Westinghouse Technology Systems Manual

Section 5.0

Introduction to Engineered Safety Features

TABLE OF CONTENTS

LIST OF FIGURES

5.0 INTRODUCTION TO ENGINEERED SAFETY FEATURES

Learning Objectives:

1. State the purposes of the Engineered Safety Feature (ESF) Systems.

2. Identify the three barriers designed to limit the escape of fission products to the environment.

3. Explain the following terms:

   a. Redundancy
   b. Physical and electrical separation
   c. Regulatory terms associated with safety:

      - Important to safety
      - Safety related
      - Safety grade

   d. Seismic Category I
   e. Diversity
   f. Single failure
   g. Active failure
   h. Passive failure
   i. ESF train

4. List the four design categories or conditions of operation, and give an example of each.

5. List the five acceptance criteria for the Emergency Core Cooling Systems (ECCSs).

5.0.1 Introduction

In a large nuclear generating station with a core output rated at over 3,000 MW thermal, about 6 pounds of fission products are produced each day the unit is operated at full power. To protect the public from these fission products, a multiple barrier concept is incorporated into the design of the plant.

The first barrier consists of an enclosed cylindrical cladding that surrounds the fuel pellets and is designed to contain the fission products.

The second barrier is the reactor coolant system (RCS) pressure boundary. This barrier is designed to withstand high pressures and temperatures. The thickness of this barrier varies from a few inches for the reactor coolant loop piping, about 8 inches for the reactor vessel walls, and about one-tenth of an inch for the steam generator U-tubes. Since the RCS pressure boundary surrounds the first barrier, it will contain any fission products that escape from the cladding.

The final barrier of protection is the containment (reactor building). Many approved designs are used, but all contain the reactor coolant system and provide a third barrier to the release of radioactivity to the public.

The three barriers and the protection against the loss of each barrier is required by the Code of Federal Regulations. The reactor trips based on avoiding departure from nucleate boiling (DNB) and excessive local power densities (kw/ft.) are installed to protect the first barrier (fuel cladding) from damage. The high pressure reactor trip and the pressurizer code safety valves provide protection for the second barrier (RCS) by limiting the pressure in the RCS to less than its design pressure. Finally, the design of the containment, its support systems, and allowable leakage specifications help to insure the integrity of the containment.

5.0.1.1 LOCA Description

Consider the effect on the fuel cladding and the containment if a gross failure of the reactor coolant system occurs without the benefit of the engineered safety features. When a loss-of-coolant accident (LOCA) occurs, hot pressurized reactor coolant is forced out of the reactor coolant system, and pressure in the RCS rapidly decreases. An automatic reactor shutdown occurs because of this decrease in pressure and the control rods drop into the core. The fission process in the core is all but stopped and heat production drops to the decay heat value. As the coolant rapidly escapes via the break, containment temperature and pressure begin to increase. In a short time the reactor coolant system has flashed to steam and the pressure has equalized with the pressure inside the containment. At this time the blowdown phase of the loss of coolant accident has ended.

The fuel cladding begins to heat up following the blowdown phase of the accident. When the cladding temperatures exceed 2200°F, a zirconium-water reaction starts to occur. The hydrogen produced from this chemical reaction escapes into the containment, and the exothermic reaction causes an extra heat input into the cladding. The extreme pellet temperatures cause increased fuel rod pressures and the weakened cladding begins to bow. As the zirconium-water reaction continues, the zircalloy cladding begins to undergo metallurgical changes and becomes brittle, adding to its destruction.

As a result of the cladding degradation, fission products are released from the reactor coolant system to the containment through the RCS break. Two of the three barriers have now failed, and the third barrier is threatened. The containment pressure has increased due to the blowdown phase and will cause the escape of fission products to the environment through minute leakage paths. For some plant designs, the potential for a gross failure of the containment due to a hydrogen explosion is of great concern. For others the continuous heat input into the containment can cause the pressure and temperature to increase to the point where the containment could rupture.

However, the engineered safety feature systems are installed in nuclear units to mitigate the consequences of the loss of the reactor coolant system pressure boundary. Among these systems are the emergency core cooling systems, which are actuated automatically during accident situations.

When a safety injection actuation signal is generated, borated water is pumped from the refueling water storage tank to the reactor coolant system, and the reactor vessel is refilled. This reflooding of the core from the refueling water storage tank is called the injection phase of the LOCA. With a flow of water into the core, decay heat is removed and the fission product release due to cladding failure is minimized. Consider the following major issues concerning the ECCSs.

First, if only one pump is installed and it fails, the consequences of a LOCA are the same as those previously discussed. But if a redundant pump that is also capable of supplying 100% of the required core cooling is installed, then the public can be protected. General Design Criterion (GDC) 35 of 10 CFR 50, Appendix A, requires redundant emergency core cooling systems.

Next, if only one sensor is used to actuate the ECCS, and it fails in a nonconservative direction, the core will not be reflooded, regardless of the number of ECCS pumps installed. If the sensor fails in the conservative direction, then an unnecessary actuation of ECCS equipment would occur. Therefore, IEEE-279 requires that redundant sensors, as well as redundant instrument strings, logic devices, and actuating devices, be installed.

After providing protection for the first two contingencies as stated above, a loss of power to the emergency core cooling system pumps must be considered. The normal power supplies to the pump motors come from the electrical grid by way of transformers, breakers, and buswork. Because this distribution system is vulnerable to thunderstorms, tornadoes, hurricanes, icing, and other acts of nature; a standby (emergency) power system is provided to ensure a power supply to the ECCS pump motors.

Redundant diesel generators are normally used as the standby power supply. GDC 17 of 10 CFR 50, Appendix A, outlines the requirements for electrical power distribution.

Finally, the emergency equipment must be designed to remain operational during a postulated seismic event. Paraphrasing 10 CFR 100, nuclear plant components designated to prevent or mitigate the consequences of accidents must be designed and built to remain functional during the design basis earthquake. Components satisfying this requirement are designated Seismic Category I.

In summary, the emergency core cooling systems must be redundant, actuated by redundant sensors, powered from redundant electrical power sources, and designed to be operational during seismic events.

5.0.1.2 Emergency Core Cooling Systems

Certain systems are installed to provide emergency cooling to the core in the event of a LOCA. These systems include the high, intermediate, and low pressure injection systems, and the cold leg accumulators .

The high pressure injection system, consisting of two redundant trains, provides protection for small-break LOCAs (SBLOCAs). This system pumps water from the refueling water storage tank (RWST) into the RCS cold legs during the injection phase. The high pressure system can also be used during the recirculation phase by connecting its suction to the residual heat removal system. In addition, this system injects boric acid from the RWST into the RCS during steam break accidents to offset the positive reactivity added by the rapid cooldown of the RCS.

The intermediate pressure injection system (safety injection system), provides protection for small to intermediate sized loss of coolant accidents. It has a greater capacity than the high pressure injection system but less than the low pressure injection system. Both safety injection system trains take suction from the RWST during the injection phase of the accident. Like the high pressure injection system, it can also be used during the recirculation phase by connecting its suction to the residual heat removal system.

The low pressure injection system (residual heat removal system) provides protection for a large loss of coolant accident. This system consists of two trains which can pump at a high rate of flow and at a low pressure from the RWST to the reactor coolant system. These pumps are also supplied with suction from the containment emergency core cooling recirculation sump. This suction source will be used during the recirculation phase of the accident. In addition to supplying cooling water to the reactor vessel, these pumps can also supply the suctions of the intermediate and high pressure injection systems.

The cold leg accumulators consists of four tanks filled with borated water and pressurized with nitrogen. When the RCS is pressurized and the reactor is at power, check valves, held closed by the higher reactor coolant system pressure, prevent the entry of water from the accumulators into the reactor coolant system. However, if a loss of coolant accident results in a reactor coolant system pressure lower than the pressure in the accumulators, then borated water will flow from the accumulators to the reactor vessel, via the cold legs. This system, unlike the high, intermediate, and low pressure injection systems, requires no actuation signal.

In addition to emergency core cooling systems, the engineered safety features design includes provisions to protect the containment barrier and to remove the core decay heat (auxiliary feedwater system).

5.0.1.3 Containment Barrier Protection

The containment spray system is installed to reduce the pressure inside the containment following a loss of coolant accident or a steam line break within the confines of the containment. The containment spray system satisfies the same design requirements as the emergency core cooling system. In addition to the containment spray system, other methods of controlling the containment pressure include containment fan coolers and hydrogen recombiners.

5.0.1.4 Decay Heat Removal

When the reactor trips, the rapid insertion of the control rods stops the heat production from the fission process. However, the heat production from fission product decay continues. This decay heat is normally removed by converting feedwater to steam in the steam generators. The main feedwater system does not meet safety system design criteria and if it is lost, the steam generators will boil dry. When the secondary inventory is lost, the decay heat will not be removed from the core. As the fission product decay continues, the resultant heat production causes an increase in reactor coolant temperature and a corresponding increase in RCS pressure. If left unchecked, the temperature and pressure increases will result in a challenge to the reactor coolant system pressure boundary.

The auxiliary feedwater system is designed to provide feedwater to the steam generators to remove decay heat in the event of a loss of main feedwater. The auxiliary feedwater system meets the same design criteria as the emergency core cooling system.

The emergency systems installed to mitigate the consequences of accidents are among the most important systems in the nuclear plant. Normally these systems are aligned for the injection phase. However, if the safety system is in use performing one of its non-safety functions, it will be automatically re-aligned to perform its safety function upon receipt of an engineered safety features actuation signal.

5.0.2 Terms

5.0.2.1 Redundancy

If a component such as a pump is installed to provide a safety function, a second 100% backup pump must also be installed. This convention is known as redundancy. Redundant instrument sensors, instrument strings, and logic devices are required to ensure that no single failure will prevent at least one of these components from performing their intended function.

5.0.2.2 Physical and Electrical Separation

All engineered safety feature systems must be physically separated so that a catastrophic failure of one system will not prevent another engineered safety feature system from performing its intended function. Electrical power to the engineered safety features comes from the transmission grid via transformers, breakers and bus work. Because this distribution system is vulnerable to thunderstorms, hurricanes, icing, and other acts of nature, a standby power system is provided to insure a reliable source of power. Redundant diesel generators are normally used for this standby power supply. These standby power supplies are normally arranged into redundant trains (typically Train A and Train B), which provide power to separate trains of redundant safety features.

5.0.2.3 Regulatory Terms Associated With Safety

1. Important to safety - Those structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. This encompasses the broad class of plant features that contribute in an important way to the safe operation and protection

of the public in all phases and aspects of facility operations. This includes "safety grade" or "safety related" as a subset.

2. Safety related - Those structures, systems, or components designed to remain functional during a safe shutdown earthquake (SSE) and are necessary to assure:

   a. The integrity of the reactor coolant system pressure boundary,
   b. The capability to shut down the reactor and maintain it in a safe shutdown condition, or
   c. The capability to prevent or mitigate the consequences of accidents which could result in potential off-site exposures comparable to the guidelines in 10CFR 100, Appendix A.

3. Safety grade - This term is not explicitly used in regulations. It is equivalent to "safety related," and is a subset of "important to safety."

5.0.2.4 Seismic Category I

Those structures, systems, and components, including their foundations and supports, designed to remain functional if the safe shutdown earthquake occurs have been designated as Seismic Category I.

The following constitutes the systems and components designated as Seismic Category I.

1. The reactor coolant pressure boundary,
2. The reactor core and vessel internals, and
3. Systems or portions of systems that are required for emergency core cooling, post-accident containment heat removal, and post accident containment atmosphere cleanup.

Seismic Category I design requirements extend to the first seismic restraint beyond the identified boundaries.

5.0.2.5 Diversity

Diversity refers to different methods of providing the same safety protection or function. An example of this is the containment fan cooler system and the containment spray system. Both of these systems are designed to lower the pressure inside the containment following a steam break or a loss of coolant accident inside the containment.

5.0.2.6 Single Failure (Active/Passive)

A "single failure" is an occurrence which results in the loss of capability of a component to perform its intended safety function when called upon. Multiple failures resulting from a single occurrence are to be considered as a single failure. Fluid process systems are considered to be designed to withstand an assumed single failure if neither a single active nor a single passive failure results in a loss of the safety function to the nuclear unit.

An “active failure” is a malfunction, excluding passive failures, of a component which relies on mechanical movement to complete its intended function on demand. Examples of active failures include the failure of a powered valve or a check valve to move to its correct position, or the failure of a pump, fan, or diesel generator to start.

Spurious action of a powered component originating within its actuation system shall be regarded as an active failure unless specific design features or operating restrictions preclude such spurious actions.

A “passive failure” is a breech of a fluid pressure boundary or blockage of a process flow path.

The design flow limit for a passive failure (i.e., flow from a pressure boundary breech or flow through the blockage of a process flow path) is analyzed by the utility. This is done by performing an analysis of passive failures in the system, considering conditions of operation and possible failure or leakage modes as appropriate. For example, a review of a system that contains piping, heat exchangers, valves, flanged joints, and system interface barriers might result in the definition of a design leak rate for passive failure in that system based on the maximum flow through a failed packing or mechanical seal rather than complete severance of the piping.

In lieu of this analysis, the designer must consider complete severance of the piping and an independently complete blockage of the process path as a passive failure.

5.0.3 General Design Requirements

The engineered safety feature systems are provided in nuclear power plants to mitigate the consequences of reactor plant accidents. Sections of the General Design Criteria (refer to Chapter 1.1) require the installation of specific ESF systems. Containment systems, the residual heat removal (RHR) system, emergency core cooling systems, containment heat removal systems, containment atmospheric cleanup systems and certain cooling water systems are typical of the systems required to be provided as ESF systems. Each of the ESF systems is designed to withstand a single failure without loss of its protective function capabilities during or following an accident condition.

5.0.3.1 Failure Criteria

The ESF systems are designed to withstand any single failure without loss of core and containment protection. However, this single failure is limited to either an active failure during the injection phase (a short period of time until the RWST empties) following an accident, or an active or a passive failure during the recirculation phase (a long period of time when water is taken from the containment recirculation sump, cooled by the RHR heat exchangers and pumped back into the RCS).

Most accidents are analyzed assuming a loss of off-site power conditions. This loss of off-site power is considered in addition the “single active failure.”

5.0.3.2 ESF Train

The engineered safety features which contain active components are designed with two independent trains. This convention is illustrated by the ECCSs, of which either train can satisfy all the requirements to safely shut down the plant or meet the final acceptance criteria following an accident.

The Technical Specifications state that one ECCS train consists of:

1. One centrifugal charging pump,
2. One safety injection pump,
3. One RHR pump,
4. An operable flow path from the RWST to the RCS and from the containment sump back to the RCS, and
5. Power supplies and instrumentation for the above items.

To guarantee that at least one train of the ECCS is available if an accident occurs, both trains must meet the operability requirements in the Technical Specifications whenever the temperature of the RCS is above 350°F. This will allow for the single active failure of the emergency power source (diesel generator), and still retain one train of ECCS for accident mitigation.

5.0.3.3 Typical Engineered Safety Feature Systems

The typical ESF systems that may be found at a Westinghouse nuclear power plant are listed below.

1. Containment - This Seismic Category I building provides a virtually leak-tight barrier to prevent the release of fission products to the environment.

2. Containment heat removal systems - These systems, containment spray and containment fan coolers, reduce the pressure and temperature inside the containment and remove fission products from the containment atmosphere.

3. Containment isolation system – This system provides isolation capability for the various lines penetrating the containment.

4. Containment combustible gas control system - The hydrogen recombiners control the concentration of hydrogen gas which may be released to the containment following an accident to assure containment integrity.

5. Emergency core cooling systems – These systems deliver the borated water from the RWST to the core following various postulated accidents.

6. Habitability systems – These systems provide the control room with adequate shielding, air purification, and climatic control.

7. Auxiliary feedwater system – This system provides makeup to the steam generators whenever the main feedwater system is not available and thus maintains the primary-to-secondary heat removal capability of the steam generators.

8. Class 1E electrical system - This vital electrical distribution system, including the emergency diesel generators, provides a reliable source of power to the active components of the ESF.

9. Essential support systems – These include any system or subsystem (component cooling water, essential raw cooling water, etc.) which would be required to operate in support of the above systems.

5.0.3.4 Design Categories or Conditions of Operation

Each facility shall, as a condition of licensing, include in its Final Safety Analysis Report (FSAR) a section titled "Accident Analysis." The requirements for the information contained in this section are outlined in 10 CFR 50.34 and are detailed in Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports. This regulatory guide sets up a standard approach to ensure the license applicant has analyzed both expected and unexpected transients and accidents, that conservative values are applied in the analysis, and that the plant design has incorporated an adequate margin of safety.

The accident analysis section of the FSAR shall include the analysis of several transients and accidents. These analyzed incidents are placed in four (4) categories or conditions of operation.

Condition I - Normal Operations

Condition I events are those occurrences which are expected to happen frequently or regularly in the course of power operation, refueling, maintenance, or changing power in the plant. Therefore, Condition I occurrences are accommodated with a margin between any plant parameter and the value of that parameter which would require either automatic or manual protective actions. Since Condition I events occur frequently or regularly, they must be considered from the point of view of affecting the consequences of fault conditions (Conditions II, III and IV). In this regard, analysis of each fault condition described is generally based on a conservative set of initial conditions corresponding to adverse conditions which can occur during Condition I operation. Below is a typical list of Condition I events:

1. Steady state and shutdown operations.

   a. Power operation (15-100% of full power)
   b. Start up (or standby) (critical, 0-15% of full power)
   c. Hot shutdown (subcritical, residual heat removal system in operation)
   d. Refueling

2. Operation with permissible deviations - Various deviations which may occur during continued operation as permitted by the plant Technical Specifications must be considered in conjunction with other operational modes. These include:

    a. Operation with components or systems out of service (such as power operation with a reactor coolant pump out of service)
    b. Leakage from fuel with clad defects
    c. Radioactivity in the reactor coolant

        - Fission Products
        - Corrosion Products
        - Tritium

    d. Operation with steam generator leaks up to the maximum allowed by the Technical Specifications
    e. Testing as allowed by the Technical Specifications

3. Operational testing

    a. Plant heatup and cooldown (up to 100°F/hour for the RCS; 200°F/hour for the pressurizer cooldown only)
    b. Step load changes (up to 10%/minute)
    c. Ramp load changes (up to 5%/minute)
    d. Load rejection up to and including a full load rejection transient

Condition II - Faults of Moderate Frequency

These faults, which are expected to happen on a once-per-year basis and at worst, result in a reactor trip with the plant being capable of returning to operations. By definition, these faults (or events) do not propagate to cause a more serious fault, i.e., a Condition III or IV event. In addition, Condition II events are not expected to result in fuel rod failures or the over pressurization of the RCS. The operational events that meet the above assumptions have been grouped below:

1. Uncontrolled rod cluster control assembly bank withdrawal from a subcritical condition
2. Uncontrolled rod cluster control assembly bank withdrawal at power
3. Rod cluster control assembly misalignment
4. Uncontrolled boron dilution
5. Partial loss of forced reactor coolant flow
6. Start-up of an inactive reactor coolant loop
7. Loss of external electrical load and/or turbine trip
8. Loss of normal feedwater
9. Loss of offsite power to the station auxiliaries.
10. Excessive heat removal due to feedwater system malfunctions
11. Excessive load increase incident
12. Accidental depressurization of the RCS
13. Accidental depressurization of the main steam system
14. Inadvertent operation of emergency core cooling system during power operation

Condition III - Infrequent Faults

Condition III occurrences are faults which are expected to happen once in the 40-year life of the plant. Such an event would result in the failure of only a small fraction of the fuel rods, although sufficient fuel damage might occur to preclude resumption of power operations for a considerable outage time. The release of radioactivity will not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius. A Condition III fault will not, by itself, generate a Condition IV fault or result in a consequential loss of function of the reactor coolant system or containment barriers. The following faults have been grouped into this category:

1. Loss of reactor coolant from small ruptured pipes or from cracks in large pipes which actuates the emergency core cooling system
2. Minor secondary pipe breaks
3. Inadvertent loading of a fuel assembly into an improper position
4. Complete loss of forced reactor coolant flow
5. Single rod cluster control assembly withdrawal at full power

Condition IV - Limiting Faults

Condition IV occurrences are faults which are never expected to take place but are postulated because the events are so severe that the consequences would include the potential for the release of significant amounts of radioactive material. These accidents are the most drastic and therefore represent the limiting design cases. Condition IV faults shall not cause a fission product release to the environment resulting in an undue risk to public health and safety in excess of the guideline values of 10 CFR Part 100. A single Condition IV fault shall not cause a consequential loss of required functions of systems needed to cope with the fault, including those of the emergency core cooling system and the containment. The following faults have been classified in this category:

1. Major ruptures of pipes containing reactor coolant up to and including the double-ended rupture of the largest pipe in the reactor coolant system (LOCAs)
2. Major secondary system pipe ruptures
3. Steam generator tube rupture
4. Single reactor coolant pump locked rotor
5. Fuel handling accident
6. Rupture of a control rod drive mechanism housing (rod cluster control assembly ejection)

5.0.3.5 Acceptance Criteria for the Emergency Core Cooling Systems (10 CFR 50.46)

In 1974, the final acceptance criteria for emergency core cooling systems for light water reactors were established. These criteria require the ECCS to be designed and built so that the calculated cooling performance following a full spectrum of postulated LOCA’s would meet the following limits during or following the accident.

1. Peak Cladding Temperature (PCT) shall remain less than 2200°F.

2. Maximum cladding oxidation shall not exceed 17% of the total cladding thickness.
3. Maximum hydrogen generated by the reaction of water or steam with the cladding shall not exceed 1% of the amount that would be generated if all the cladding reacted chemically with water or steam.
4. Coolable geometry - Any changes in core geometry shall be such that the core remains in a coolable configuration.
5. Long-term cooling - Core temperature, after the injection phase, shall be maintained at an acceptably low value. Decay heat shall be removed for the extended period of time required.

5.0.3.6 Engineered Safety Features Actuation Signals

Many of the engineered safety feature systems of a facility are actuated by any of the safety injection actuation signals, listed below:

1. High steam line flow coincident with low steam line pressure or low-low T_{avg}.
2. High steam line differential pressure - One steam line lower in pressure than at least two of the remaining three by 100 psid/or more.
3. Low pressurizer pressure – At least two of four measured pressurizer pressures less than setpoint.
4. High containment pressure – At least two of three measured containment pressures greater than setpoint.
5. Manual – Operation of one of two control board switches.

It should be noted that, with a few exceptions, each safety injection actuation signal achieves identical results. That is, regardless of the protection signal being generated, each signal causes the same equipment to be operated.

An additional ESF actuation signal is the containment spray actuation signal, which actuates the containment spray system when containment pressure reaches approximately half of design pressure.

5.0.4 Typical Analysis Limits and Assumptions

For conservatism, each accident that is analyzed assumes the most conservative conditions, setpoints, equipment operability, and other factors which could conceivably affect the severity of the event. Listed below are some of the assumptions used in the accident analysis.

1. Maximum time delays for reactor trip, safety injection actuation, steam line isolation valve closure, etc., are assumed.
2. Starting values for the various plant parameters will be assumed to be at their worst-case conditions.
3. Plant history, reactivity coefficients and other variables affecting the accident are chosen to produce the most severe transient.

5.0.4.1 Steam Line Break Accident Analysis

The steam break accident is outlined here as an example of the goals and concerns that are assumed in performing accident analysis.

The analysis is performed to demonstrate that:

1. There is no consequential damage to the primary system and the core remains intact.
2. Energy release for the worst-case break does not cause failure of the containment.
3. There is no return to criticality after the reactor trip for a break equivalent to a stuck-open steam bypass, relief, or safety valve.

5.0.4.2 Assumptions for Steam Line Break Analysis

The assumptions used for the steam line break accident are listed as follows:

1. The design end-of-life shut down margin at no-load, equilibrium xenon conditions, and with the most reactive rod stuck in its fully withdrawn position.

2. The negative moderator temperature coefficient corresponding to the end-of-life rodded core with the most reactive rod in the fully withdrawn position. The variation of the coefficient with temperature and pressure has been included.

3. The minimum capability for injection of concentrated boric acid solution corresponding to the most restrictive single active failure in the safety injection system. This corresponds to the flow delivered by one centrifugal charging pump delivering its full contents to the cold legs.

4. The design value of the steam generator heat transfer coefficient, including an allowance for tube fouling.

5. Hot channel factors corresponding to the worst-case stuck rod at end of core life.

6. Several combinations of break sizes and initial plant conditions have been considered in determining the core power transient which can result from large area pipe breaks:

    a. Complete severance of a pipe downstream of the steam flow restrictor with the plant initially at no-load conditions and all reactor coolant pumps running. (Figure 5.0-1).

    b. Complete severance of a pipe inside the containment at the outlet of the steam generator with the same plant conditions as above (Figure 5.0-2).

    c. Case (a) above with loss of outside power simultaneous with the generation of the safety injection signal (loss of ac power results in coolant pump coastdown).

d. Case (b) above with the loss of offsite power simultaneous with the safety injection signal. A fifth case was analyzed consistent with the criterion stated earlier that there should be no return to criticality after reactor trip in the event of the spurious opening of a steam bypass or relief valve.

e. A break equivalent to a steam flow of 247 lb/sec at 1100 psi from one steam generator with offsite power available.

7. Initial hot shutdown conditions were considered for all of the above cases since this represents the most pessimistic initial condition for the accident.

8. The containment pressure response was evaluated for case 6.b above, since this results in the most severe steam break containment transient. In addition to the full contents of the faulty steam generating unit being delivered to the containment, it was also assumed that break flow was delivered from the other three steam generators through a failed nonreturn valve in the broken steam line. The latter flow continues until the main steam isolation valves close in the intact steam lines.

9. Perfect moisture separation in the steam generator is assumed. This assumption leads to conservative results since, in fact, considerable water would be discharged. Water carryover would reduce the magnitude of the temperature decrease in the core and the pressure increase in the containment.

5.0.4.3 Systems Which Provide Protection Against Steam Line Break Accidents

The following protection signals and plant features mitigate the consequences of a main steam line rupture.

1. Safety injection actuation signal (any of the following):

   a. High steam line flow
   b. High steam line differential pressure
   c. Low pressurizer pressure
   d. High containment pressure

2. Reactor trip (any of the following):

   a. High neutron flux
   b. Overpower ΔT
   c. Safety injection reactor trip

3. Main feedwater isolation signal, generating the following responses:

   a. Close feedwater isolation valves
   b. Close feedwater control valves
   c. Close feedwater control bypass valves
   d. Trip main feedwater pumps

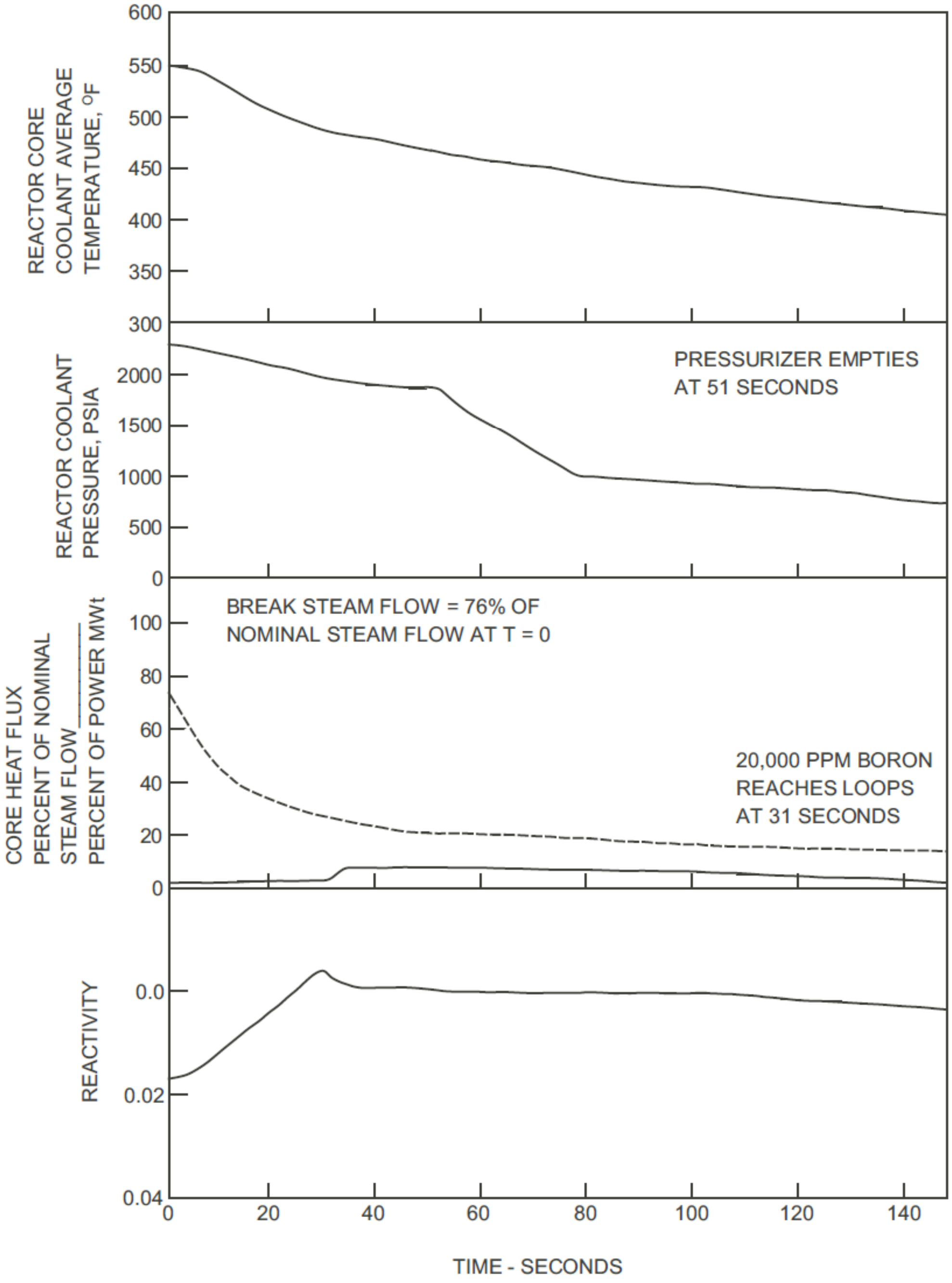
4. The shutting of the main steam isolation valves and/or the affected generator's main steam check valve prevents the blowdown of more than one steam generator for any break location.

5. The steam line flow venturi of the affected steam generator limits break flow.

5.0.5 Summary

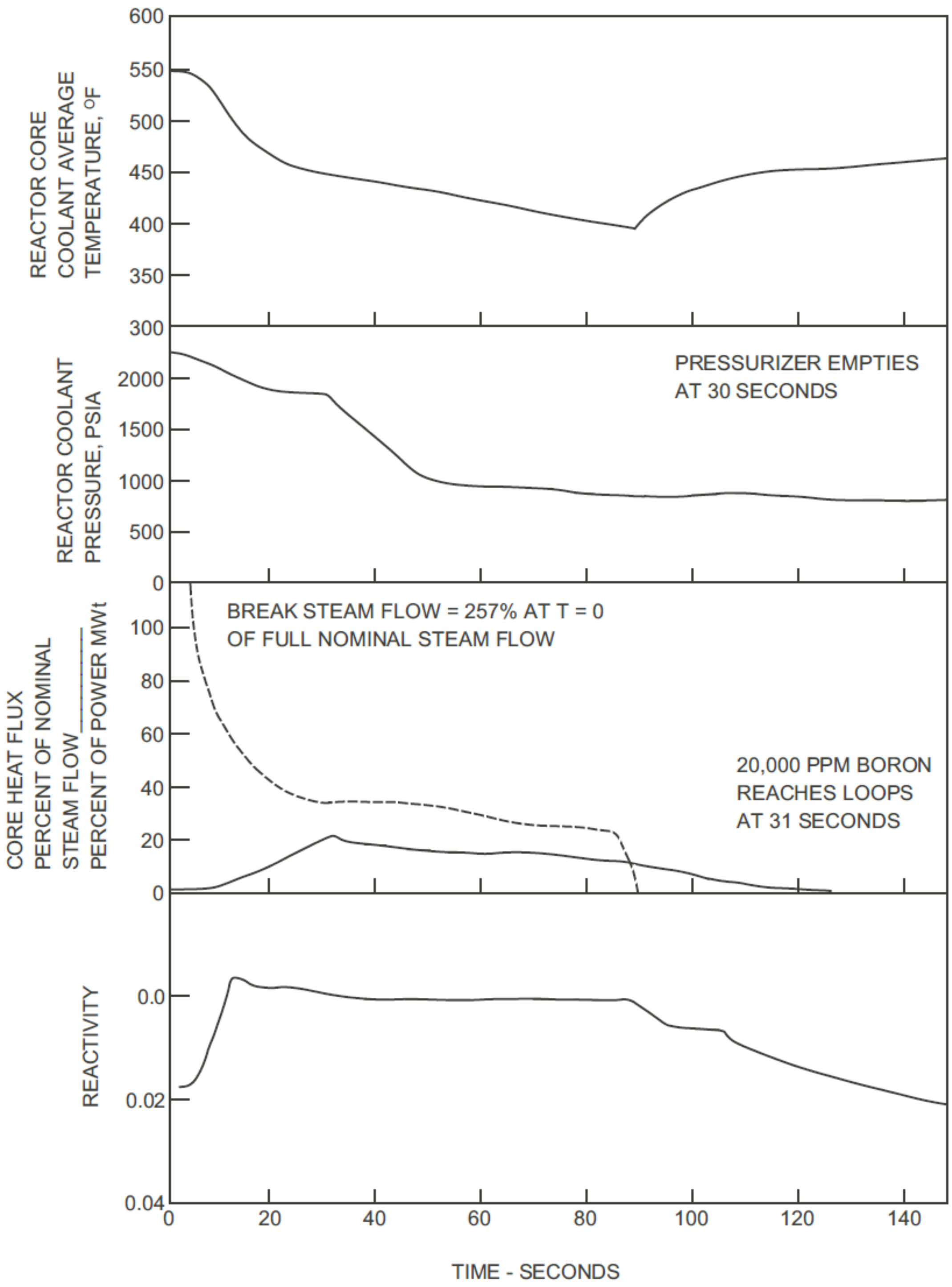
To protect the public from fission products, multiple barriers of protection are incorporated into the design of a commercial pressurized water reactor plant.

If the reactor enters unsafe regions of operation, the reactor protection system will generate a reactor trip to protect the cladding and reactor coolant system pressure boundary (first two barriers of protection). If an accident has occurred, such as a loss-of-coolant accident (LOCA), the reactor protection system actuates the engineered safety feature systems to mitigate the consequences of the accident and to protect the containment (third and final barrier of protection). The engineered safety feature systems must be redundant, actuated by redundant sensors and instrument strings, physically separated, powered from redundant electrical power supplies, and designed to remain operational during seismic events.



Safety Injection with Offsite Power

Figure 5.0-1 Steam Line Break Downstream of Flow Measuring Nozzle



Safety Injection with Offsite Power

Figure 5.0-2 Steam Line Break at Exit of Steam Generator