *GT-MHR Operations and Controls*, General Atomics Project 7600, GA-A21894, November 1994.
30. *Pre-Application Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, December 1995.