UCID- 18698, Vol. I

Schoch - XTMA

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VI-7.A3 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION AND CONTROL PORTIONS OF THE ECCS ACTUATION SYSTEM FOR THE DRESDEN II NUCLEAR POWER PLANT

Gerald St. Leger-Barter

November 1980

Lawrence Livermore Laboratory

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

DISCLAIMER

Available from: National Technical Information Service - U.S. Department of Commerce
5285 Port Royal Road - Springfield, VA 22161 - $6.00 per copy - (Microfiche $3.50)

ABSTRACT

This report documents the technical evaluation and review of NRC Safety Topic VI-7.A.3, associated with the electrical, instrumentation, and control portions of the classification of the ECCS actuation system for the Dresden II nuclear power plant, using current licensing criteria.

FOREWORD

This report is supplied as part of the Systematic Evaluation Program being conducted for the U.S. Nuclear Regulatory Commission by Lawrence Livermore National Laboratory. The work was performed under U.S. Department of Energy contract number DE-AC08-76NV01183.

TABLE OF CONTENTS

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VI-7.A.3 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION AND CONTROL PORTIONS OF THE ECCS ACTUATION SYSTEM FOR THE DRESDEN II NUCLEAR POWER PLANT

Gerald St. Leger-Barter
Lawrence Livermore National Laboratory

1. INTRODUCTION

This safety topic deals with the testability and operability of the emergency core cooling system (ECCS) actuation system. The ECCS test program should demonstrate a high degree of availability of the system to perform its design function. This report reviews the plant design to assure that all ECCS components, including the pumps and valves, are included in the component and system test, the frequency and scope of the periodic testing is identified, and the test program meets the requirements of the review criteria detailed in Section 2 of this report.

2. CURRENT LICENSING CRITERIA

GDC 37, entitled, "Testing of Emergency Core Cooling System," states in item 3 that:

> The ECCS be designed to permit appropriate periodic pressure and functional testing to assure the operability of the system as a whole and, to verify under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection system, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

Branch Technical Position ICSB 25, entitled, "Guidance for the Interpretation of GDC 37 for Testing and Operability of the Emergency Core Cooling System as a Whole," states that:

> All ECCS pumps should be included in the system test.

Regulatory Guide 1.22, entitled, "Periodic Testing of the Protection System Actuation Functions," states in Section D.1.a that:

> The periodic tests should duplicate as closely as practicable the performance that is required of the actuation devices in the event of an accident.

Regulatory Guide 1.22 also states in Section D.4 that:

> Where actuated equipment is not tested during reactor operation, it should be shown that:
>
> a. There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant;
>
> b. The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation, and
>
> c. The actuated equipment can be routinely tested when the reactor is shut down.

Standard Review Plan, section 7.3, Appendix A, entitled, "Use of IEEE Std 279 in the Review of the ESFAS and Instrumentation and Controls of Essential Auxiliary Supporting Systems," states in Section 11.b that:

> Periodic testing should duplicate, as closely as practical, the integrated performance required from the ESFAS, ESF systems, and their essential auxiliary supporting systems. If such a "system level" test can be performed only during shutdown, the testing done during power operation must be reviewed in detail. Check that "overlapping" tests do, in fact, overlap from one test segment to another. For example, closing a circuit breaker with the manual breaker control switch may not be adequate to test the ability of the ESFAS to close the breaker.

3. REVIEW GUIDELINES

(1) Verify that the test conditions come as close as possible to the actual performance required by ECCS during accident mitigation. (GDC-37 item 3, ICSB-25, RG 1.22-D.1.a, SRP 7.3 - Appendix A-11.b.)

(2) Verify that the system test covers from end to end (sensor through actuated device). If partial tests are performed, verify that the overlapping tests indeed overlap from one test segment to another. (GDC-37 item 3, ICSB-25, SRP 7.3 - Appendix A-11.b, RG 1.22-D.2.)

(3) Summarize the ECCS system surveillance testing interval as defined in the plant's technical specification.

4. SYSTEM DESCRIPTION

Means are needed to provide continuity of core cooling during those postulated accident conditions where it is assumed that mechanical failures occur in the primary system and coolant is partially or completely lost from the reactor vessel. Also normal auxiliary power is unavailable to drive the feedwater pumps or the loss of coolant occurs at a rate beyond the capability of the feedwater system. Under these circumstances core cooling is accomplished by means of the emergency core cooling system (ECCS). The ECCS consists of two independent core spray subsystems, the low pressure coolant injection (LPCI) subsystem, the high pressure coolant injection (HPCI) subsystem and the automatic pressure relief subsystem. Although these subsystems were each designed to specific design bases, the overall ECCS design bases are:

> The ECCS is designed to prevent fuel cladding melting for any mechanical failure of the primary system, up to and including a break area equivalent to the largest primary system pipe.
>
> The entire spectrum of line breaks, up to and including this maximum, is designed to be protected against by at least two independent cooling methods which are activated automatically.
>
> No reliance is assumed to be placed on external sources of power.

4.1 CORE SPRAY SUBSYSTEM

The core spray subsystem consists of two independent spray systems each with its own pump, valves, and associated piping and instrumentation. The water source is common to both systems and can be from the suppression pool in the torus, or by appropriate valving, from the contaminated demineralized water storage tank. Initiation of the core spray subsystem occurs on signals indicating reactor low-low water level and reactor low pressure or high drywell pressure. Low-low water level

and high drywell pressure are each detected by four independent level and pressure switches connected in a form of one-of-two-twice logic array. These same signals also initiate starting of the diesel generator. Water injection can start when the admission valve is opened and when the reactor vessel pressure drops below pump discharge pressure (350 psig). The pumps are operated on the minimum flow bypass which discharges back to the suppression pool. During this period the pumps are running while the admission valves are closed. The minimum flow bypass valves close when the flow through the main flow lines exceeds a preset value. Rated flow is sprayed over the top of the core at 90 psig in the reactor vessel. Opening of the admission valves is accomplished only after the reactor pressure decays to approximately the design discharge pressure of the pump, at which time the permissive signal to open the valves is initiated by two pressure switches connected in a one out of two logic array. When the vessel pressure decreases to below the shutoff head of the core spray subsystem, core spray injection begins.

4.2 LOW PRESSURE COOLANT INJECTION SUBSYSTEM

The LPCI subsystem consists of two main subdivisions: one, the LPCI system and the other, the containment cooling system. The major equipment of the entire subsystem consists of two heat exchangers, four containment cooling service water pumps, four main system pumps, two drywell spray headers, a suppression chamber spray header, and associated valving, piping and instrumentation. The LPCI piping injects the water into the outlet headers of the main recirculation pumps. During LPCI subsystem operation, water is taken from the suppression pool and is pumped into the core region of the reactor vessel via one of the two recirculation loops. (There is also a connection on the contaminated demineralized condensate storage tank to make condensate available for use in functional testing of the system.) Full flow capacity for the LPCI subsystem is available by operating three of the four main system pumps providing redundancy of pump capacity.

The system pumps are activated on either a signal of reactor low-low water level and reactor low pressure or a signal of high drywell pressure similar to that received by the core spray pumps. The initiation signal also trips the recirculation pumps and supplies a start signal to the diesel

generator which will provide power for the pump prime mover if normal auxiliary power has failed. The check and admission valves in the high pressure part of the system operate on reactor low pressure signal similiar to that of the valving on the core spray subsystem, thereby establishing a flow path. There is a minimum flow bypass line (not so named or referred to in the FSAR) through valves 1501-13A (and B). When flow through the LPCI lines to the recirculation pump outlet lines exceeds a preset value of the flow switch, the bypass valves 1501-13A (and/or B) close. Instrumentation is provided to sense the water level in the reactor shroud, which causes necessary valves to close or open (as needed) to establish the full LPCI flow. Instrumentation also determines whether there is a recirculation line break and appropriate valving is selected to inject LPCI flow into the recirculation leg which retains piping integrity. Since the LPCI flow passes through heat exchangers, heat may be rejected from the containment by starting the containment cooling service water pumps to cool the heat exchangers when sufficient electrical power is available. The containment cooling function can be performed with the residual heat removal system after the core is flooded.

4.3 HIGH PRESSURE COOLANT INJECTION SUBSYSTEM

The HPCI subsystem is provided to ensure that adequate core cooling takes place for all break sizes which do not result in rapid depressurization of the pressure vessel. The system meets this requirement without reliance on an external power source for the injection system.

The HPCI subsystem consists of a single steam turbine driving a multi-stage high pressure pump and a gear driven single stage booster pump, valves, high pressure piping, water sources, and instrumentation. The turbine is driven with steam from the reactor vessel. Exhaust steam from the turbine is discharged to the suppression pool. Suction for the HPCI pump is taken from the suppression pool. Suction for the HPCI pump can also be taken from the condensate storage tank by remote manual operation. The water is pumped into the reactor vessel through the feedwater sparger and water leaving the vessel through a line break drains by gravity back to the suppression pool.

Operation of the system is dependent upon reactor water level signals. Either low water level or high primary containment pressure signals start the system, and high water level will stop it. A minimum flow bypass system directing flow back to the suppression chamber via valve 2301-14 is provided for pump protection. The auto-open permissive for this valve is only valid when it is not fully closed. This valve closes when HPCI flow into the the main feedwater leg is above the preset value for the flow switch FSL 2-2354. The level and pressure switch for starting (i.e., opening valve 2301-3 to provide steam to the HPCI turbine) are in a one-of-two-twice logic array similar to that of the reactor protection system. The high water level switches for stopping HPCI flow operate in two-of-two logic. The high water level switches stop the HPCI flow by tripping the HPCI turbine but should the drywell pressure be high or the low water level mark be reached again the HPCI turbine trip is reset. The system will automatically maintain reactor water level between low level and high level if the break size is within the capacity of the pump and the reactor is not depressurized below 165 psia.

To inject water at a high pressure, three major active components must operate. A motor-operated valve must open to admit steam to the turbine driving the pump, a motor-operated valve must open to admit the discharge flow from the pump into the reactor feedwater line, and the turbine driven pump itself must operate.

4.4 AUTOMATIC PRESSURE RELIEF SUBSYSTEM

The automatic pressure relief subsystem is provided for backup of the HPCI subsystem and performs the function of vessel depresssurization for all small breaks. When the automatic pressure relief subsystem is actuated, the critical flow of steam through the relief valves results in a maximum energy removal rate with a corresponding minimum mass loss. Since the automatic pressure relief subsystem does not provide coolant make up to the reactor, its function is considered only in conjunction with the LPCI or core spray subsystems as a backup to the HPCI.

There are two power sources for this subsystem with automatic switchover for reliability: one is the 125-volt main bus No. 2; the other is reserve bus No. 2 (normally supplied from Unit III's dc system) to power the solenoid valves. There are five valves in this system, of which one is a Target Rock solenoid-operated air-assisted valve and the other four are directly solenoid-operated electromatic valves. There are two actuation chains to operate the automatic pressure relief subsystem for the EECS: one on main bus No. 2, and the other supplied by power with the same switchover arrangement as the solenoid valve operators. Either actuation chain will operate the valves and three basic functions must be completed for the chain to be complete. Each function is entered into the chain twice from separate sensors. Automatic actuation requires coincident reactor low-low water level and high drywell pressure with one set maintained for a period of about 2 minutes and the other set without a time delay. This is required in conjunction with LPCI and/or core spray pump operation sensed by two of the LPCI and/or core spray pressure switch relay logic functions. The time delay is in series with the blowdown activation signal to allow the coolant injection systems to achieve proper operation before actuation of the relief valves.

5.0 EVALUATION AND CONCLUSIONS

5.1 CORE SPRAY SUBSYSTEM

The core spray subsystems are designed so that each component of the system can be tested periodically. The instrumentation for initiation is tested and calibrated on a three-month cycle using test lines. A logic system functional test and a simulated automatic actuation test is completed at each refueling outage.

The pumps and valves of the system are subject to preoperational tests and periodic (quarterly) tests during operation using test lines. Once each quarter it is to be verified that each pump delivers at least 4500 gpm against a system head corresponding to a reactor vessel pressure of 90 psig. The condensate storage tank water is used for initial flushing and periodic testing of the system.

A test line capable of full system flow is connected from a point near the outside isolation valve back to the suppression chamber. Flow can be diverted into this line to test operability of the pumps and control system during reactor operation.

Each core spray subsystem may be tested individually during reactor operation. The pumps, admission valves and testable check isolation valves may all be tested independently. In the event that a reactor low-low water level and reactor low pressure signals occur or a high drywell pressure actuation signal occurs during a loop test, the loop not under test will start automatically. The loop being tested will return automatically to the operational mode and will then restart automatically.

The power sources for the core spray subsystems are located on separate emergency buses that have provisions to protect them from adverse environments. Power for these emergency buses can be supplied from the diesel generators if offsite power is not available. With core spray pump 1401-2A on

bus 23-1 it implies that it is supplied by the auxiliary transformer 21 fed from the main generator. Assuming the core spray is required coincidentally with a scram and a turbine trip, this bus would have to be supplied by the diesel generator. The other core spray pump is powered by bus 24-1 fed through transformer 22. Transformer 22 being fed from the switchyard.

The test frequencies for the components of the core spray subsystem are shown in Table 5.1.

Based on the information available it is concluded that the core spray subsystem of the ECCS meets the curent licensing criteria listed in section 2 of this report.

5.2 LOW PRESSURE COOLANT INJECTION SUBSYSTEM

The LPCI/containment cooling systems are designed so that each component of the system can be tested and inspected periodically to demonstrate availability of the system. The LPCI subsystem is initiated by the same parameters as the core spray subsystem and the instrumentation is calibrated on a three-month cycle. A logic system functional test and simulated automatic actuation test is completed at each refueling outage.

The pumps and valves of the system are subject to preoperational tests and periodic (quarterly) tests during operation. A design flow functional test of the LPCI pumps will be performed once each quarter during normal plant operation by taking suction from the suppression pool and discharging through the test lines back to the suppression pool. The discharge valves to the reactor recirculation loops remain closed during this test and reactor operation is undisturbed. An operational test of these discharge valves will be performed by shutting the downstream valve after it has been satisfactorily tested and then operating the discharge valve. The discharge valves to the containment spray headers are checked in a similar manner by operating the upstream and downstream valves individually. Control system design provides automatic return from test to operating mode if LPCI initiation is required during testing. The initiating conditions for the LPCI also start the diesel

generators so that ac power is available if offsite power is not available. The LPCI pumps are split, two each on bus 23-1 and two each on bus 24-1 with the same arrangement for power source selection as the core spray pump subsystem (i.e., immediate start with offsite auxiliary power and time delayed start if diesel generator power only is available). The containment and pressure suppression pool cooling subsystem's pumps are the same ones used for the LPCI; the valve sequencing determines the cooling mode. The valving to containment spray from the LPCI pumps is accomplished at operator's discretion. A reactor low water level inside the shroud interlock is provided to prevent LPCI flow from being diverted to the containment spray system unless the core is flooded. A key lock switch permits this interlock to be overridden only if containment pressure (1 of 2 taken twice) is still above 1 psi. The test frequencies for logic functional testing and the components of the low pressure coolant injection/containment spray subsystem are shown in Table 5.1. The calibration interval for the instrumentation is shown in the Technical Specifications Table 4.2.1.

Based on the information available it is concluded that the low pressure coolant injection subsystem of the ECCS meets the current licensing criteria listed in section 2 of the report.

5.3 HIGH PRESSURE COOLANT INJECTION (HPCI) SUBSYSTEM

The HPCI subsystem is designed so that each component of the system can be tested on a periodic basis. The instrumentation for initiation is calibrated on a three-month cycle.

A logic system functional test and simulated automatic actuation test is accomplished at each refueling outage.

The plant Technical Specifications call for surveillance testing once per quarter to verify that the HPCI pump delivers at least 5000 gpm against a system head corresponding to a reactor vessel pressure of 1150 psig to 150 psig. A test of the system up to the isolation valve can be conducted with steam from the reactor vessel. The steam admission valve is opened, driving the turbine-pump unit at its rated output. The valves from the suppression

chamber and to the feedwater line remain closed and water is pumped from the condensate storage tank, through the system, and returned to the condensate storage tank by way of the test line. To assure proper operation of the valves and strainers when pumping from the suppression chamber, the turbine-pump unit is run at a reduced rate by throttling at the turbine and pumping from the suppression chamber and returning the flow back to the suppression chamber by way of the minimum bypass line. In the event that an accident signal occurs while the HPCI subsystem is being tested, the subsystem is automatically restored to the automatic startup status and will begin operation. The HPCI subsystem is designed to operate without external power for the pump prime mover and uses station battery for valve operation.

The test frequencies for the components of the HPCI subsystem are shown in Tabl 5.1

Based on the information available it is concluded that the HPCI subsystem of the ECCS meets the current licensing criteria listed in section 2 of this report.

5.4 AUTOMATIC PRESSURE RELIEF SUBSYSTEM

Pressure relief of the reactor vessel may be accomplished manually by the operator or without operator action by the automatic pressure relief circuitry, either as overpressure relief or as part of the ECCS. A manual actuation test of each valve is required on an interval determined by observed failure rates. Proper operation is to be verified by observation of other steam flow parameters. Individual sensors for the automatic pressure relief subsystem are tested and calibrated singly without initiating the valves safety function. The plant Technical Specifications indicate a three-month calibration cycle. These specifications also require that a logic system functional test and simulated automatic actuation test are accomplished during each operating cycle. With the system powered from the 125-volt dc station battery system it is not sensitive to onsite/offsite ac power sources. The referenced drawings do not indicate operating air reserve accumulators for the

Target Rock valve but this is only one of the five APRS valves. The four electromatic valves are 125-volt dc operated which are supplied either by the station 125 volt battery or via either charger. There are two battery chargers which are on busses which can be supplied by either diesel generator (2 or 2/3).

The test frequencies for the components of the automatic pressure relief subsystem are shown in Table 5.1.

Based on the available information it is concluded that the automatic pressure relief subsystem of the ECCS meets the current licensing criteria listed in section 2 of this report.

TABLE 5.1

SURVEILLANCE REQUIREMENTS *

CORE AND CONTAINMENT COOLING SYSTEM

Applicability;

The operational readiness of the following subsystems shall be demonstrated in accordance with the Inservice Testing Program for Pumps and Valves defined in Section 1.0 (F.F.) of Dresden II Plant Technical Specifications. Additional requirements for each subsystem are listed below.

Objective

To verify the operability of the core and containment cooling subsystems.

Specification:

A. Surveillance of Core Spray Subsystem

1. Once each quarter, it shall be verified that each pump delivers at least 4500 gpm against a system head corresponding to a reactor vessel pressure of 90 psig.

2. A simulated Automatic Actuation Test shall be completed each refueling outage.

3. The Core Spray header Δp instrumentation shall be checked as follows:

check	once/day
calibrate	once/3 months
test	once/3 months

4. A Logic System Functional Test shall be completed each refueling outage.

B. Surveillance of LPCI/Containment Cooling Subsystems

1. Once each quarter, it shall be verified that three LPCI pumps deliver at least 14,500 gpm against a system head corresponding to a reactor vessel pressure of 20 psig.

2. A simulated Automatic Actuation Test shall be completed each refueling outage.

3. A Logic System Functional Test shall be completed each refueling outage.

* Extracted from the Dresden II Plant Technical Specifications, section 4.5

Table 5.1 cont.

4. During each five year period, an air test shall be performed on the drywell spray headers and nozzels.

5. Once each quarter, it shall be verified that each containment cooling water pump can be deliver at least 3500 gpm against a pressure of 180 psig.

C. Surveillance of the HPCI Subsystem.

1. Once per quarter, it shall be verified that the HPCI pump delivers at least 5000 gpm against a system head corresponding to a reactor vessel pressure of 1150 psig to 150 psig.

2. A Simulated Automatic Actuation Test shall be completed each refueling outage.

3. A Logic System Functional Test shall be completed each refueling outage.

D. Surviellance of the Automatic Pressure Relief Subsystem

1. During each operating cycle the following shall be performed:

   (a) A simulated automatic initiation which opens all pilot valves.

   (b) A logic system functional test shall be performed each refueling outage.

   (c) A visual inspection of the target rock and relief valve line restraints in the torus to verify structural integrity for continued operation.

2. After March 1, 1979, the following test program shall be performed:

   (a) With the reactor at $\geq$ 100 psig in the Steam Dome each relief valve shall be manually opened. Relief valve opening shall be verified by a compensating turbine bypass valve or control valve closure.

   (b) The initial required test interval shall be determined by the number of remotely operated relief valves found inoperable from March 1, 1978 to March 1, 1979.

   (c) The initial valve tests shall be completed by the earlier of the completion of the next refueling outage occurring after March 1, 1979 or the time period defined by March 1, 1979 plus the initial test interval determined above.

6.0 SUMMARY

The Dresden Station Unit II nuclear power plant ECCS testing complies with the current licensing criteria listed in section 2 of this report.

It was noted that there were no direct references to explicit testing or observation of the valving for the minimum flow bypass lines for the core spray, low pressure coolant injection, and the high pressure coolant injection subsystem pumps. The minimum flow bypass line valves for the core spray, LPCI, and HPCI subsystems are normally open. Test procedures indicate that operators shall verify the valves changing state during tests.

REFERENCES

1. Code of Federal Regulations, Title 10, Part 50 (10 CFR 50) Appendix A, (General Design Criteria 37), 1979.

2. U.S. Nuclear Regulatory Commission, Branch Technical Position ICSB 25, "Guidance for Interpretation of GDC 37 for Testing Operability of the Emergency Core Cooling System as a Whole."

3. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.22, "Periodic Testing of the Protection System Actuation Functions."

4. U.S. Nuclear Regulatory Commission, Standard Review Plan, Section 7.3, Appendix A, "Use of IEEE-Std-279 in the Review of the ESFAS and Instrumentation and Controls of Essential Auxiliary Supporting Systems."

5. Commonwealth Edison Company, Dresden Station Unit II Final Safety Analysis Report.

6. Commonwealth Edison Company, Dresden Station Unit II Technical Specifications.

7. Dresden II Mechanical Drawing, M-27, April 1977, Core Spray Piping.

8. Dresden II Mechanical Drawing M-29, September 1977, LPCI Piping.

9. Dresden II Mechanical Drawing M-51, June 1977, HPCI Piping.

10. Dresden II Mechanical Drawing M-12, August 1977, Main Steam Piping.

11. Dresden II Electrical Drawing 12 E 2429, September 1976, Relaying for Core Spray Pumps.

12. Dresden II Electrical Drawing 12 E 2430, February 1977, Core Spray Systems 1 and 2.

13. Dresden II Electrical Drawing 12 E 2436, September 1976, LPCI/Containment Cooling Pumps Switch Gear Control.

14. Dresden II Electrical Drawing 12 E 2437, September 1976, LPCI/Containment Cooling System 1.

15. Dresden II Electrical Drawing 12 E 2438, September 1976, LPCI/Containment Cooling System 2.

16. Dresden II Electrical Drawing 12 E 2527, September 1976, HPCI Sensors and Auxiliary Relays.

17. Dresden II Electrical Drawing 12 E 2528, December 1976, HPCI Valves and Turbine Auxiliaries.

18. Dresden II Electrical Drawing 12 E 2529, December 1976, HPCI Valves.

19. Dresden II Electrical Drawing 12 E 2461, September 1976, Auto Blowdown Control.

20. Dresden II Electrical Drawing 12 E 2462, September 1976, Auto Blowdown Control.

APPENDIX A

1. Topic VI-3, "Containment Pressure and Heat Removal Capability."

2. Topic VI-4, "Containment Isolation System."

3. Topic VI-7, "Emergency Core Cooling System".

4. Topic VI-7.C, "ECCS Single Failure Criterion and Requirements for Locking Out Power to Valves Including Independence of Interlocks on ECCS Valves."

5. Topic VI-9, "Main Steam Isolation."

6. Topic VI-10, "Selected ESF Aspects".

Technical Information Department · Lawrence Livermore Laboratory
University of California · Livermore, California 94550

Schoo - KTRA

UCID-18698, Vol. II

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VI-10.A ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION AND CONTROL PORTIONS OF THE TESTING OF REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES, INCLUDING RESPONSE TIME FOR THE DRESDEN STATION, UNIT II NUCLEAR POWER PLANT

Gerald St. Leger-Barter

November 1980

Lawrence Livermore Laboratory

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

8102170035

DISCLAIMER

Available from: National Technical Information Service - U.S. Department of Commerce
5285 Port Royal Road - Springfield, VA 22161 - $6.00 per copy - (Microfiche $3.50)

ABSTRACT

This report documents the technical evaluation and review of NRC Safety Topic VI-10.A, associated with the electrical, instrumentation, and control portions of the testing of reactor trip systems and engineered safety features including response time for the Dresden II nuclear power plant, using current licensing criteria.

FOREWORD

This report is supplied as part of the Systematic Evaluation Program being conducted for the U.S. Nuclear Regulatory Commission by Lawrence Livermore National Laboratory. The work was performed under U.S. Department of Energy contract number DE-AC08-76NV01183.

TABLE OF CONTENTS

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VI-10.A ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION AND CONTROL PORTIONS OF THE TESTING OF REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES, INCLUDING RESPONSE TIME FOR THE DRESDEN STATION UNIT II NUCLEAR POWER PLANT

Gerald St. Leger-Barter

1.0 INTRODUCTION

This safety topic deals with the testability and operability of the reactor trip system (RTS) and the engineered safety feature (ESF) systems. The RTS and ESF test program should demonstrate a high degree of availability of the systems and that the response times assumed in the accident analysis are within the design specifications.

This report reviews the plant design to assure that all RTS components are included in the component and system test, that the frequency and scope of the periodic testing is adequate, and that the test program meets the requirements of the General Design Criteria (GDC) and the Regulatory Guides (RG) defined in Section 2 of this report.

This report will also address the containment spray system as a typical example to all ESF systems. A review of the plant design will be made to assure that all containment spray system portions of the ESF components, including the pumps and valves, are included in the component and system test, that the frequency and scope of the periodic testing is adequate, and that the test program meets the requirements of the GDC and RGs defined in Section 4 of this report.

2. CURRENT LICENSING CRITERIA

2.1 LICENSING CRITERIA FOR THE REACTOR TRIP SYSTEM (RTS)

GDC 21, entitled "Protection System Reliability and Testability", states in part that:

> The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Regulatory Guide 1.22 entitled "Periodic Testing of the Protection System Actuation Functions" states in Section D.1.a that:

> The periodic tests should duplicate as closely as practicable, the performance that is required of the actuation devices in the event of an accident.

Regulatory Guide 1.22 states in Section D.4 that:

> Where actuated equipment is not tested during reactor operation, it should be shown that:
>
> a. There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant;
>
> b. The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation, and;
>
> c. The actuated equipment can be routinely tested when the reactor is shut down.

Regulatory Guide 1.118, entitled "Periodic Testing of Electric Power and Protection Systems", Section C-12 describes in part that:

> Safety system response time measurements shall be made periodically to verify the overall response time (assumed in the safety analysis of the plant) of all portions of the system from and including the sensor to operation of the actuator.
>
> The response time test shall include as much of each safety system, from sensor input to actuated equipment, as possible in a single test. Where the entire set of equipment from sensor to actuated equipment cannot be tested at once, verification of system response time may be accomplished by measuring the response times of discrete portions of the system and showing that the sum of the response times of all portions is equal to or less than the overall system requirement.

IEEE Std-338-1975 entitled "Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems", states in Section 3 that:

> Overlap testing consists of channel, train, or load group verification by performing individual tests on the various components and subsystems of the channel, train, or load group. The individual component and subsystem tests shall check parts of adjacent subsystems, such that the entire channel, train, or load group will be verified by testing of individual components or subsystems.

2.2 CURRENT LICENSING CRITERIA OF THE ENGINEERED SAFETY FEATURES (ESF)

All criteria listed in Section 2 of this report are applicable to the engineered safety feature systems. In addition, the following criteria are also applicable.

GDC 40, entitled "Testing of Containment Heat Removal System", states the containment heat removal system shall be designed to permit appropriate periodic pressure and functional testing to assure:

a. The structural and leaktight integrity of its components.

b. The operability and performance of the active components of the system.

c. The operability of the system as a whole and under conditions as close to the design as practical the performance of the full operational sequence that brings the system into operation, including operation of applicable portions of the protection systems, the transfer between normal and emergency power sources, and the operation of the associated cooling water system.

Standard Review Plan, Section 7.3, Appendix A, entitled "Use of IEEE Std-279 in the Review of the ESFAS and Instrumentation and Controls of Essential Auxiliary Supporting Systems", states in Section 11.b that:

> Periodic testing should duplicate, as closely as practical, the integrated performance required from the supporting systems, and their essential auxiliary supporting systems. If such a "system level" test can be performed only during shutdown, the testing done during power operation must be reviewed in detail. Check that "overlapping" tests do, in fact, overlap from one test segment to another. For example, closing a circuit breaker with the manual breaker control switch may not be adequate to test the ability of the ESFAS to close the breaker.

3. REVIEW GUIDELINES

3.1 REVIEW GUILDELINES (RTS)

A. Verify that the test conditions come as close as possible to the actual performance required by RTS (GDC-21, RG 1.22-D.1.a).

B. Verify that the system test covers from end-to-end (sensor through actuated device). If partial tests are performed, verify that the overlapping tests indeed overlap from one test segment to another (IEEE Std 338/1975-3).

C. Summarize the RTS surveillance testing interval as defined in the plant's technical specification.

D. Verify that the plant performs a response time testing of sensors and that these response times are within the margin used in the plant's accident analysis (RG 1.118-C.12).

E. Identify the related NRC safety topics in an appendix to the report.

3.2 REVIEW GUIDELINES (ESF/CONTAINMENT SPRAY SYSTEM)

A. Verify that the test condition came as close as possible to the actual performance required by the ESF/containment spray system (GDC-21, GDC-40, SRP 7.3 - Appendix A-11.b).

B. Verify that the system test covers from the system end-to-end (sensor through actuated device). If partial tests are performed, verify that the overlapping tests indeed overlap from one test segment to another (GDC-40, SRP 7.3, Appendix A-11.b).

C. Summarize the ESF/containment spray system surveillance testing interval as defined in the plant's technical specification.

D. Verify that the plant performs a response time testing of sensors and that these response times are within the margin used in the plant's accident analysis (RG 1.118-C12).

E. Identify the related NRC safety topic as an appendix to the report.

4. SYSTEM DESCRIPTIONS

4.1 SYSTEM DESCRIPTION (REACTOR PROTECTION SYSTEM)

The reactor protection system (RPS) receives signals from plant instrumentation indicating the approach of an unsafe operating condition, actuates alarms, prevents control rod motion, and initiates load cutback, and/or opens the reactor trip breakers depending upon the severity of the condition.

The Reactor Protection System is designed to:

1. Prevent, in conjunction with the containment and containment isolation system, the release of radioactive materials in excess of the limitations of 10CFR100 as a consequence of any of the design basis accidents.

2. Prevent fuel damage following any single equipment malfunction or single operator error.

3. Function independently of other plant controls and instrumentation.

4. Function safely following any single component malfunction.

In order to meet its design requirement, the reactor protection system, under various conditions, initiates a reactor scram. The reactor protection system is referred to sometimes as the dual logic reactor protection system and has been utilized on most General Electric reactor plants.

This part of the report is concerned with the reactor trip system (RTS) portion of the RPS and the licensing criteria will be applied only to the RTS here.

The system is made up of two independent logic channels, each having two subchannels of tripping devices. Each subchannel has an input from at least one independent sensor, monitoring each of the critical parameters.

The output of each pair of subchannels is combined in a one-out-of-two logic: That is, an input in either one or both of the independent subchannels will produce a logic channel trip. Both of the other two subchannels are likewise combined in a one-out-of-two logic, independent of the first logic channel. The outputs of the two logic channels are combined in two-of-two arrangement so that they must be in agreement to initiate a scram. An off-limit signal in one of the subchannels in one of the logic channels must be confirmed by any other off-limit signal in one of the subchannels of the remaining logic channel to provide a scram.

Theoretically, this system's reliability is slightly higher than that of a 2-out-of-3 system and slightly lower than that of a 1-out-of-2 system. However, since the differences are slight, they can, in a practical sense, be neglected. The advantage of the dual logic channel reactor protection system is that it can be tested completely during full-power operation. This capability for a thorough testing program, which contributes significantly to increasing reliability, is not possible on a 1-out-of-2 system. Topical Report, APED-5179,* presents a discussion of the reliability of the dual logic channel system.

During normal operation, all vital sensor and trip contacts are closed, and all sensor relays are operated energized. The control rod pilot scram valve solenoids are energized, and instrument air pressure is applied to all scram valves. When a trip point is reached in any of the monitored parameters, a contact opens, de-energizing a relay which controls a contact

*APED-5179, I. M. Jacobs, "Reactor Protection System, A Reliability Analysis" General Electric Co., June, 1966.

in one of the two subchannels. The opening of a subchannel contact de-energizes a scram relay which opens a contact in the power supply to the pilot scram valve solenoids supplied by its logic channel. To this point only one half the events required to produce a reactor scram have occurred. Unless the pilot scram valve solenoids supplied by the other logic channel are de-energized, instrument air pressure will continue to act on the scram valves and operation can continue. Once a single channel trip is initiated, contacts in that scram relay circuit open and keep that circuit de-energized until the initiating parameter has returned within operating limits and the reset switch is actuated manually. Reset of that circuit is possible if all parameters in that circuit are within operating limits. Once a full scram is initiated (i.e., one in channel A and one in channel B) reset is possible for each channel that has returned to operating limits. The electrical logic indicates that if a scram conditon occurs simultaneously in both channels A and B, scram valve sequences are initiated to drive the control rods into the core. Should one of the scram channels then become clear (i.e., within operating limits) and if at this time the reset switch is manually actuated, the scram condition is removed from all four rod groups. Rod motion at this time is a function of the time after scram signal, control rod dynamics, rod positon, prescribed procedures and operator action. If the scram is initiated by the mode switch (i.e., from "RUN" to "START" to "REFUEL" to "SHUTDOWN") the scram cannot be reset until the time delay in the "Shutdown Scram Reset Interlock" has timed out. This time delay is nominally sufficient to allow full insertion of the control rods at which time reset of the scram will have no direct effect on the control rods. A failure of any one reactor trip system input or component will produce a trip in just one subchannel of one logic channel, a situation insufficient to produce a reactor scram. This resistance to spurious scrams contributes to plant safety, since unnecessary cycling of the reactor through its operating modes would increase the probability of error or actual failure.

Since each control rod is scrammed as an independent unit, the failure of any one rod to scram does not affect the ability of the other rods to scram.

The following parameters enter the Reactor Trip System chain:

1. High neutron flux. To prevent fuel damage resulting from bulk power increases, high neutron flux will initiate a scram. The nuclear instrumentation provides high neutron flux trip signals. Four IRM channels and four APRM channels are connected to each of the dual logic channels. Whether the IRM or APRM trip inputs initiate a scram is determined by the mode switch position.

2. High reactor pressure. An increase in reactor vessel pressure threatens the integrity of the reactor vessel (an important barrier to the uncontrolled release of fission products). The high pressure scram terminates the pressure rise before reactor vessel damage occurs. The referenced drawings do not indicate a recirculation pump trip to assist the termination of the pressure rise. The referenced Commonmwealth Edison letter (Ref. 10) indicates an autumn 1980 refueling outage schedule for incorporating a recirculating pump trip modification to the Dresden II plant.

3. High primary containment system pressure. Abnormal pressure could indicate a rupture of, or excessive leakage from, the reactor coolant system into the drywell structure.

4. Low reactor water level. This scram signal assures that the reactor will not be operated without sufficient water above the reactor core.

5. Control rod system scram discharge volume high level. This scram signal assures that the reactor will be operated with sufficient free volume in the scram discharge system, if properly vented, to receive the control rod drives discharge upon scram.

6. Main condenser low vacuum. This scram signal anticipates loss of the main heat sink which would result in a reactor vessel pressure rise as the condenser is isolated to protect it from overpressure. The effects of increased reactor pressure rise are discussed in parameter 2.

7. Main steam line high radiation. The radiation monitors at each of the main steam lines near the primary containment system inboard isolation valves will scram the reactor on a high radiation signal. High steam line radiation is indicative of fuel failures; a scram is necessary to prevent further fuel damage.

8. Loss of a-c power to the protection system. All electronic trips, logic relays, and scram solenoid valves will operate due to loss of power, as the Reactor Protection System M-G sets coast down and trip on loss of a-c power.

9. Partial closure of main steam line isolation valves. This scram signal assures that the reactor will not be operated without its main heat sink, since the resulting reactor vessel pressure increase could cause a fuel-damaging power transient as described in parameter 2. There are four main steam lines with two valves per line. The logic is arranged such that the partial closure of either the inboard or the outboard valve in any three steam lines (i.e., if any combination of three of the steam lines is being closed by a main steam line isolation valve) will initiate a scram. This scram is bypassed when the reactor pressure is below 600 psig.

10. Generator load rejection. A loss of generator load will cause the turbine-generator to speed up. The turbine speed governor will react by closing the turbine admission valves. The reduction of steam flow will cause the reactor vessel pressure to rise, and the initial pressure regulator will open the turbine bypass valves in an attempt to maintain reactor pressure constant. If the load reduction is sudden and of a greater magnitude than bypass valve capacity, the reactor pressure will rise, resulting in the condition described in parameter 2. To prevent fuel damage and the lifting of reactor safety valves, a sudden rejection of generator load will cause a scram. According to the FSAR, this condition is sensed by comparing turbine first stage shell pressure to generator electrical output. A high first stage shell pressure coincident with low generator electrical output will cause a scram. The referenced schematic drawings indicate that this scram is implemented by a pressure switch indicating loss (below 900 psig) of oil pressure at the hydraulic inlet of fast acting control values or by a position switch indicating the fast closure solenoid valves controlling fast closure of the turbine control valves are energized and move. This scram is bypassed when the first stage turbine presssure corresponds to less than 45% rated steam flow.

11. Turbine stop valve closure. In order to protect the turbine, generator, output transformer, and main condenser, the four turbine stop valves are automatically closed upon certain conditions described in the FSAR for the turbine control system. The sudden closure of the turbine stop valves reduces the steam flow from the reactor and causes the reactor vessel pressure to rise. The initial pressure regulator responds to the pressure rise by opening the turbine bypass valves unless opening the bypass valves would overpressurize the condenser. If the required reduction in reactor steam flow is of greater magnitude than can be compensated by bypass valve capacity, or if the bypass valves are not allowed to open, the

reactor vessel pressure rise causes a positive reactivity insertion which would lead to fuel damage. In order to prevent fuel damage resulting from a reactor pressure rise resulting from turbine stop valve closure, the four turbine stop valves have valve stem limit switches which enter the reactor trip system logic channels and trip when the valves start to close. The logic is arranged so that the partial closure of any three of the four stop valves will initiate a reactor scram. This scram is bypassed when the first stage turbine pressure corresponds to less than 45% rated steam flow.

12. Manual. A separate scram push button is provided for each logic channel. To initiate a reactor scram, the pushbuttons for both logic channels must be pushed. The reactor is also manually scrammed when the reactor mode selector switch is moved to the "Shutdown"position, this places all the logic subchannels in scram.

There are three groups of entries to each scram channel in respect to functional testing.

1. On-off sensors that provide a scram trip function.

2. Analog devices coupled with bistable trips that provide a scram function.

3. Devices which only serve a useful function during some restricted mode of operation, such as startup or shutdown, or for which the only practical test is one that can be performed at shutdown.

The functional testing (i.e., injection of a simulated signal into the instrument primary sensor to verify proper instrument responses and trip operation) is carried out on a periodic basis as noted for each subchannel trip parameter. Each group of entries to the scram channels is covered with surveillance intervals, response time testing and bypassing noted where appropriate in Table 5-1.1. (The Plant Technical Specifications for these parameters indicate that the response times of the individual trip functions shall not exceed 0.1 second.)

TABLE 5.1.1*

SCRAM INSTRUMENTATION FUNCTIONAL TESTS
MINIMUM FUNCTIONAL TEST FREQUENCIES FOR SAFETY INSTR. AND CONTROL CIRCUITS

Instrument Channel	Group (3)	Functional Test	Minimum Frequency (4)
Mode Switch in Shutdown	A	Place Mode Switch in Shutdown	Each Refueling Outage
Manual Scram	A	Trip Channel and Alarm	Every 3 Months
IRM			
High Flux	C	Trip Channel and Alarm (5)	Before Each Startup (6)
Inoperative	C	Trip Channel and Alarm	Before Each Startup (6)
APRM			
High Flux	B	Trip Output Relays (5)	Once Each Week
Inoperative	B	Trip Output Relays	Once Each Week
Downscale	B	Trip Output Relays (5)	Once Each Week
High Flux (15% scram)	B	Trip Output Relays	Before Each Startup
High Reactor Pressure	A	Trip Channel and Alarm	(1)
High Drywell Pressure	A	Trip Channel and Alarm	(1)
Reactor Low Water Level (2)	A	Trip Channel and Alarm	(1)
High Water Level in Scram Discharge Tank	A	Trip Channel and Alarm	Every 3 Months
Turbine Condenser Low Vacuum	A	Trip Channel and Alarm	(1)
Main Steamline Isolation Radiation (2)	B	Trip Channel and Alarm (5)	Once Each Week
Main Steamline Isolation Valve Closure	A	Trip Channel and Alarm	(1)
Generator Load Rejection	A	Trip Channel and Alarm	(1)
Turbine Stop Valve Closure	A	Trip Channel and Alarm	(1)
Turbine Control-Loss of Control Oil Pressure	A	Trip Channel and Alarm	(1)

*Extracted from Table 4.1.1 Dresden Station Unit II, Plant Technical Specifications, Change #16, November 1971.

TABLE 5.1.1 (Continued)

NOTES:

1. Once per month until sufficient exposure hours have been accumulated and interpretation of failure rate curves to give an interval of not less than one month nor more than three months. The compilation of instrument failure rate data may include data obtained from other Boiling Water Reactors for which the same design instrument operates in an environment similar to that of Dresden Unit 2.

2. An instrument check shall be performed on low reactor water level once per day and on high steamline radiation once per shift.

3. The three groups are:

   A. The sensors that make up group (A) are specifically selected from among the whole family of industrial on-off sensors that have earned an excellent reputation for reliable operation.

   B. Group (B) devices utilize an analog sensor followed by an amplifier and a bi-stable trip circuit. The sensor and amplifier are active components and a failure is almost always accompanied by an alarm and an indication of the source of trouble. The bi-stable trip circuit which is a part of the Group (B) devices can sustain unsafe failures which are revealed only on test. Therefore, it is necessary to test them periodically.

   C. Group (C) devices are active only during a given portion of the operational cycle. For example, the IRM is active during startup and inactive during full-power operation. The only test that is meaningful is the one performed just prior to shutdown or startup, i.e., the tests that are performed just prior to use of the instrument.

4. Functional tests are not required when the systems are not required to be operable or are tripped. If tests are missed, they shall be performed prior to returning the systems to an operable status.

5. This instrumentation is exempted from the Instrument Functional Test Definition (Section 1.F of Dresden II Plant Technical Specifications). This Instrument Functional Test will consist of injecting a simulated electrical signal into the measurement channels.

6. If reactor start-ups occur more frequently than once per week, the functional test need not be performed; i.e., the maximum functional test frequency shall be once per week.

All control rods are tested for scram times at each refueling outage. Fifty percent of the control rods will be checked every 16 weeks to verify the performance so that every 32 weeks all of the control rods have been tested.

All reactor vessel instrumentation inputs to the reactor protection system operate on a pressure or differential pressure signal. These devices are piped so that they may be individually actuated with a known pressure (or differential pressure) signal during functional testing to initiate a protection system single logic channel trip. Other on-off devices are tested similarly with basic signals.

Analog devices, notably the the flux monitoring channels, are tested in two phases. First, the device must show reasonable agreement with other similar devices and must respond normally to power level changes and control rod movements. Second, a dummy electrical signal may be introduced which uses some or all of the amplifier already tested. This dummy signal is adjusted until the set point limit is exceeded to initiate a single logic subchannel trip. These instrument subchannels are exempt from the Instrument Functional Test definition. The Instrument Functional Test for these subchannels will consist of injecting a simulated electrical signal into the measurement subchannels and is performed on a one-week cycle.

Other than the mode selector switch, the Intermediate Range Monitor (IRM) trip is only active during restricted modes of operation. The IRM is required in the "Refuel" and "Start/Hot Standby" modes only and the only meaningful tests that are performed are those just prior to use. The IRM system provides protection against excessive power levels and short reactor periods in the startup and intermediate power ranges. This instrumentation is exempted from the Instrument Functional Test definition. The Instrument Functional Test used consists of injecting a simulated electrical signal into the measurement subchannels and is performed before each startup or a maximum of once per week.

4.2 SYSTEM DESCRIPTION (ESF/CONTAINMENT SPRAY SYSTEM)

The functional requirements and performance characteristics of the engineered safety features (ESF) serve no function which is necessary for normal station operation. They are included in the plant for the sole purpose of reducing the consequences of postulated accidents. This part of the report is concerned with the containment spray system portion of the ESF and the licensing criteria will be applied only to the containment spray system here.

The major equipment of the entire low pressure coolant injection (LPCI)/ containment cooling subsystem consists of two heat exchangers, four containment cooling service water pumps, four main system pumps, two drywell spray headers, and a suppression chamber spray header. Full capacity flow for the LPCI subsystem (i.e., 14,500 gpm against a system head of 20 psig) is provided by operating three of the four main system pumps. The containment spray subsystem and the low pressure coolant injection (LPCI) subsystem share the same pumps and heat exchangers and the functions performed are determined by valve sequencing. The function of the containment spray is to reduce pressure in the primary containment caused by postulated accidents. During LPCI subsystem operation, water is taken from the suppression pool and is pumped into the core region of the reactor vessel via one of the two recirculation loops. (There is also a connection on the condensate storage tank to make condensate available for use in functional testing of the system.)

The initiating logic to start the LPCI pumps is a form of the one-of-two-twice logic basically requiring the LPCI pump and valve selector switches to be in "AUTO" and either low-low reactor water level and reactor low pressure or 2 or greater psi high drywell pressure to be present. Since the LPCI flow passes through heat exchangers, heat may be rejected from the containment by starting the containment cooling service water pumps to cool the heat exchangers when sufficient electrical power is available. The valving to containment spray from the LPCI pumps is accomplished at operator's discretion. Interlocks (low water level inside shroud) are provided to

prevent LPCI flow from being diverted to the containment spray system unless the core is flooded. A key lock switch permits these interlocks to be overridden if containment pressure is high (greater than 1 psig).

The LPCI/containment cooling system is designed so that each component of the system can be tested and inspected periodically to demonstrate availability of the system. The Plant Technical Specifications indicate that a logic system functional test and simulated automatic actuation test of the LPCI portion of the system is completed at each refueling outage. Testing of the operation of the valves required for the various modes of operation of the system will be performed at this time. A design flow functional test of the LPCI and containment cooling water pumps will be performed once each quarter during normal plant operation by taking suction from the suppression pool and discharging through the test lines back to the suppression pool. The discharge valves to the reactor recirculation loops remain closed during this test and reactor operation is undisturbed. An operational test of these discharge valves will be performed by shutting the downstream valve after it has been satisfactorily tested and then operating the discharge valve. The discharge valves to the containment spray headers are checked in a similar manner by operating the upstream and downstream valves individually. All these valves can be actuated from the control room using remote manual switches. Control system design provides automatic return from test to operating mode if LPCI initiation is required during testing. The surveillance interval for the instrumentation for the ECCS is noted in Table 5-2.1.

TABLE 5.2.1*

MINIMUM TEST AND CALIBRATION FREQUENCY FOR CONTAINMENT COOLING SYSTEMS INSTRUMENTATION

Instrument Channel	Instrument Functional Test (2)	Calibration (2)	Instrument Check (2)
ECCS INSTRUMENTATION			
1. Reactor Low-Low Water Level	(1)	Once/3 Months	Once/Day
2. Drywell High Pressure	(1)	Once/3 Months	None
3. Reactor Low Pressure	(1)	Once/3 Months	None
4. Containment Spray Interloc			
a. 2/3 Core Height	(1)	Once/3 Months	None
b. Containment High Pressure	(1)	Once/3 Months	None
5. Low Pressure Core Cooling Pump Discharge	(1)	Once/3 Months	None
6. Undervoltage Emergency Bus	Refueling Outage	Refueling Outage	None
7. Sustained High Reactor Pressure	(1)	Once 3/Months	None

NOTES:

1. Once per month until sufficient exposure hours have been accumulated and interpretation of failure rate curves give an interval of not less than one month nor more than three months. The compilation of instrument failure rate data may include data obtained from other Boiling Water Reactors for which the same design instrument operates in an environment similar to that of Dresden Unit II.

2. Functional test calibrations and instrument checks are not required when these instruments are not required to be operable or are tripped. Functional tests shall be performed before each startup with a required frequency not to exceed once per week. Calibrations shall be performed during each startup or during controlled shutdowns with a required frequency not to exceed once per week. Instrument checks shall be performed at least once per week. Instrument checks shall be performed at least once per day during those periods when the instruments are required to be operable.

*Extracted from Table 4.2.1 Dresden Station Unit II, Plant Technical Specification, Change #16, November 1971.

5. EVALUATIONS AND CONCLUSIONS

5.1 EVALUATION AND CONCLUSIONS (RTS)

The reactor trip system electrically is the dual logic reactor protection system and as such can be tested completely during full-power operation. The Plant Technical Specifications indicate a requirement for test of each of the scram parameters on a frequency as shown in Table 5-1.1. The variables for scramming are introduced as noted in the table. The individual control rods are tested for scram operability during the operating cycle and for scram times during the refueling outage. The Plant Technical Specification for the parameters that enter the scram chain indicates that the response time of the individual trip functions should not exceed 0.1 second. Neither a procedure for measurement of, nor frequency of, observation of the response time of the trip functions was located. The response (and travel) time measurement of the scram of the control rods is performed at least at each refueling outage and the required performance is within the time used for the analytical treatment of transients.

The test conditions for the various parameters are inserted in the sensors so that scram performance can be verified. The sum of the tests indicates sufficient overlap through the activated scram of the control rods to comply with the end-to-end criterion. The reactor trip system surveillance testing interval is extracted from the Plant Technical Specification and summarized in Table 5.1.1. Not available were references to the response time measurement of the individual trip functions.

Based on the information available, it is concluded that the reactor trip system meets the current licensing criteria listed in Section 2 of this report except for instrument response time testing.

5.2 EVALUATION AND CONCLUSIONS (ESF/CONTAINMENT SPRAY SYSTEM)

The testing of all portions of the ESF/Containment Spray System is called for in the Plant Technical Specification. A logic system functional test and simulated automatic actuation test of the LPCI portion of the system is completed at each refueling outage. Also testing of the operation of the various valve sequences is performed at this time. With the one-of-two-twice logic, the instruments and parameters to automatically initiate the LPCI can be tested and calibrated and the Technical Specifications (extracts appropriate to this are in Table 5.2.1) indicate periods for this to be done. The LPCI and containment cooling water pumps are required to have a quarterly flow check. The containment cooling service water pumps supply the water from the crib house for the containment cooling heat exchangers which could then be used for heat exchange performance verification when the service water pumps are tested. The operations of the valves to direct flow for LPCI or containment spray are tested by appropriate valve sequencing and overlap testing.

Response time testing requirements for the sensors for the containment cooling were not found in the references. The switchover from LPCI is manually initiated at operator's discretion, sometime after the water level in the reactor shroud is raised above the minimum two-thirds core height interlock to assure the core is flooded. The Technical Specifications indicate the interlock is functionally tested on an interval not less than monthly or greater than three months and is calibrated on a three month cycle. It does not appear that response time testing for the instrumentation for the containment spray system would be of value based on the manual valve sequencing required to initiate system's operation.

From the information available, it is concluded that the containment spray subsystem of the ESF meets the current licensing criteria listed in Section 2 of this report.

6. SUMMARY

The Dresden Station Unit II nuclear power plant complies to current licensing criteria for RTS testing as defined in Section 2 of this report except for instrument response time testing.

The plant also complies to current licensing criteria for ESF/Containment Spray System testing as defined in Section 2 of this report.

REFERENCES

1. Code of Federal Regulations, Title 10, Part 50 (10CFR50), 1979, Appendix A, (General Design Criteria).

2. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.22, "Periodic Testing of the Protection System Activation Functions".

3. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems".

4. IEEE Std-338-1975, "Periodic Testing of Nuclear Power Generating Station Class 1E Power and Protection Systems".

5. U. S. Nuclear Regulatory Commission, Standard Review Plan, Section 7.3, Appendix A, "Use of IEEE Std-279 in the Review of the ESFAS and Instrumentation and Controls of Essential Auxiliary Supporting Systems".

6. Commonwealth Edison Company, Dresden Station Unit II Final Safety Analysis Report.

7. Commonwealth Edison Company, Dresden Station Unit II Technical Specifications.

8. Dresden II Mechanical Drawings: M-22, February 1978; M-26-2, June 1977; M-29, September 1977; M-34, June 1977; M-35-1, February 1978.

9. Dresden II Electrical Drawings: 12E2421, March 1971; 12E2422, August 1977; 12E2423, February 1977; 12E2435, February 1977; 12E2436, September 1976; 12E2437, September 1976; 12E2438, September 1976; 12E2438A, January 1977; 12E2439, December 1976; 12E2440, December 1976; 12E2441, December 1977; 12E2441A, December 1977; 12E2464, September 1976; 12E2465, October 1976; 12E2466, September 1976; 12E2467, January 1977; 12E2468, September 1976.

10. Commonweath Edison letter (Cordell Reed) to U.S. Nuclear Regulatory Commission (Harold Denton), March 29, 1979.

APPENDIX A

1. Topic VI-3, "Containment Pressure and Heat Removal Capability".

2. Topic VI-4, "Containment Isolation System".

3. Topic VI-7, "Emergency Core Cooling System".

4. Topic VI-7.C, "ECCS Single Failure Criterion and Requirements for Locking Out Power to Valves Including Independence of Interlocks on ECCS Valves".

5. Topic VI-9, "Main Steam Isolation".

6. Topic VI-10, "Selected ESF Aspects".

Technical Information Department · Lawrence Livermore Laboratory
University of California · Livermore, California 94550

~~Lawrence~~
SCHOLL - XTRA

UCID-18698, Vol. III

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VII-2 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION AND CONTROL PORTIONS OF THE ESF SYSTEM CONTROL LOGIC AND DESIGN FOR THE DRESDEN STATION, UNIT II NUCLEAR POWER PLANT

Gerald St. Leger-Barter

November 1980

Lawrence Livermore Laboratory

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

8102170038

DISCLAIMER

Available from: National Technical Information Service - U.S. Department of Commerce
5285 Port Royal Road - Springfield, VA 22161 - $5.00 per copy - (Microfiche $3.50)

ABSTRACT

This report documents the technical evaluation and review of NRC Safety Topic VII-2, associated with the electrical, instrumentation, and control portions of the ESF system control logic and design for the Dresden Station Unit II nuclear power plant, using current licensing criteria.

FOREWORD

This report is supplied as part of the Systematic Evaluation Program being conducted for the U.S. Nuclear Regulatory Commission by Lawrence Livermore National Laboratory. The work was performed under U.S. Department of Energy contract number DE-AC08-76NV01183.

TABLE OF CONTENTS

SYSTEMATIC EVALUATION PROGRAM REVIEW OF NRC SAFETY TOPIC VII-2 ASSOCIATED WITH THE ELECTRICAL, INSTRUMENTATION, AND CONTROL PORTIONS OF THE ESF SYSTEM CONTROL LOGIC AND DESIGN FOR THE DRESDEN STATION UNIT II NUCLEAR POWER PLANT

GERALD ST. LEGER-BARTER

1. INTRODUCTION

The Engineered Safety Features Actuation Systems (ESFAS) of both PWRs and BWRs may have design features that raise questions about the electrical independence of redundant channels and isolation between ESF channels or trains.

Non-safety systems generally receive control signals from the ESF sensor current loops. The non-safety circuits are required to have isolation devices to insure electrical independence from the ESF channels. The safety objective is to verify that operating reactors have ESF designs which provide effective and qualified isolation between ESF channels, and between ESFs and non-safety systems.

This report reviews the plant's ESF EI&C design features to insure that the non-safety systems electrically connected to the ESFs are properly isolated from the ESFs. This report also reviews the plant's ESFs to insure that there is proper isolation between redundant ESF channels or trains, and that the isolation devices or techniques meet the current licensing criteria detailed in Section 2 of this report. The qualification of safety-related equipment is not within the scope of this report and is discussed in NRC Safety Topic III-12 and NUREG-0458.

2. CURRENT LICENSING CRITERIA

GDC 22, entitled "Protection System Independence," states that:

> The protection system 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 that they shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

GDC 24, entitled "Separation of Protection and Control Systems," states that:

> 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 system leave intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

IEEE Std-279-1971, entitled "Criteria for Protection Systems for Nuclear Power Generating Stations," states in Section 4.7.2 that:

> The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall

be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design bases.

Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible a-c or d-c potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the protection system.

3. REVIEW GUIDELINES

The following NRC guidelines were used for this review:

Verify that the signals used for ESF functions are isolated from redundant ESF trains or channels. Review the schematic diagrams to assure that the wiring satisfies the functional logic diagrams in the FSAR or its equivalent (GDC 22).

Verify that qualified electrical isolation devices are utilized when redundant ESF trains or channels share safety signals. Identify and describe the type of isolation device employed (GDC 22).

Verify that the safety signals used for ESF functions are isolated from control or non-safety systems. Identify and describe the type of isolation device employed (GDC 24, IEEE Std-279-1971, Section 4.7.2).

Verify that the logic does not contain sneak paths that could cause false operation or prevent required action as the result of operation of plant control.

Identify the related NRC Safety Topics in an appendix to the report.

4. SYSTEM DESCRIPTION

Means are needed to provide continuity of core cooling during those postulated accident conditions where it is assumed that mechanical failures occur in the primary system and coolant is partially or completely lost from the reactor vessel. Under these circumstances core cooling is accomplished by means of the emergency core cooling system (ECCS). The ECCS consists of two independent core spray subsystems, the low pressure coolant injection (LPCI) subsystem, the high pressure coolant injection (HPCI) subsystem and the automatic pressure relief subsystem.

4.1 CORE SPRAY SUBSYSTEM

The core spray subsystem consists of two independent spray systems each with its own pump, valves, and associated piping and instrumentation. The water source is common to both systems and can be from the suppression pool in the torus or, by appropriate valving, from the contaminated demineralized water storage tank.

Initiation of the core spray subsystem occurs on signals indicating reactor low-low water level and reactor low pressure or high drywell pressure. Low-low water level and high drywell pressure are each detected by four independent level and pressure switches connected in a form of one-of-two-twice logic array. Water injection can start when the admission valve is opened and when the reactor vessel pressure drops below pump discharge pressure (350 psig). Rated flow is sprayed over the top of the core at 90 psig in the reactor vessel. Opening of the admission valves is accomplished only after the reactor pressure decays to approximately the design discharge pressure of the pump, at which time the permissive signal to open the valves is initiated by two pressure switches connected in a one-out-of-two logic array.

4.2 LOW PRESSURE COOLANT INJECTION SUBSYSTEM (LPCI)

The LPCI subsystem consists of two main subdivisions: one the LPCI system, and the other the containment cooling system. The major equipment of the entire subsystem consists of two heat exchangers, four containment cooling service water pumps, four main system pumps, two drywell spray headers, a suppression chamber spray header, and associated valving, piping and instrumentation.

The system pumps are activated on either a signal of reactor low-low water level and reactor low pressure or a signal of high drywell pressure similar to that received by the core spray pumps. The initiation signal also trips the recirculation pumps and supplies a start signal to the diesel generator which will provide power for the pump prime mover if normal auxiliary power has failed. The valves in the high pressure part of the system are activated on a preset reactor low pressure signal similar to that of the valving on the core spray subsystem, thereby establishing a flow path.

4.3 HIGH PRESSURE COOLANT INJECTION SUBSYSTEM (HPCI)

The HPCI subsystem consists of a single steam turbine driving a multi-stage high pressure pump and a gear driven single stage booster pump, valves, high pressure piping, water sources, and instrumentation. The turbine is driven with steam from the reactor vessel. Exhaust steam from the turbine is discharged to the suppression pool. Suction for the HPCI pump is taken from the suppression pool.

Initiation of operation of the system is on a signal of either reactor low water level or high drywell pressure. These level and pressure switches are in a one-of-two-twice logic array similar to the reactor protection system. The system will automatically maintain reactor water level between low level and high level if required flow is within the capacity of the pump and the reactor is not depressurized below 165 psia.

4.4 AUTOMATIC PRESSURE RELIEF SUBSYSTEM (ADS)

The automatic pressure relief subsystem is provided for backup of the HPCI subsystem and performs the functions of vessel depressurization for all small breaks. When the automatic pressure relief subsystem is actuated, the critical flow of steam through the relief valves results in a maximum energy removal rate with a corresponding minimum mass loss. Since the the automatic pressure relief subsystem does not provide coolant makeup to the reactor, its function is only in conjunction with the LPCI or core spray subsystems as a backup to the HPCI.

Automatic actuation requires coincident indication of reactor water low-low level and drywell high pressure which is maintained for a period of 2 minutes. It also requires LPCI pressure switches to be made up and/or core spray pressure switches to be made up (i.e., their pump outputs to be above preset levels). There are two actuation chains and each circuit requires the same parameters for actuation.

5. EVAULATION AND CONCLUSIONS

The primary sensors for initiation of the ECCS functions were determined to be pressure and level switches. These switches and their associated ESF systems are tabulated in Table 5.1. It is noted that some of the switch functions are shared but that the isolation between functions is by the use of separate contacts from the relay operated by the pressure/level switch. The reference drawings also note the two switch functions are incorporated in the pressure switches operated by a common actuator. The parameters that initiate the primary function are listed but not all parameters which control the valve sequencing are shown as the isolation carried through for them is similar to that for initiation.

The systems were reviewed in accordance with the review guidelines for isolation and any apparent sneak paths for false operations or inhibition of operation. The isolation of each system from other functions is accomplished by use of separate sensor switches and/or separate contacts.

Based on the review of plant drawings it is concluded that the ESF systems are adequately isolated from control or non-safety systems and each other in accordance with the requirements of section 2 of this report.

TABLE 5.1

ECCS ACTUATION SYSTEM PRIMARY SENSOR SWITCHES

FUNCTION	RELAY	RELAY	ECCS LOGIC
Drywell High Pressure P.S.			
2202-5 / 1632A	902-32 / 1530-108		Core Spray
		902-32 / 1430-103A	LPCI
2202-5 / 1632A (B) 2NO,2COM	902-32 / 2330-142		HPCI
2202-6 / 1632B	902-33 / 1530-208		Core Spray
		902-33 / 1430-103B	LPCI
2202-6 / 1632B 2NO, 2COM			HPCI
2202-5 / 1632C	902-32 / 1530-109		Core Spray
		902-32 / 1430-104A	LPCI
2202-5 / 1632C (B) 2NO, 2COM	902-32 / 2330-143		HPCI
2202-6 / 1632D	902-33 / 1530-209		Core Spray
		902-33 / 1430-104B	LPCI
2202-6 / 1632D 2NO, 2COM			HPCI
2202-5 / 1628A	902-32 / 287-101A		ADS
2202-5 / 1628B	902-32 / 287-102A		ADS
2202-6 / 1629A	902-33 / 287-108BB	902-33 / 287-101B	ADS
2202-6 / 1629B	902-33 / 287-109BB	902-33 / 287-102B	ADS

FUNCTION	RELAY	RELAY	ECCS LOGIC
Drywell 1 PSI High Pressure P.S.			
2202-5 / 1501-62A →	902-32 / 1530-134 →		LPCI
2202-5 / 1501-62B →	902-33 / 1530-234 →		LPCI
2202-5 / 1501-62C →	902-32 / 1530-199 →		LPCI
2202-5 / 1501-62D →	902-33 / 1530-299 →		LPCI

FUNCTION		RELAY	RELAY	ECCS LOGIC
REACTOR LOW WATER LEVEL LIS				
2202-5 / 263-72A	7,8	902-32 / 1430-105A		ADS
				Core Spray
2202-5 / 263-72A	5,6	902-32 / 1530-103		HPCI
				LPCI
2202-6 / 263-72B	7,8	902-33 / 1430-105B		ADS
				Core Spray
				HPCI
2202-6 / 263-72B	5,6	902-33 / 1530-203		LPCI
2202-5 / 263-72C	7,8	902-32 / 1430-106A		ADS
				Core Spray
2202-5 / 263-72C	5,6	902-32 / 1530-104		HPCI
				LPCI
2202-6 / 263-72D	7,8	902-33 / 1430-106B		ADS
				Core Spray
				HPCI
2202-6 / 263-72D	5,6	902-33 / 1530-204		LPCI

FUNCTION	RELAY	RELAY	ECCS LOGIC
Reactor Low Level Inside Shroud LITS			
2202-7 / 263-73A	902-32 / 1530-110		LPCI
2202-7 / 263-73B	902-33 / 1530-211		LPCI
Reactor Low Pressure P.S.			
2202-5 / 263-52A	902-32 / 1530-150		LPCI
2202-5 / 263-52A 2NC,2COM	902-32 / 1430-107A		Core Spray
	902-32 / 1430-129A		Core Spray
2202-6 / 263-52B	902-33 / 1530-250		LPCI
2202-6 / 263-52B 2NC, 2COM	902-33 / 1430-107B		Core Spray
	902-33 / 1430-129B		Core Spray

FUNCTION	RELAY	RELAY	ECCS LOGIC
CORE SPRAY PUMP DISCHARGE P.S.			
2202-19A / 1430-1466A	→ 902-32 / 1430-125A	→	ADS
2202-19B / 1430-1466B	→ 902-33 / 1430-125B	→	ADS
2202-19A / 1430-1466C	→ 902-32 / 1430-128A	→	ADS
2202-19B / 1430-1466D	→ 902-33 / 1430-128B	→	ADS

FUNCTION	RELAY	RELAY	ECCS LOGIC
LPCI PUMP DISCHARGE P.S.			
2202-19A / 1554 A or 2202-19A / 1554B	→ 902-32 / 1530-198	→	ADS
2202-19B / 1554C or 2202-19B / 1554D	→ 902-33 / 1530-298	→	ADS
2202-19A / 1554E or 2202-19A / 1554F	→ 902-32 / 1530-168	→	ADS
2202-19B / 1554H or 2202-19B / 1554J	→ 902-33 / 1530-268	→	ADS

6. SUMMARY

Based on the review of Dresden Station Unit II Plant drawings it is concluded that the isolation of the ESF systems satisfies the current licensing requirements in section 2 of this report.

REFERENCE

1. Code of Federal Regulations, Title 10, Part 50 (10 CFR 50), 1979, Appendix A, (General Design Criteria).

2. Commonwealth Edison Company, Dresden Station Unit II Final Safety Analysis Report.

3. Dresden II Mechanical Drawings: M-25, January 1978; M-26-1, August 1977; M-27, April 1977.

4. Dresden II Electrical Drawings: 12E2429, September 1976; 12E2430, February 1977; 12E2435, February 1977; 12E2436, September 1976; 12E2437, September 1976; 12E2438, September 1976; 12E2461, September 1976; 12E2462, September 1976; 12E2527, September 1976; 12E2528, December 1976; 12E2529, December 1976; 12E2530, December 1976.

APPENDIX A

1.	Topic VI - 7.A.3	"Testability and Operability of the ECCS Actuation System".
2.	Topic VI - 10.A	"Testing of RTS and ESF including Response Time Testing".
3.	Topic VI - 10.B	"Shared ESFs On-Site Emergency Power and Service Systems for Multiple Unit Facilities".
4.	Topic VII - 1.A	"Isolation of the RPS from Non-Safety Systems".
5.	Topic VII - 4	"Effects of Failure in Non-Safety Related Systems on Selected ESF's".

Technical Information Department · Lawrence Livermore Laboratory
University of California · Livermore, California 94550