NUREG/CR-xxxx
BNL-NUREG-yyyyy-20zz

DEVELOPMENT OF A STATISTICAL TESTING APPROACH FOR QUANTIFYING SOFTWARE RELIABILITY AND ITS APPLICATION TO AN EXAMPLE SYSTEM

Draft

Tsong-Lun Chu[1], Athi Varuttamaseni[1], Joo-Seok Baek[1], Meng Yue[1], Tim Kaser[2], George Marts[2], Paul Murray[2], Bentley Harwood[2], and Ming Li[3]

[1]Brookhaven National Laboratory
[2]Idaho National Laboratory
[3]U.S. Nuclear Regulatory Commission

Software Failure Quantification

JCN V-6196

October 15, 2014

Prepared for

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Division of Risk Analysis

The Disclaimer is provided by NRC.

ABSTRACT

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) encourages the use of probabilistic risk assessment (PRA) technology in all regulatory matters, to the extent supported by the state-of-the-art in PRA methods and data. Although much has been accomplished in the area of risk-informed regulation, the process of risk-informed analysis for digital systems has not been fully developed. The NRC established a plan for digital system research to identify and develop methods, analytical tools, and regulatory guidance for (1) including models of digital systems in nuclear power plant (NPP) PRAs and (2) incorporating digital systems in the NRC's risk-informed licensing and oversight activities.

Past NRC research explored possibilities of addressing digital instrumentation and control (I&C) system failures in present NPP PRA framework. Reliability modeling for digital I&C systems, including hardware reliability modeling, software reliability modeling, and dependency modeling among hardware, software components and even operator interactions, were identified as necessities to integrate digital I&C failures into PRAs. This statistical testing research jointly conducted by Brookhaven National Laboratory (BNL) and Idaho National Laboratory (INL) attempts to advance the state of the practice of software reliability quantification.

It is widely recognized that software fails due to defects (including errors made in user requirements, defects introduced during development process and deployment, and erroneous uses of software) residing in the software and the use of the software triggers these defects. Software reliability is thus a function of the manner software is used. Research presented in this report utilizes the statistical testing method (STM) to capture such manners and test the software accordingly. Test results (number of failures) thus represent the operational software failures. Since digital I&C system (including the software) will be modeled in the nuclear power plant (NPP) PRA sequences, manners in which the digital system is used would be determined by each PRA sequence. For instance, if one postulated digital reactor protection system (RPS) appears in both primary LOCA and SGTR sequences, inputs to this RPS and its software (such as reactor temperature, pressure, steam generator level, steam pressure, etc.) would follow different patterns, and different part of the RPS software would be challenged, and consequently the probability of RPS failure might be different for each sequence. The STM method developed in this research produces test cases specific to each sequence and tests the RPS system against these test cases to generate the sequence-specific software failure probability.

The STM method consists of the following steps, which assumes a PRA and an appropriate thermal-hydraulic model have been developed:

1. Select the system under test (SUT);
2. Identify SUT related PRA sequences (represented by cutsets);

3. Determine the thermal-hydraulic simulation boundary conditions corresponding to the selected cutsets;
4. Run the thermal-hydraulic model and output reactor and plant physical conditions. Such outputs are test cases to the SUT;
5. Execute test cases and collect test results;
6. Analyze test results to quantify the software failure probability.

In this study BNL selected a Loop Operating Control System (LOCS) for the Advanced Test Reactor (ATR) at INL as the SUT. INL provided BNL the ATR PRA and RELAP5 models relevant to the LOCS system. BNL revised these models to make them STM friendly, identified LOCS relevant cutsets, configured the RELAP5 model according to plant conditions defined by cutsets, executed the RELAP5 model and produced test cases. These test cases delivered to INL to conduct the software testing.

INL developed a LOCS test bed that automated the software testing. This test bed automatically fed the BNL test cases into the LOCS and collected test results. The test results were statistically analyzed to generate the LOCS failure probability.

TABLE OF CONTENTS

ABSTRACT iii
EXECUTIVE SUMMARY iv
ACRONYMS AND ABBREVIATIONS x
ACKNOWLEDGEMENTS xii
1. INTRODUCTION 1-1
1.1 Background 1-1
1.2 Objective and Scope 1-3
2. GENERAL APPROACH 2-1
2.1 Use of PRA Defined Contexts 2-1
2.2 Characterization of Operational Profiles 2-1
2.3 Sampling from the Operational Profiles 2-3
2.4 Use of a Thermal-Hydraulic Simulation 2-3
2.5 Test Configuration 2-4
2.6 Determination of the Number of Tests Needed 2-5
2.7 Performing Tests and Analysis of Results 2-5
2.8 Assumptions and Limitations 2-6
2.9 An Issue on Quantifying Software Failure Probability Using Statistical Testing 2-7
3. SYSTEM DESCRIPTION 3-1
3.1 ATR Facility Description 3-1
3.2 Overview of the Loop Operating Control System 3-3
3.3 LOCS Control Functions 3-34
3.4 LOCS Protective Functions 3-5
4. PRA MODEL DESCRIPTION 4-1
4.1 Overview 4-1
4.2 LOCS's Role in ATR PRA 4-1
4.3 PRA Analysis of Reactivity Insertion Accidents of Loop 2A 4-2
4.3.1 Description of Reactivity Insertion Event Tree 4-3
4.3.2 Description of the Reactivity Accident Fault Tree 4-4
4.3.3 Modifications to the ATR PRA 4-5
4.3.4 Quantitative PRA Results 4-89
4.4 Risk-Informed Considerations 4-112
4.5 Assumptions and Limitations of the Application 4-12
5. . USING THE RELAP5 MODEL TO GENERATE TEST CASES 5-1
5.1 RELAP5 Model of Experimental Loop 2A 5-1
5.2 Modeling of Reactivity Insertion Cutsets with RELAP5 5-5
5.2.1 Issues Associated with Modeling of PRA-Defined Reactivity Insertions 5-5
5.2.2 Categories of Failure Effects and Their Associated Probabilistic Failure Models ..5-67
5.3 Simplifications, Assumptions, and Limitations of the RELAP5 Simulation 5-13
6. TEST CASE GENERATION 6-1
6.1 Grouping of Cutsets for Generating Test Cases 6-1
6.1.1 Grouping of Cutset by Failure Impacts 6-1
6.1.2 Automation of Cutset Group Assignment 6-4

6.1.3 Use of Probabilistic Failure Models of Failure Effect Groups in Generating Test Cases 6-6
6.2 Sampling and Simulation of Test Cases 6-7
6.2.1 Sampling of Cutsets 6-7
6.2.2 Generation of Input Decks 6-7
7. TEST CONFIGURATION, EXECUTION, AND EVALUATION 7-1
7.1 Introduction 7-1
7.2 Establishment of a Test Configuration 7-2
7.3 Execution of the Test Cases 7-7
7.4 Assumptions and Limitations 7-8
8. EVALUATION OF TEST RESULTS 8-1
8.1 Determination of a Success Criterion 8-1
8.1.1 Estimating a Predicted Trip Time Window 8-2
8.1.2 Determination of Actual Trip Time 8-3
8.2 ATR LOCS Testing Results 8-3
8.3 Reproducibility of the Test Cases 8-8
9. ESTIMATION OF SOFTWARE PROBABILITY OF FAILURE ON DEMAND 9-1
10. CONCLUSIONS AND INSIGHTS 10-1
11. REFERENCES 11-1
Appendix A A-1

LIST OF TABLES

Table 4-1 High level structure of the fault tree for loop 2A reactivity insertion (EXT-2AC-AQU). 4-5
Table 4-2 Assignment of cutset categories to branches 1 and 3 of the event tree. 4-67
Table 4-3 Summary of PRA calculations..... 4-9
Table 5-1 Bounds for probabilistic modeling of cutset groups. 5-10
Table 5-2 Justification of bounds for probabilistic modeling of cutset groups. 5-12
Table 6-1 Failure effect groups and their modeling in RELAP5. 6-3
Table 6-2 Sample cutset showing failures leading to reactivity insertion and their group assignment. . 6-4
Table 6-3 Portion of the sample file. 6-8
Table 6-4 Accuracy of sensors modeled in RELAP5 Loop 2A Model. 6-10
Table 7-1 ATR Loop 2A signals simulated with the RELAP5 model and used as input to the CSFT-SS. 7-6
Table 7-2 Output record data collected in the CSFT-SS scenario output files. 7-7
Table 8-1 Trip setpoints and hysteresis window for the trip-capable loop protective functions. 8-2
Table 8-2 Delayed Trips. 8-4
Table 8-3 Early Trips. 8-4
Table 8-4 Summary of cases with anomalies. 8-6
Table 8-5 Distribution of the actual trip record for the cases that were rerun. 8-9

LIST OF FIGURES

Figure 1-1 NRC Research Activities on Digital System Reliability 1-2
Figure 2-1 Overall Statistical Testing Approach for Quantifying Software Reliability 2-2
Figure 3-1 Location of the in-pile tubes in the ATR and cut-away view of the core 3-2
Figure 3-2 ATR's flux trap and irradiation test positions 3-2
Figure 3-3 Cross section of the in-core portion of a typical pressurized water loop 3-3
Figure 3-4 Simplified flow diagram of loop 2A 3-6
Figure 3-5 IPT high inlet temperature protection channel 3-8
Figure 3-6 Typical processing logic of the loop protective channel 3-9
Figure 4-1 The RLH event tree in the original PRA model 4-3
Figure 4-2 Fault tree model of failure events in loop 2A leading to reactivity insertion 4-5
Figure 4-3 Branching of the event tree by the reactivity insertion events characteristics 4-7
Figure 5-1 RELAP5 nodalization of the original model for the out-of-pile loop piping. 5-2
Figure 6-1 Algorithm for the script used to classify cutsets 6-5
Figure 6-2 Portion of the template file 6-9
Figure 6-3 Algorithm for the script used to generate RELAP5 input file 6-9
Figure 7-1 Work flow associated with performing the tests 7-1
Figure 7-2 CSFT-SS testing environment 7-3
Figure 7-3 A view of the CSFT-SS main window 7-5
Figure 8-1 Relationship between LOCS cycle and host computer cycle 8-2
Figure 8-2 Distribution of the difference between the actual trip record and the predicted trip window 8-4
Figure 8-3 LO_FO_HO_TV_2994 is an example of a delayed trip case. 8-7
Figure 8-4 HI_217 is an example of an early trip case. 8-8

ACRONYMS AND ABBREVIATIONS

ABWR	advanced boiling water reactor
ACRS	Advisory Committee on Reactor Safeguards
AIM	analogy input module
AOM	analog output module
ATR	Advanced Test Reactor
BBN	Bayesian belief network
BNL	Brookhaven National Laboratory
CCF	common cause failure
CDF	core damage frequency
CLLC	contact-to-logic level convertor
COMPSIS	Computer Systems Important to Safety
CSFT	Control Software Failure and Test Simulator
CV	control variable
DCS	distributed control system
DOM	digital output module
DPU	distributed processing unit
EPRI	Electric Power Research Institute
ESFAS	engineered safety features actuation system
FCV	flow control valve
FPGA	field programmable gate array
HDW	high pressure demineralized water
HTC	heat transfer coefficient
I&C	instrumentation and control
I/O	input/output
IE	initiating event
IEC	International Electrotechnical Commission
INL	Idaho National Laboratory
IPT	in-pile tube
LERF	large early-release frequency
LLOCA	large loss of coolant accident
LOCA	loss of coolant accident
LOCS	loop operating control system
MOU	memorandum of understanding
NASA	National Aeronautics and Space Administration
NEA	Nuclear Energy Agency
NI	National Instruments
NPP	nuclear power plant

NRC	Nuclear Regulatory Commission
NSUF	National Scientific User Facility
OECD	Organisation for Economic Cooperation and Development
pdf	probability density function
PID	proportional, integral, and derivative
PPS	plant protection system
PRA	probabilistic risk assessment
PWR	pressurized water reactor
QSRM	quantitative software reliability method
RCCS	rod clutch control system
RG	regulatory guide
RPS	reactor protection system
RPU	remote processing unit
RTD	resistance thermal detector
SBLOCA	small break loss of coolant accident
SCR	silicon-controlled rectifier
STM	statistical testing method
TCV	temperature control valve
TH	thermal-hydraulic
V&V	verification and validation
WGRisk	Working Group on Risk Assessment

ACKNOWLEDGEMENTS

11. INTRODUCTION

1.1 Background

The U.S. Nuclear Regulatory Commission's (NRC's) current licensing process for digital systems relies on deterministic engineering criteria. In its 1995 probabilistic risk assessment (PRA) policy statement [NRC 1995a], the Commission encouraged the use of PRA technology in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data. Although much has been accomplished in the area of risk-informed regulation, the process of risk-informed analysis for digital systems is not fully developed. Since digital instrumentation and control (I&C) systems are expected to play an increasingly important safety role at nuclear power plants (NPPs), the NRC established a plan for digital system research [NRC 2010a] defining a coherent set of projects to support regulatory needs. Some of the projects included in this research plan address risk assessment methods and data for digital systems. The objective of the NRC's digital system risk research is to identify and develop methods, analytical tools, and regulatory guidance for (1) including models of digital systems in NPP PRAs, and (2) incorporating digital systems in the NRC's risk-informed licensing and oversight activities.

Figure 1-1 graphically depicts the interrelationship between the various activities associated with the NRC's digital system risk research. The work on developing a digital system reliability modeling approach is being coordinated with several other related research efforts being carried out by the NRC. As indicated in Figure 1-1, these other areas include failure mode identification and analysis [Chu 2008 and 2009a], operating experience analysis [Korsah 2010], and digital system inventory and classification [Wood 2012]. In addition, this research has benefited from interactions with the Electric Power Research Institute (EPRI) and the National Aeronautics and Space Administration (NASA) under separate memoranda of understanding (MOUs), and with the Organisation for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA), more specifically the Working Group on Risk Assessment (WGRisk) and the OECD/NEA activity on Computer Systems Important to Safety (COMPSIS).

An important insight from the initial digital system reliability research is the need to establish a commonly accepted basis for incorporating the behavior of software into digital I&C system reliability models that is compatible with existing NPP PRAs[1]. For several years, Brookhaven National Laboratory (BNL) has worked on NRC projects, investigating methods and tools for the probabilistic modeling of digital systems, as documented mainly in NUREG/CR-6962 [Chu 2008] and NUREG/CR-6997 [Chu 2009a]. The NRC also sponsored research at the Ohio State University investigating the modeling of digital systems using dynamic PRA methods, as detailed in NUREG/CR-6901 [Aldemir 2006], NUREG/CR-6942 [Aldemir 2007], and NUREG/CR-6985 [Aldemir 2009].

[1] Existing NPP PRAs are assumed to be developed using traditional (static) event tree and fault tree methods. In order to address software failures in current PRA framework, software failures need to be captured in PRA sequences. In other words, software functions or components need to be modeled as event tree top events or fault tree basic events, and quantified using one or more quantitative software reliability methods, which are the primary interest of this study.

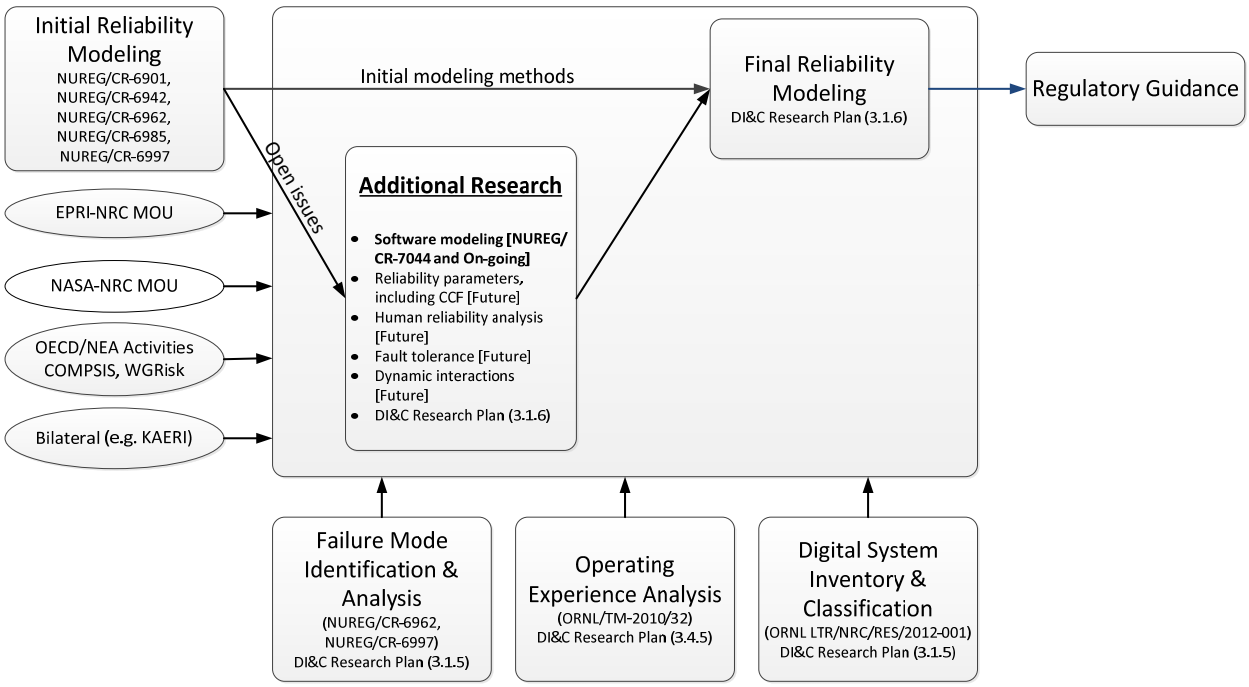


Figure 1-1 NRC Research Activities on Digital System Reliability

Software failure has been defined in the literature differently [IEEE 610, Lyu 1996] and there is no consensus on the definition. In this study, software failure is defined as the triggering of a fault of the software, introduced during its development life cycle, which results in, or contributes to, the host (digital) system failing to accomplish its intended function or initiating an undesired action. The triggering includes the generation of particular inputs to the software due to the state of the operating environment (i.e. of the NPP), in combination with the internal state of the digital system.

BNL has been exploring how software failures can be included into these reliability models, so that their contribution to the risk of the associated NPP can be assessed. Based on a recommendation from the NRC's Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital I&C Systems to investigate the philosophical basis of software failures, the NRC tasked BNL in 2008 with organizing and running an expert panel meeting (workshop) with the goal of establishing a "philosophical basis" for incorporating software failures into digital system reliability models for use in PRAs [Chu 2009b]. The experts were recognized specialists from around the world with knowledge of software reliability and/or PRA. The following philosophical basis for incorporating software failures into a PRA was established at the meeting [Chu 2009b]:

"Software failure is basically a deterministic process. However, because of our incomplete knowledge, we are not able to fully account for and quantify all the variables that define the software failure process. Therefore, we use probabilistic modeling to describe and characterize it."

They also agree that:

1. Software fails

2. The occurrence of software failures can be treated probabilistically
3. It is meaningful to use software failure rates and probabilities
4. Software failure rates and probabilities can be included in reliability models of digital systems.

Subsequently, BNL reviewed a spectrum of quantitative software reliability methods (QSRMs) to catalog potential methods that may serve to quantify software failure rates and per-demand failure probabilities of digital systems at NPPs, such that the system models can be integrated into a PRA [Chu 2010]. The QSRMs were identified by reviewing research on digital system modeling methods sponsored by the NRC or by the National Aeronautics and Space Administration, performed by international organizations, and published in journals and conferences. The strengths and limitations of QSRMs for PRA applications were categorized, described, and evaluated. In addition, a set of desirable characteristics of a QSRM was established. In a later study [Chu 2013], the QSRMs were evaluated against the desirable characteristics that were enhanced by adding a characteristic on the availability of needed data, to identify candidate methods to apply in case studies. Based on this evaluation, the statistical testing method was deemed the preferred approach. However, facing the limitations of the statistical testing method, and to account for the quality in carrying out software-lifecycle activities, it was decided to first develop a prior distribution (using the BBN method), and then undertake a Bayesian update to this distribution using the results of statistical testing. (Alternatively, a non-informative or uniform prior distribution can be used for a comparison with the BBN derived prior distribution.) Therefore, the combination of the two methods may have the benefits of both methods, that is, being able to capture the quality in carrying out the software development activities and to take into consideration the contexts defined by the accident scenarios of a PRA. Both methods were developed further to evaluate their use in estimating the probability of failure-on-demand of the software of a protection system, including examining their issues and limitations.

The study documented in this report continued the preceding work on software reliability by further developing the statistical testing method and applied it to an example system, that is, the loop operating control system (LOCS) of the Advanced Test Reactor (ATR) at Idaho National Laboratory (INL). The work involved collaboration between BNL and INL staff following the overall approach developed by BNL. In addition to supplying the ATR PRA and the RELAP5 model of the experiment loop, INL established the needed test configuration and carried out the tests. Section 2 provides more description of the approach of this study including a step by step procedure followed. A separate study at BNL based on the BBN method is ongoing and its results can be used as a prior distribution in a Bayesian analysis using the test results of this study. In this report, a non-informative prior distribution was used with the test results.

1.2 Objective and Scope

The following are the objectives of the statistical test method:

(1) Develop a statistical testing approach for estimating software failure probability on demand[2] that is suitable for inclusion of the results into a PRA; and

[2]By “demand”, it means a plant condition that requires actuation of safety systems, for example, the reactor trip system.

(2) Apply the approach to an example system to estimate its failure probability, and obtain insights into the feasibility, practicality, and usefulness of the estimation in digital system models for inclusion in NPP PRAs.

Digital protection systems modeled in a PRA may have multiple failure modes. For example, a reactor protection system (RPS) may fail to generate a reactor trip signal when a trip condition occurs, or may generate a spurious trip signal. The scope of this study is limited to modeling software failures in perform its protection functions (represented by the probability of failure on demand) at an NPP.

Presently, there is no consensus method for modeling digital systems in NPP PRAs [NRC 2008, NEA 2009]. Different methods have been proposed, including the fault tree method. However, whether or not fault tree models adequately capture the dependencies and fault tolerant features of digital systems has not been adequately demonstrated. The possibility exists that reliability models of digital systems may include software failures representing different software failure modes[3] at different levels of detail (e.g., the software may be modeled at a system, subsystem, or module level). However, a review of the literature [Chu 2010] revealed that most of the QSRMs consider the software system as a whole, not as separate modules or broken down by failure modes. That is, the software system is a collection of software including application, operating system, and platform software implemented in a digital system consisting of multiple microprocessors. Depending on the method of reliability modeling used for digital systems in a PRA, and the associated level of detail, different QSRMs may be needed to quantify the contribution of software failure to the digital system's failure probability or rate. It may also be necessary to separately model different types of software (e.g., application-specific software and operating system software), using different QSRMs. These considerations notwithstanding, for practicality, this study considered only a system level failure mode for the protection system to fail to perform its needed function, consistent with most previous QSRM applications.

Many protection systems are designed with identical redundant channels that run the same software. As such, it is expected that these channels would fail together in statistical testing due to common software faults when the same input signals are encountered. Therefore, this type of common-cause failure (CCF) can be quantified using the methods discussed in this study if multiple channels are tested simultaneously.[4] The potential for CCF between diverse channels of the same system or due to dependencies between two digital protection systems performing similar functions in the same accident scenarios was considered beyond the scope of this study. Similarly, any CCFs that can affect other plant systems modeled in the PRA are beyond the scope of the study.

---

[3] Software failure modes in this report are defined as the ways software fails from the output perspective. This definition differs from how it is defined in software failure modes and effects analysis, which is the root cause of a software failure.

[4] In addition, since the actual system hardware is used in testing. The tests also test the system hardware and its interactions with software.

2. GENERAL APPROACH

This section describes a probabilistic risk assessment (PRA) based statistical testing approach designed for estimating the failure probability of a nuclear power plant (NPP) digital protection system as originally suggested in [Chu 2013]. Figure 2-1 is a step by step flow graph of the approach of this study. The subsections of this section provide summary descriptions of the steps. Each subsection first describes the general approach of the step and then the specifics associated with this study. It also refers to later sections or subsections that provide the details of this study.

2.1 Use of PRA Defined Contexts

In a PRA, the digital protection systems can be either modeled as the top events of an event tree (e.g., a reactor protection system [RPS]) or as support system (e.g., the engineered safety feature actuation system [ESFAS]) fault trees are typically used as transfer gates in the fault trees of emergency safety features (e.g., a safety injection system). PRA scenarios leading to the demand on a digital protection system define the higher level contexts for testing the system's software. For example, an initiating event such as a small loss of coolant accident (LOCA) defines the PRA context for a RPS. The statistical testing approach of this study can be used in estimating the failure probabilities of software at the higher level of the PRA contexts.

More detailed lower level contexts can be defined using a PRA. Such contexts can be used to build the operational profiles of the system under test. For example, the cutset of a sequence that leads to a safety injection demand is a more detailed context for the ESFAS. In addition, events used in PRA are simplified representations of NPP physical operation conditions of the plant during transients and accidents. Such physical conditions could vary significantly; for example, small LOCA events can be of different sizes and can occur at different locations. Such different physical conditions might feed the safety digital system with different inputs. In this study, the cutsets and the variability in the associated NPP physical conditions constitute the operational profiles upon which test cases were generated. A thermal-hydraulic model is used to simulate the NPP physical conditions and generate the test cases.

In this project, the LOCS of the Advanced Test Reactor (ATR) was used as an example system. It controls the primary cooling system of an experiment loop (Loop 2A). Its function of generating a reactor trip signal upon detecting abnormal conditions (i.e., reactivity insertion events) in Loop 2A was tested. In the ATR's PRA, a fault tree is used to model scenarios that lead to reactivity insertion events and defines the higher level PRA context for statistical testing; its cutsets (the lower level contexts) define the LOCS operational profile. Section 4.3 provides the details of the PRA model. A RELAP5 [NRC 1995] model of the loop was used in generating the test case inputs to the LOCS. Section 5 describes the RELAP5 model in detail.

2.2 Characterization of Operational Profiles

The higher level PRA contexts described in Section 2.1 must further be characterized in terms of the variability of the associated physical conditions of the plant. The objective is to realistically represent the plant condition, especially its variability, which are inputs to the digital protection system during the transients defined by the PRA contexts. As described below, such variability can be represented by probability distributions of different types of parameters and captured in the simulations using a thermal-hydraulic model of the plant.

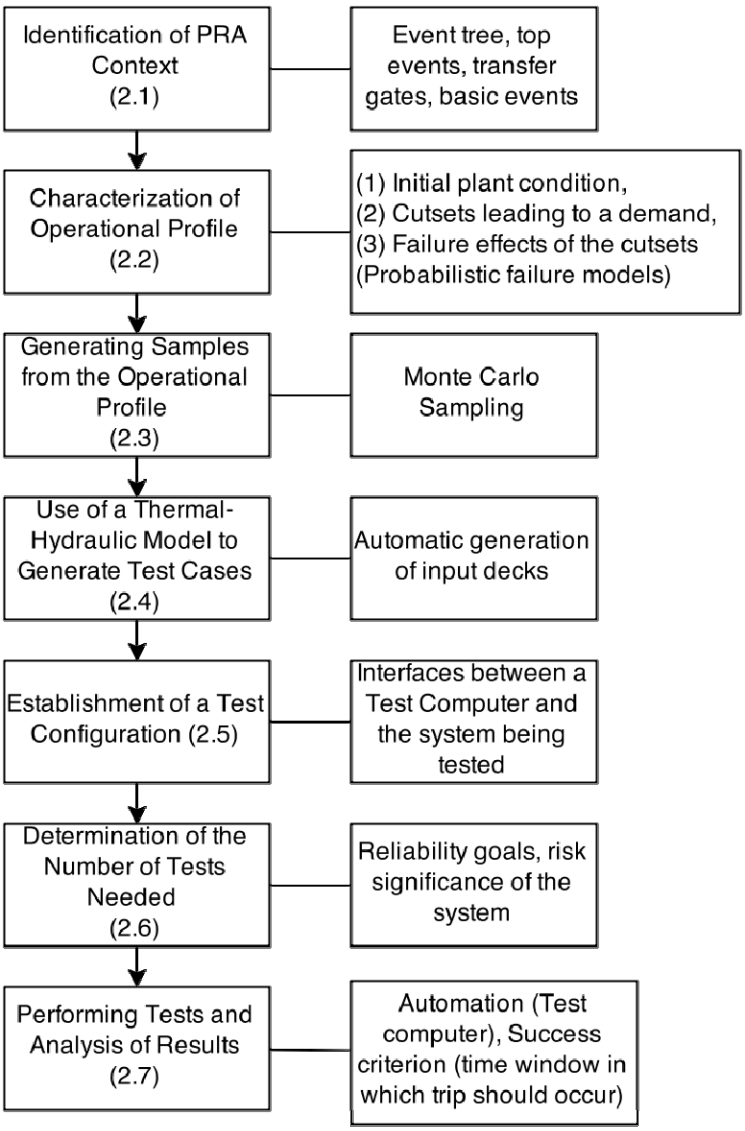


Figure 2-1 Overall Statistical Testing Approach for Quantifying Software Reliability

(1) Initial condition of the plant-The plant's condition prior to the transients/accidents can vary significantly. For example, during power operation, the reactor power may not be exactly at 100%. Such variability in power level can in general be captured by using different power levels as the initial condition of the thermal-hydraulic model.

(2) Likelihood of cutsets-Each of the higher level PRA contexts can be represented by a list of cutsets. When a sample is taken from the list of cutsets, the frequencies or probabilities of the cutsets should be considered. For an initiating event, for example, a reactor trip, a more detailed model needs to be developed to account for the different ways that the event can occur and their likelihood. The different ways may have different effects on the plant's condition.

(3) Effects of failure events modeled in the PRA- The PRA contexts are defined in terms of failure events whose failure effects may vary significantly. For example, a small LOCA initiating

event occurring at different locations may have different break sizes. Similarly, a pump may fail in different ways and has different effects to plant condition, that is, a trip of the pump leading to its coast down can lead to different plant condition than a seizure of the pump. To capture this type of variability, more detailed models of the failure events than those in the PRA must be developed. The more detailed models need to include probabilistic information such as the relative likelihood of different small LOCA locations and sizes, so that the probabilistic information can be used in sampling test cases simulated via a thermal-hydraulic model.

In this study, for simplicity, it is assumed that the reactor is at 100% power and no variation in the power level was considered. The cutsets representing different reactivity insertion scenarios were sampled according to their frequencies. Thirteen probabilistic failure models[5] were developed for 13 types of failure events represented in the cutsets. For example, the closure of a flow control valves was modeled in terms of its closure time that is assumed to be uniformly distributed between 15 and 45seconds. Section 5.2 provides detailed description of the probabilistic failure models.

2.3 Sampling from the Operational Profiles

Each test case can be defined by taking a sample from the operational profile. A sample can be generated by sampling (1) the distributions representing the plant's initial condition, (2) a cutset from the list of those representing the higher level PRA context, and (3) the probabilistic failure model of each of the failure events in the cutset.

Each sample from the operational profile then is used in defining a thermal-hydraulic run that simulates the plant condition experienced by the digital protection system. The results of the run are then used as the input to the protection system being tested.

In this study, the top 200 cutsets from the reactivity insertion fault tree were sampled according to the cutset frequencies and a total of 10,000 cutset samples were generated. For each sampled cutset, its associated probabilistic failure model's parameters were then sampled to completely define the scenario to be simulated using the RELAP5 model such that a test case can be defined. That is, each test case represents a reactivity insertion event caused by component failures in a sampled cutset with associated probabilistic failure model(s). The 200 cutsets were considered enough for the demonstration because they cover all those failures in the primary system that are modeled in the RELAP5 model; however, failures in the secondary and tertiary sides that may be dominant contributors to reactivity insertion can only be approximately modeled with this model due to the limitations that are described in Section 2.4. Section 6 details the generation of test cases.

2.4 Use of a Thermal-Hydraulic Simulation

In general, a thermal-hydraulic model that can realistically simulate the effects of the failure events sampled from the operational profile of a PRA context as described in Section 2.3 is needed. The model first should establish a steady state of the plant before failures are

[5] A probabilistic failure model is a model that uses a probability distribution to represent the variability of the associated physical process of a failure event of a PRA.

introduced. It should be able to realistically model the failure effects defined by the probabilistic failure modes.

In this study, an INL RELAP5 model of Loop 2A was modified to include additional features necessary to support the full characterization of the operational profile of the statistical testing method. One limitation of the model is that it does not include a thermal hydraulic model of the ATR. In general, the pressure tube of Loop 2A is located in the core region of the ATR and receives gamma heating from the reactor and also may transfer heat with the reactor by other means. In the Loop 2A model, the reactor is modeled as a constant heat source which should be the case before reactivity insertion occurs but not during the reactivity insertion. The RELAP5 model of Loop 2A is a simplified one, that is, it does not model all of the primary system components which are included in the PRA (e.g., the makeup to the loop is not modeled), does not include the secondary and tertiary sides of the loop, and does not model all the control functions of the loop including those performed by the LOCS. Modifications made in the RELAP model for this study were intended only to represent the failure of effects of components not included in the initial model. For example, in the RELAP5 model, the secondary side is modeled using only a boundary condition at the secondary side of the heat exchanger. Therefore, all secondary side failures modeled in the PRA had to be modeled in terms of the heat transfer coefficient at this boundary. Section 5 documents the model that was used in simulating the test cases.

2.5 Test Configuration

The objective of a test configuration is to provide test inputs such as the simulation results of a thermal-hydraulic code to the digital protection system and record the outputs from that system such that the correctness of the outputs can be verified. To make the tests realistic, the digital protection system in its original configuration, including the I/O modules, should be used. The test configuration consists of the digital protection system, a host computer, and the interfaces between them (i.e., I/O modules). The host computer controls the inputs generated from the thermal-hydraulic simulation to the protection system and performs the role of the sensors and transmitters in the plant. It also captures the outputs from the protection system and adopts the role of the equipment being controlled at the plant.

Due to resource limitations and time constraints, an approximate configuration to the actual configuration of the LOCS at the plant was used. It includes a host computer running the LabVIEW software [Labview] developed by National Instrument; it supplies the inputs to, and records the outputs from the LOCS. A complicating factor is that the LOCS also performs control functions such as flow control that involves sharing the sensors with the protection functions that are the subject of the statistical testing. It was assumed that those signals not used in the protection functions do not affect these functions and so they were given dummy values, thus, avoiding the need of a large number of I/O modules; only those signals used in supporting protection functions were used as inputs to the LOCS. This restriction reduced the number of signals from few hundred to 14 and the number of input and output modules of the LOCS to 3 analog input modules and 3 digital output modules. Section 7 describes the test configuration and its use in performing the tests.

2.6 Determination of the Number of Tests Needed

The number of test cases that are needed can be determined in two ways [Chu 2013]: (1) based on a reliability goal specified for the software, and (2) based on a software failure probability derived from risk considerations such that the software's contribution to the overall risk is considered acceptable. The number of tests without failure that is needed to demonstrate the failure probability can be determined by a standard statistical analysis.

In this study, the LOCS has a reliability goal of 10^{-4} [Marts 2012]. Using a uniform prior distribution between zero and one in a Bayesian analysis, it would require 10,000 tests without failure to demonstrate a mean failure probability of 10^{-4} [Chu 2013]. On the other hand, using risk-informed considerations, it was determined in Section 4.3 that the software failure probability needs only to be 7.2210^{-3} to make it an insignificant contributor to the risks of the reactor, and thus only 136 successful tests are needed. The main reason is the ATR has a reactor trip system that can detect reactivity increases and automatically trip the reactor, so lessening the importance of LOCS.

2.7 Performing Tests and Analysis of Results

The results of the thermal-hydraulic simulation are in the format of time-stamped records containing the values of the physical parameters representing sensor signals. The records are converted by the host computer into the format that the digital protection system can read, and are sent to the digital protection system according to the time stamps. The host computer also captures the outputs from the digital protection system and saves them as records with time stamps. The records then are examined to determine if the trip signal is generated at the right time to verify the correctness of the test results. An important part of the examination is to determine the criterion of success in terms of the time when an actual trip signal is generated, based on the design requirements of the system. For example, given a small LOCA, a high pressure safety injection system has to be actuated before core damage occurs. Therefore a safety injection signal has to be generated in this time frame. Since the digital protection system will generate a trip signal only when a threshold is exceeded, a requirement may be stated like "a trip signal should be generated within 0.1 second after the threshold is exceeded. The output record of a test can be evaluated against the input record in deciding if it is successful. The findings of the evaluation then are used in a Bayesian analysis to obtain a posterior distribution for the probability of software failure. Note that the evaluation is based on the design requirements not any physical conditions of the plant.

In this study, evaluation of test results is based on our understanding of how the test configuration works and is not related to the design requirements. The evaluation can better explain the test results especially the occurrence of trips near the beginning of the test runs. The main consideration of the evaluation is associated with the fact that the host computer and the LOCS were not synchronized. The LOCS has a cycle time of approximately 300 milliseconds, while the host computer has approximately 100 milliseconds. Accordingly, the RELAP5 model generates inputs to the LOCS at a rate of every 100 milliseconds (RELAP5 can simulate at a higher speed). Whether or not a test resulted in a success or failure was based on an estimated time-window in which the trip signal is expected to be generated based on the possible delay caused by the cycle times of the host computer and the LOCS. Section 8 provides details of the evaluation of the test outputs. A total of 10,000 tests were performed and

no failure was observed. Using this data in a Bayesian updating of a uniform prior distribution, a mean value of $1*10^{-4}$ was obtained[6].

2.8 Assumptions and Limitations

Potential limitations of the application of the statistical testing approach are summarized and demonstrated in terms of the following examples. More detailed discussions are presented in the individual sections on the subjects.

(1) Whether or not the PRA accurately models the demands on the protection system. For example, in this study, the different ways reactivity accidents can occur have been explicitly modeled and the mitigation of the accidents varies with the accidents' severity that has to be accounted for by introducing additional branches in the event tree. In addition, both the control and protection functions of the LOCS are modeled in the PRA, and the dependency between the two functions must be correctly modeled. The use of only the top 200 cutsets in generating the test cases also is a limitation of the study. Additional cutsets and non-minimal cutsets may represent additional failure scenarios that were not included.

(2) Whether or not the probabilistic failure models of the failure events truly represent such events in terms of their effects and associated probability distributions. In this study, a few probabilistic failure models were developed to capture the potential variability of failure events modeled in the PRA. In this study, the use of uniform distributions is a simplifying assumption. It may be improved if engineering and data analyses of the failure modes are performed.

(3) Whether or not the thermal-hydraulic model realistically models the plant and the failure effects. This issue is applicable to any thermal-hydraulic modeling. In this study, the RELAP5 model has only simplified models of some of the control functions of the LOCS that is the subject of the study. Therefore, the thermal-hydraulic response during a reactivity accident may not be realistic.

(4) Whether or not the test configuration truly represents the configuration of the digital protection system during its actual operation. For example, in this study, the use of fewer I/O modules for protection functions and the use of dummy values to simulate the control functions of the LOCS may affect the system's internal states.

(5) Whether or not the timing criterion in determining if a test result represents a success should be based on engineering analyses. The design of a protection system should be based on engineering consideration of the potential accidents. In this study, the engineering (design basis) analysis was not available, however the maximum allowed channel response times of different types of trips (e.g., low flow, high temperature, and low pressure) were specified with the shortest maximum response time being 0.78 second [INL 2010] for low pressure[7]. Instead of using the channel response times, this study's success criterion was determined from the

---

[6] Note that the use of a different prior distribution would result in a different estimate of posterior reliability. For example, a Jeffreys non-informative prior would result in a reliability estimate of $5*10^{-5}$.

[7] The maximum allowed response times for the low flow and high temperature trips are slightly longer than the low pressure trip and were specified as 1.13 seconds.

cycle times of the LOCS and the host computer. That is, a time window during which a trip signal should be generated was estimated based on input records, and a test is considered a success if the actual trip signal is generated within that window.

All the above considerations are related to the realism and accuracy of the different models used. The potential effects of the lack of realism or accuracy are difficult to quantify. Such limitations are shared by any modeling efforts. It is desirable to develop some criteria for the models' degree of realism and accuracy that can be linked to the accuracy of the estimated probabilities of software failure.
The assumptions and limitations of this study are discussed in more detail in later sections. In addition, Section 2.9 discusses a theoretical issue that seems to claim that the statistical testing method is non-conservative, and provides counter arguments that support the statistical testing method.

2.9 An Issue on Quantifying Software Failure Probability Using Statistical Testing

In this section, an important issue associated with estimating the probability of software failure using the statistical testing approach of this study is discussed. This problem was first pointed out by Miller [1992] and further extended by May [1995]. It suggests that the quantification method of software failure probability of this study may be optimistic and non-conservative. Kuball [2004] considers that this drawback has not been adequately addressed. A literature search was performed as part of this study; the search did not find any significant recent progress in the area. We summarize the issue here and provide arguments that show the quantification method used in this study is not optimistic as the earlier research suggested.

The issue identified in the earlier research can be demonstrated in terms of an example. Consider a simple case in which a system is needed in 10 different PRA contexts (each with its associated path in the software) with the same frequency of occurrence. Assuming the same number of tests were performed with no failures in each of the contexts, *regardless of the quantification method used*, the mean software failure probability of the individual contexts and the mean of the averaged system failure probability (over the contexts) are the same. On the other hand, if the same tests performed above are considered black-box tests at the system level, that is, the tests for the PRA contexts are combined as the black-box tests of the overall system, then a smaller mean system failure probability (by a factor of ~10) would be obtained. May [1995] pointed out this discrepancy in terms of partitioning of the input profile and the associated software portions that are exercised by the different partitions. He pointed out that the tests performed for specific partitions (PRA contexts) do not test the complete software and that combining them and using them in standard statistical analysis for the system may be non-conservative. On the other hand, he considered that averaging over the partitions assumes they are completely independent and may be unduly conservative. (A basic problem with the averaging is that it does not account for the overlaps in the paths followed by the test cases.) May's interpretation has a deeper implication because if the test results obtained for different PRA contexts cannot be combined and used at the system level in quantifying the probability of system failure due to non-conservatism, then quantification at the individual context level also may be subject to the same issue because a PRA context can be further decomposed into sub-contexts. Therefore, quantifying at a PRA context level may also be non-conservative, unless the digital protection system software has only one pathway for the context.

The statistical testing approach of this study considers the contexts (cutsets) defined in the PRA and performs tests sampled from the cutsets (contexts) using a black-box approach. Each sample challenges the part of the software that is needed in performing the specific protection function (e.g., actuating safety injection on low system pressure), and may not challenge other parts of the software that are exercised only by the system's other protection functions (e.g., actuation of safety injection on high system temperature). In this sense, the statistical testing approach has some flavor of white-box testing [May 1995]. In general, the same software may have different failure probabilities for different PRA contexts. This is the case when different initiating events demand that a reactor trip signal be generated, for example, a loss of feedwater initiating event may lead to a reactor trip on a low steam generator level while a reactivity accident may lead to a reactor trip on high neutron flux.

In this study, a black-box quantification method was used, therefore, it effectively calculated an overall system failure probability over the different contexts. Since each test case was sampled from the operational profile and follows a particular path in the software, (1) the probability that the path is visited is automatically accounted for by the sampling from the operational profile and (2) the overlap of the paths in the software followed by different test cases are also automatically accounted for. Besides the limitations on the realism of the PRA and thermal hydraulic models used and the test configuration used, the tests results are effectively the same as the data collected from operational experience. This is the reason that the quantification method would generate the correct estimate, as opposed to what the earlier research suggested that it may be optimistic.

3. SYSTEM DESCRIPTION

In this section, the Advanced Test Reactor (ATR) at Idaho National Laboratory (INL) is briefly described. In particular, the example system of this study, that is, the loop operating and control System (LOCS) of an experimental loop, is discussed in more detail. The descriptions in this section are based on three ATR documents [INL 2008, 2009, and 2010].

3.1 ATR Facility Description

Idaho National Laboratory's (INL) Advanced Test Reactor (ATR) is a 250-MWth light water moderated and cooled reactor located at the ATR complex on the INL site. Its initial mission was serving the U.S. Navy in research on nuclear-propulsion systems. In 2006, it was designated as the National Scientific User Facility (NSUF) that supports nuclear-engineering programs at universities and collaborations among researchers working in nuclear fuels and materials.

The ATR core (Figure 3-1) has a serpentine arrangement that permits positioning of the fuel closer to the positions of the flux-trap than does the traditional rectangular grid. The reactor has a maximum thermal power of 250 MW. The coolant is pressurized water at 2.5 MPa (360 psig). Water enters the bottom of the vessel at an average temperature of 52 ^{o}C (125 ^{o}F) and flows upward through the annulus outside the cylindrical tank containing the core. The coolant then moves down through the core and, at full power, leaves the core with an average temperature of 71 ^{o}C (160 ^{o}F).

The core is composed of fuel plates arranged in assemblies, each with 19 plates; there are 40 assemblies. These curved-plate fuel elements are arranged in a serpentine shape around a 3x3 array of primary testing locations. The ATR contains 68 experiment positions and nine high-intensity neutron flux traps, six of which are equipped with pressurized water loops. Each of the water loops can be operated independently with a preset temperature, pressure, and flow rate. The temperature and pressure for the experiment loops may be set higher than the standard operating condition of commercial pressurized water reactors (PWRs). These six experiment loops are designated 1C-W, 1D-N, 2A-C, 2B-SE, 2D-SW, and 2E-NW. The loop studied in this research was 2A-C. Figure 3-2 shows the location of some of these experiment locations in relation to the fuel elements.

The piping assembly for each experiment loop consists of three concentric loops (Figure 3-3). The assembly penetrates the vessel's bottom closure plate and has its inlet and outlet below the vessel. For most loops, the coolant flows upward through the innermost tube (flow tube) and passes the sample. Near the top of the vessel, the coolant flows down the annulus enclosed by the pressure tube. For loop 2A-C, water moves upward through the outermost tube and downward through the inner annulus. Helium flows through the annulus enclosed by the outermost tube; it serves as an insulating jacket that is needed because the inside of the pressure tube is in contact with the high temperature loop coolant.

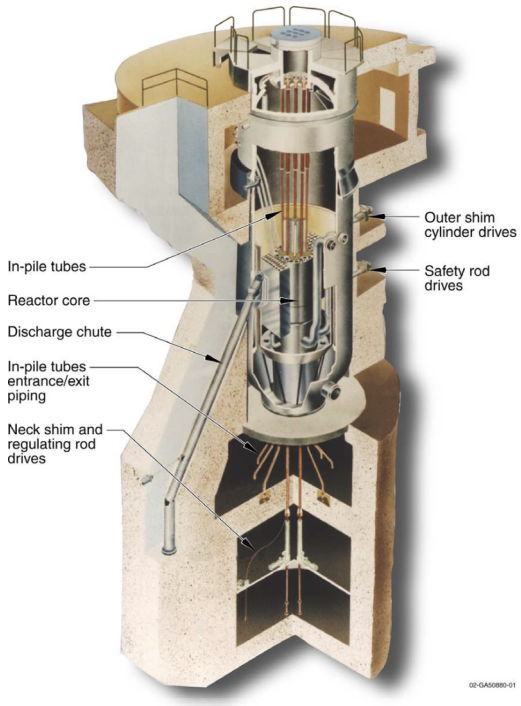


Figure 3-1 Location of the in-pile tubes in the ATR and cut-away view of the core

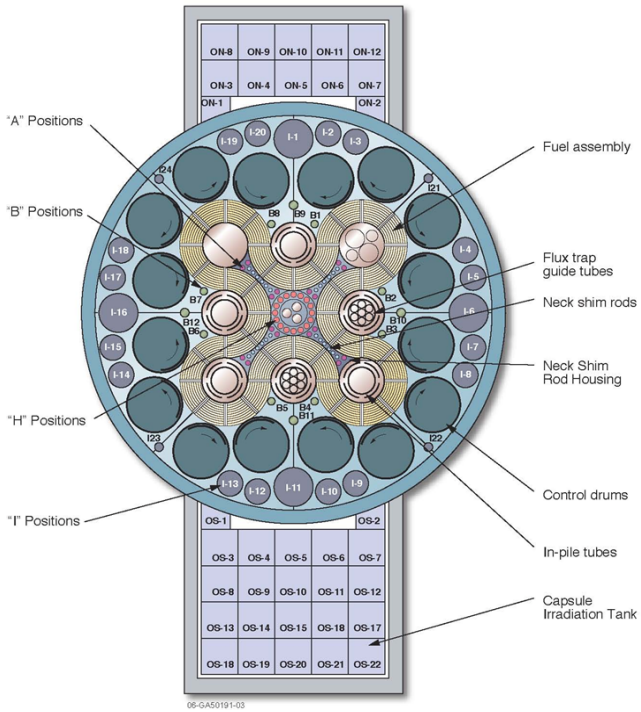


Figure 3-2 ATR's flux trap and irradiation test positions

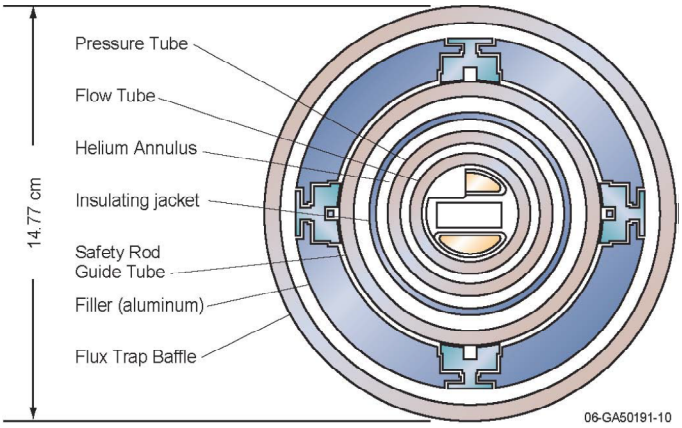


Figure 3-3 Cross section of the in-core portion of a typical pressurized water loop

The ATR has six in-pile tubes (IPTs) through which water circulates at set pressure, temperature, and flow rate. The IPT essentially is an insulated pressure vessel within the reactor vessel and serves as the experiment portion of the test loop that lies within the reactor vessel. The flow rate is between 10 and 80gpm. IPTs are used for irradiating the experimental material and nuclear fuel specimens. Line heaters are available that can raise the temperature of the loop coolant. Figure 3-4 is a schematic representation of loop 2A showing the location of the IPT in relation to other components.

3.2 Overview of the Loop Operating Control System

The function of the loop operating control system (LOCS) is to detect abnormal conditions in the IPT and its supporting systems that can lead to damage of the hardware or disruption of the experiment. The LOCS is used to control the loop parameters specified by the sponsor's experiment requirements and to provide protective interlocks for the loop equipment. The LOCS protective function detects abnormal conditions and initiates actions to mitigate damage to the loops' hardware and to experiments.

The major component of LOCS is the Metso Automation maxDNA distributed control system (DCS) which comprises one remote processing unit (RPU) per experiment loop. Each RPU contains the I/O modules, two pairs of redundant distributed processing units (DPUs), two pairs of redundant power supplies, and two optical-to-electrical interface modules. For each loop, the RPU is contained in two RPU cabinets. Each cabinet contains two redundant 120- VAC to 24-Vdc power supplies, input and output modules, and a DPU pair. The input modules interface with the loop equipment to convert field signals into digital ones. The output modules convert digital signals to interface with the loop equipment, for example to start or stop a piece of equipment. The two pairs of DPUs (A/B and C/D pairs) interface with the I/O modules to operate the loop equipment since a single DPU cannot process all the information needed to control the loop facility. There are two pairs of redundant power supplies that power the electric equipment such as the RPU and transmitters. A dual-directional fiber-optic highway is used for communication between the workstations and the RPUs.

3.3 LOCS Control Functions

The control functions of LOCS are designed to maintain the conditions in the experiment loop within the range specified by the experimenter. Failures of the control functions may result in reactivity insertion accidents. During reactivity accidents initiated in the loop, the control functions if available continue controlling the thermal hydraulic conditions of the loop. Equipment controlled by LOCS include the primary coolant pumps, loop line heaters, loop pressurizer heaters, makeup pumps, purification flow control valve, makeup system recirculation pump, and conductivity flow control. The process variables controlled by the LOCS are the primary coolant flow rate, temperature, and pressure, the degassing flow rate, and the flow rate at the exchanger column.

The control of the primary coolant flow rate consists of a PID (proportional, integral, and derivative) controller which outputs to the loop flow control valves via an analog output channel. The PID input is selectable between the IPT inlet flow channels A and B. At any time, only one of these two channels is selected. The loop flow control valve (FCV) opens on the loss of either air or an electrical signal. They are fully open at 4 mA and fully closed at 20 mA. The DCS fully close the valves when the operator's input is 0%and fully open them on an input of 100%. Increasing the controller output (opening the FCV) increases the loop flow. Figure 3-4 shows the location of the FCV in loop 2A.

The primary coolant temperature is controlled via the temperature control valve (TCV). The input to the PID controller is selected from the mixing tee outlet temperature channels. The feed-forward control is selectable between two IPT outlet temperature channels. The loop TCV provides full flow to the loop heat exchanger on a loss of either air or an electrical signal. A 4 mA output signifies that the valve is providing full flow to the heat exchanger; a 20 mA output means a full bypass. The DCS provides a full flow through the heat exchanger on the operator's input of 0% and a full bypass on the operator's input of 100%. Decreasing the controller's output lowers the temperature in the loop.

Control of the primary coolant temperature also can be achieved via the line heater. The power for a clamp on line heaters is controlled proportionally by silicon-controlled rectifiers (SCRs). The input to the PID controller is selectable between two mixing tee outlet temperature channels. A 4 mA output corresponds to 0% power to the line heaters while a 20 mA output corresponds to 100% power. Decreasing the controller output lowers the temperature of the loop.

The loop degassing flow also is regulated by LOCS. The control rate of degassing is achieved by adjusting the degassing flow rate to each loop pressurizer. The PID controller determines the output to the degassing flow control valve via an analog output channel. The input to the PID controller is the degassing flow. The valve will close on a loss of either air or an electrical signal. Decreasing the controller output (0% output corresponds to a closed valve) will lower the flow.

The flow in the ion-exchange column is controlled by regulating the flow rate of the coolant to the purification ion-exchange column; the latter is done by adjusting the flow rate of the primary coolant to the manifold. The PID controller is used to determine the output to the ion-exchanger flow control valve via an analog output channel. The input to the PID controller is the ion-exchanger inlet flow. The valves close on the loss of either air or an electrical signal. Decreasing the controller output (which closes the valve) reduces the flow. The valve automatically closes on a high temperature in the ion-exchanger inlet. In addition to the

processes detailed above, the LOCS similarly controls the pressurizer level and the makeup system storage tank.

The LOCS control function extends to individual components such as the primary coolant pumps, loop line heaters, loop pressurizer heaters, makeup pumps, and the makeup system's recirculation flow and level control. The control components include the sensors and the DCS. There are two sensors, each connected to a separate input module which, in turn, is connected to the DCS. Only one sensor is used for control at any time; the operator manually can select the sensor to use. There is no automatic switching upon failure of the input channel. The DCS has redundant 24 VDC power supplies for which there are two separate 120 VAC power sources. The loss of DPU communication from the redundant DPUs with the I/O modules will cause a reactor scram.

The primary coolant pumps are powered by either commercial or diesel sources with the restriction that only one pump is allowed to operate on diesel at any given time. The pumps can be shut off (unless set in a bypass or RTD mode) by a trip signal from an overload condition, a low-low trip from the net positive suction head to the first pump, or a low-low high pressure demineralized water (HDW) coolant pump.

The makeup pumps maintain level control in the pressurizer. The pump starts on a pressurizer low-level signal and shuts off on a high-level signal. The pumps also are turned off from either a high pressurizer or high inpile tube-inlet pressure signal.

The control of the makeup system's recirculation flow and level control (there are two makeup systems) comprises a recirculation pump and a level controller. The level in the storage tank determines if there is an adequate water supply to the recirculation pump; this pump is shut off after an alarm for a low-low level in the storage tank. The level in the storage tank is used to determine if the water supply is adequate for the loop makeup pumps. The control valve for the storage tank level is opened when it is low.

3.4 LOCS Protective Functions

The protective functions of LOCS are designed to initiate mitigating actions to prevent damage to the loop hardware and installed experiments. The LOCS monitors seven process variables. The conditions for scram are the following: (1) low IPT inlet flow, (2) low IPT inlet pressure, (3) high IPT inlet temperature, (4) high IPT outlet temperature, (5) high temperature of the experimental specimen, (6) high IPT coolant differential temperature, and (7) low voltage on the loop coolant pumps. Conditions (1) through (4) are designed to protect the IPT and will always cause a scram (if not disabled which is only allowed during reactor outage), whereas conditions (5) and (6) can be set to either scram or power setback. Condition (7) will cause a scram if the function is enabled; if not required, this function can be disabled.

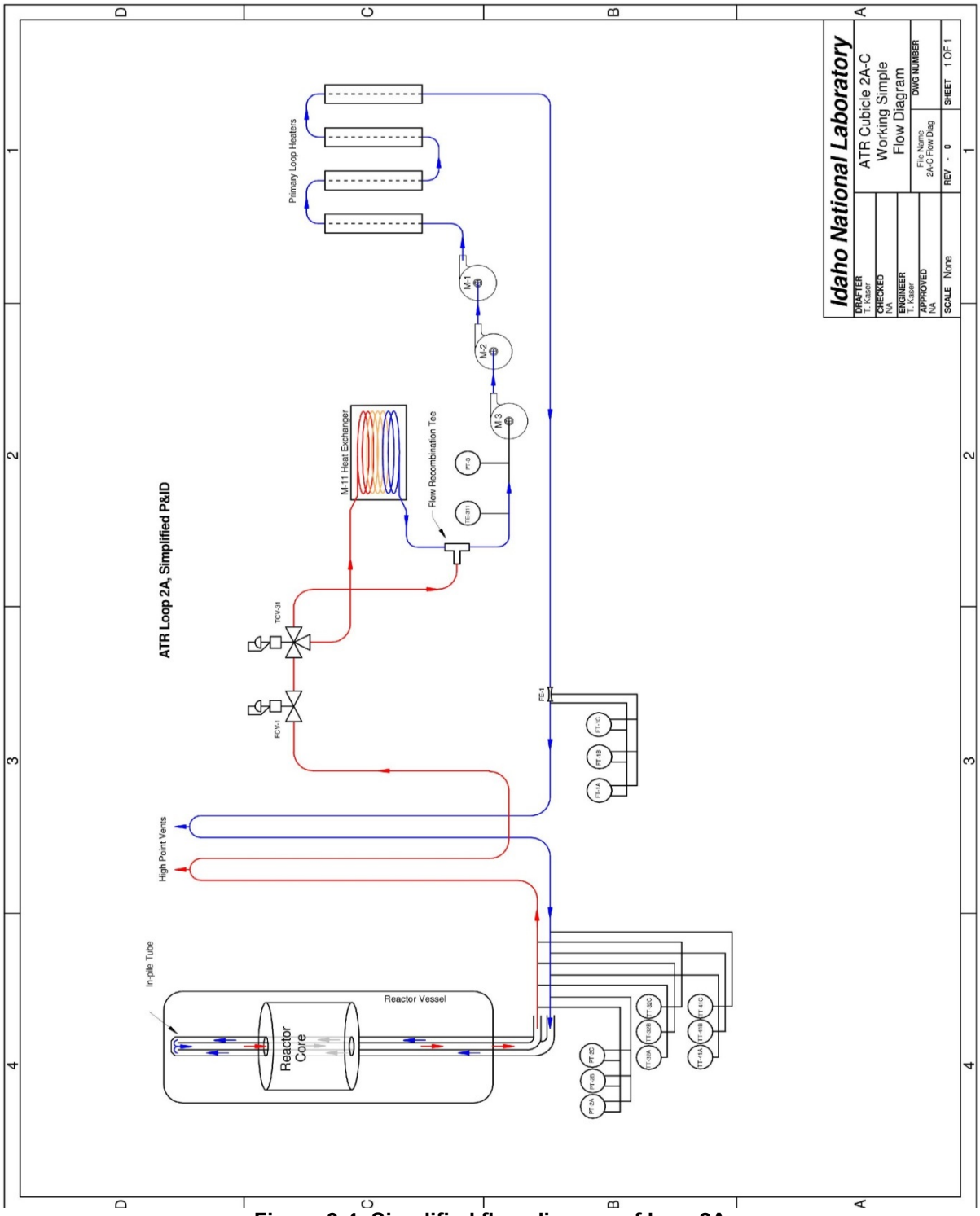


Figure 3-4 Simplified flow diagram of loop 2A

A low IPT inlet flow is detected via delta pressure. Rosemount 1151 Smart transmitters convert the signal into 4 to 20mA input to the DCS. Three inlet flow transmitters (channels A, B, and C) are connected to three separate analog input modules. Low IPT inlet pressure and high IPT inlet and outlet temperatures also will trip the reactor. Both are also required for protecting the IPT. Their temperatures are sensed via 4-wire, platinum-type resistance thermal detectors (RTD). Rosemount 3044 smart temperature transmitters convert the RTD signal to a linear 4 to 20mA signal for input into the DCS.

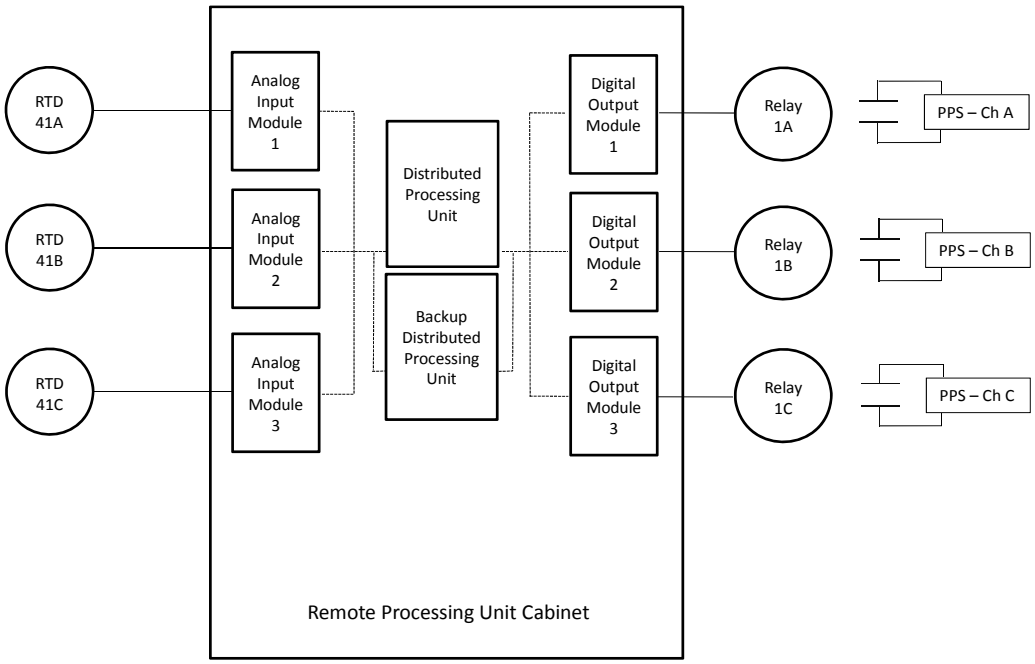
A high temperature in an experimental specimen can either trip the reactor or initiate a power setback. This function can be disabled if it is not required. Sensing is done by thermocouples in the experiment test train. High IPT coolant differential temperatures either trip the reactor or initiate a power setback; this function also can be disabled if not required. Sensing is done by the difference between the temperatures of the IPT outlet and inlet; the difference is calculated in the DCS. The low loop coolant pump power (low voltage) can trip the reactor; it also can be disabled. Two under voltage relays monitor the differential phase voltages to each loop primary coolant pump. Each pump can be chosen to scram on low voltage or can be bypassed.
For the conditions that initiate a reactor trip, there are three scram channels (A, B, C), each with its own analog input modules. For example, all channel B inputs are connected to analog input module B. The three scram channels are driven by three separate relay output modules that normally are energized. With a trip from any experiment loops, all three relay output channels are deactivated (de-energized), causing the contact-to-logic level convertor (CLLC) modules to trip. Each parameter uses a 2/3 logic block to process a trip signal such that at least 2 out of 3 analog input modules must be in a trip condition for the reactor to trip.

To ensure the integrity of the DPU, a watchdog timer continuously checks the status of the DPUs. The watchdog timer will trip the reactor five seconds after a loss of a loop's DPU pair. The timer operates by having three digital output channels on three separate digital output modules toggle on/off every second. The digital outputs are connected to three separate dead-man timer relays that cause the reactor to trip if the on/off cycle is interrupted for more than five seconds. LOCS connects to the reactor PPS channels A, B, and C through the CLLC which provides the 12 VDC that is interrupted by a trip.

Figure 3-5 illustrates the connections involved in the protective function of sensors TT-41. The three TT-41 sensors, TT-41A, TT-41B, and TT-41C monitor the IPT inlet temperature. Each sensor is connected to its respective analog input modules whose output is connected to the DPU pair. The DPU will initiate a reactor trip from high IPT inlet temperature if two out of these three sensors read a trip condition. In this state, the DPU sends out a trip status to its three digital output modules that are connected to the CLLC which in turn interfaces with the plant protection system (PPS). A reactor trip occurs when at least two of three scram relays are de-energized.

Figure 3-6 shows another view of the logic involved for the IPT inlet temperature protection channel. It illustrates how the different protective functions are logically connected to each other via an OR gate. Hence, regardless of the channels that initiate the trip, the three digital output modules should normally be in the same state (i.e., the status of all three should show a either a trip or non-trip). In all, two 2/3 logics are used in the protection channels: one is used at the level of sensor/analog input module; a second is at the level of the digital output modules.

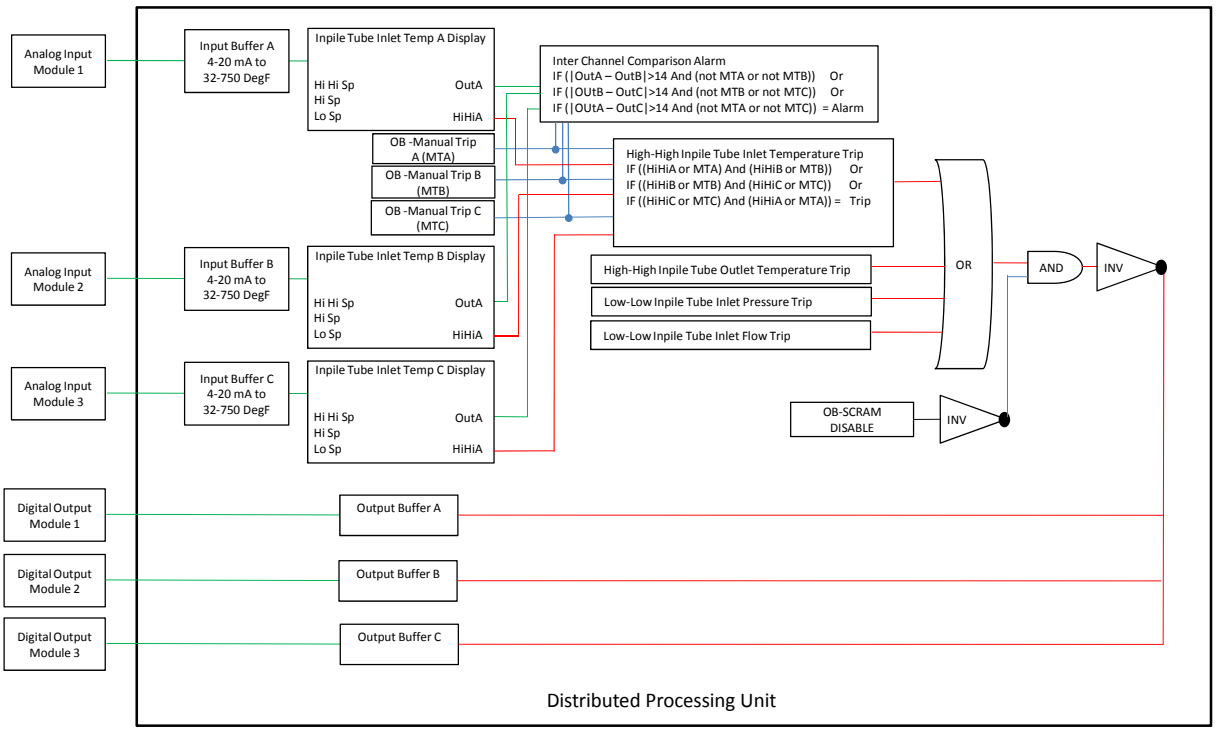
INPILE TUBE INLET TEMPERATURE CHANNEL PROTECTION ONE LINE DIAGRAM



RTD – Resistance Thermal Detector
PPS – Plant Protection System

Figure 3-5 IPT high inlet temperature protection channel

INPILE TUBE INLET TEMPERATURE CHANNEL PROTECTION ONE LINE DIAGRAM



HiHi – Out above the Hi Hi set point (SP)
MT – manual trip (channel out-of-service)
OB – Operator Button (Off/On)

Inv – Inverter
Out – Engineering Units (for temperature degrees Fahrenheit)
SP – Set point

Figure 3-6 Typical processing logic of the loop protective channel

4. PRA MODEL DESCRIPTION

4.1 Overview

The probabilistic risk assessment (PRA) of the Advanced Test Reactor (ATR) was used in this study in defining the PRA contexts employed in generating test cases for the loop operating and control system (LOCS) of experiment Loop 2A; this is one of the six experiment loops modeled in the PRA. That is, the reactivity insertion accidents due to component failures in Loop 2A serve as the demands on the LOCS to generate a trip signal and are used in generating test cases for statistical testing. This section describes the PRA model that was used in defining and generating the test cases simulated using a RELAP5 [NRC 1995] model of Loop 2A (see Sections 5 and 6).

Section 4.2 describes the role that the LOCS plays in the ATR's PRA in terms of its control and protection functions. Section 4.3 details the reactivity insertion accidents associated with Loop 2A that are modeled as a fault tree in the PRA. It also describes the changes that were made in ATR PRA to meet our specific needs[8]. Sensitivity and importance calculations were performed to gain insights from the model. Section 4.4 uses the PRA model in some risk-informed considerations regarding the needed reliability for the LOCS software and the number of tests without failure to demonstrate the reliability. Section 4.5 summarizes the assumptions and limitations of using the PRA model.

4.2 LOCS's Role in ATR PRA

As described in Section 3, the ATR has 6 experiment loops including Loop 2A, the subject of this study. Each experiment loop is controlled by a LOCS that maintains the loop in a steady state condition. In addition, the LOCS has protection functions that can detect abnormal conditions and initiate mitigating actions to protect the IPT; in some cases, the LOCS may generate a reactor trip or power setback signal when some physical parameters of the loop exceeded their corresponding thresholds. In the ATR's PRA, the different experiment loops are modeled in the same way while accounting for minor differences in design between the loops. The following is a detailed description of how Loop 2A and its associated LOCS are modeled in the PRA.

In the ATR's PRA, the experiment loops are modeled in an event tree that models the associated reactivity insertion accidents. For example, a large LOCA in the loop may result in voiding in the loop which is a fast and large reactivity insertion; a trip of the loop's primary cooling pump may lead to a slower reactivity insertion. Loop 2A is modeled in terms of two fault trees: (1) One that models potential reactivity insertion accidents due to failures of components associated with the loop, including those of the LOCS, for example, failure of the LOCS's pressure control function, and (2) A fault tree that models failure of LOCS's protection functions (i.e., high inlet and outlet temperature, low flow, and low pressure) due to failures of LOCS's

[8] It should be point out that BNL does not have detailed design information on the ATR, especially on the LOCS. The ATR's PRA was provided to BNL without any documentation except for those from a few conferences between BNL and INL to resolve some questions directly related to the modeling of the LOCS. The changes made to the PRA were based on the judgment of the BNL analysts and may not be consistent with the ATR design. This approach is considered not to affect the objective of demonstrating the statistical testing approach.

components during reactivity insertion accidents[9]. The first fault tree is used in calculating the frequencies of different reactivity insertion scenarios (cutsets) defining the PRA context for the statistical testing of this study. The LOCS is modeled in the two fault trees that are effectively intersected (ANDed) in the event tree sequences that model the mitigation of the reactivity accident. The intersection of the two fault trees assumes that any cutset of the first fault tree can be mitigated with the same logic in the second one. In addition, the PRA assumes that any failure of the modeled protection functions would result in a failure to trip. This assumption is conservative because for each reactivity insertion accident, there may be more than one protection function that would generate a trip signal.

In the ATR's PRA, there are three ways in which signals may be generated that would result in a reactor trip or power setback: (1) The plant protection system (PPS) responds to any reactivity accidents and triggers the rapid insertion of the control rods; (2) the LOCS generates a reactor trip signal when the threshold of some physical parameters in its loop is exceeded (i.e., the inpile tube low inlet flow, low inlet pressure, high inlet temperature, and high outlet temperature) with a maximum delay of 0.3 second of the system's cycle time; and, (3) the LOCS generates a setback signal to insert the shim rods upon high specimen temperature or high coolant differential temperature of the IPT. The trip signals generated by PPS and LOCS activate insertion of the same control rods, while a setback signal would activate the insertion of a different set of rods that may take few minutes to complete. In the PRA, depending on the timing of the reactivity insertion scenarios, credit was taken for different combinations of the signals in shutting down the reactor for different reactivity insertion scenarios. Section 4.3 details the modeling of the PRA. Failure of the LOCS to generate a reactor trip signal is modeled in terms of failures of its components. For example, failures of two out of three digital output modules would cause a failure to generate a reactor trip signal.

Failure of the LOCS control functions contributes to reactivity insertion accidents and failure of its protection functions would contribute to failure to mitigate the reactivity accidents and the associated core damage frequency. Section 4.3 calculates these quantitative contributions of the LOCS.

4.3 PRA Analysis of Reactivity Insertion Accidents of Loop 2A

In the ATR PRA, one of the event trees models the Loop 2A reactivity insertion accidents. In this event tree, a fault tree is used to model the different ways in which reactivity insertions can occur due to failures of the equipment of Loop 2A. A separate fault tree is used in modeling the protection functions of the LOCS. Section 4.3.1 describes the event tree on reactivity insertion accidents associated with experimental loops and the fault trees associated with different ways reactor trip signal can be generated. Section 4.3.2 describes the fault tree that models reactivity insertion accidents; Section 4.3.3 describes the changes BNL made to the PRA model to meet the needs of this study including the event tree that models the LOCS. Section 4.3.4 discusses some results of the analysis, including the risk contributions of the LOCS.

[9] The protection functions of the LOCS are designed for protecting the IPT. The use of some protection functions in the PRA to mitigate reactivity insertion accidents may not have a good basis unless the selection of the thresholds considered reactivity insertion accidents.

4.3.1 Description of Reactivity Insertion Event Tree

Figure 4-1 shows the original RLH event tree that models how the reactivity insertion associated with the experiment loops can damage the core. The initiating event is calculated via the fault tree RLHIE that includes events related to all six experiment loops, but unless otherwise stated, this report looks only at events related to loop 2A. The RLH event tree is set up so that should there be a reactivity insertion, the LOCS protection first is queried to determine whether it can trip the reactor. Failure of the LOCS protection function is modeled using the LOCS fault tree that considers both the LOCS hardware (e.g., the data processing units (DPUs), sensors, analog input modules (AIMs)) failures, and other failures including mechanical (e.g., stuck control rod) failure, rod clutch control system (RCCS) failure, and the CCF of divisional logic. The mechanical failures comprise individually stuck rods and common cause failures that result in the failure of insertion of multiple rods. Should the LOCS fail to trip the reactor, the RLH event tree first uses the SLH fault tree to determine whether the plant protection system (PPS) can mitigate the accident. Examples of dominant causes of failure for the PPS are stuck rod and failure of the RCCS. An example of a PPS-specific failure event is a failure of the transmitters from the high neutron flux instrumentation. Should the PPS fail to trip, the last opportunity to do so is via manual shutdown and slow insertion (MRSR). If an event fails the LOCS, SLH, and MRSR, then it ultimately leads to core damage (P4 state in RLH). Even with a successful trip, it is possible that a loss of long-term cooling also leads to core damage. These events are further developed via the transient event tree that transfers off some braches in the RLH.

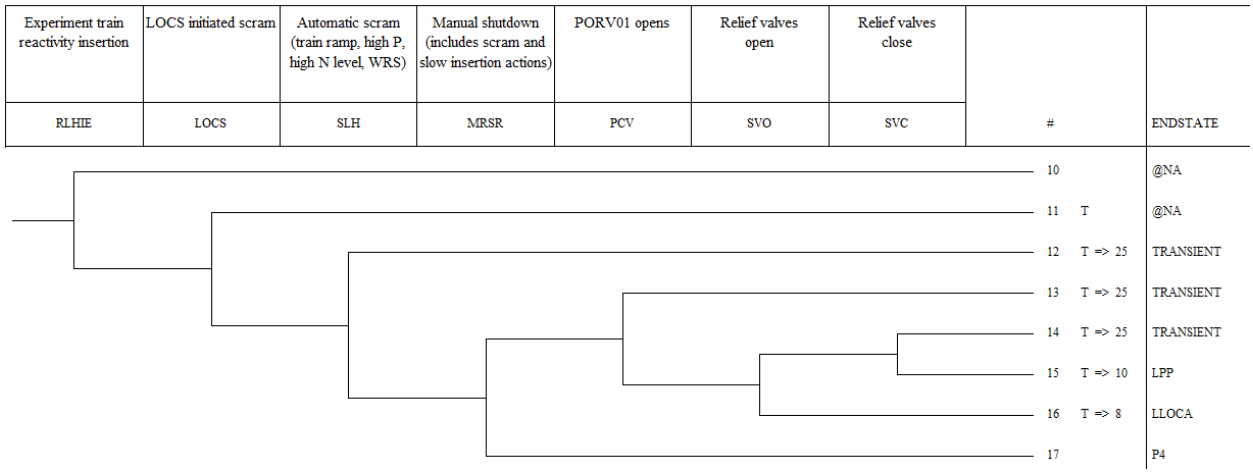


Figure 4-1 The RLH event tree in the original PRA model

It is noted that in the PRA model, the LOCS and SLH use the same fault tree, while flag sets[10] are used to select appropriate branch when solving the event tree. LOCS and SLH share some events, such as a stuck rod, whereas LOCS-specific subtrees simply are de-selected when

[10] A flag set is a feature of the Saphire code. It is a set user-defined changes that are used to indicate modifications to particular events on a sequence-by-sequence basis. For example, a flag set can be used to set a house event (i.e., a Boolean event) to TRUE or FALSE.

solving SLH. The MRSR tree also partially shares subtrees with LOCS and SLH but it contains added logic that models slow insertion.

The MRSR tree accounts for both manual scram and the slow insertion system. The latter basically is a mechanism to reduce the power of the reactor after an event. This is achieved via a rotating drum with the neutron absorbers covering half of the drum. Normally, the absorber face points away from the core, but on demand, the drums rotate the absorber face towards the core, thereby reducing neutron flux. A typical demand for the slow insertion system is when the temperature of an experiment specimen is too high. Then, a reactor trip may not be immediately necessary and slow insertion can be used to reduce the reactor power to lower the specimen temperature to an acceptable value. The time needed for reducing power typically is several minutes. Accordingly, for events that need a fast reactor trip, the MRSR tree cannot be credited.

The description in this subsection refers to the original event tree in the PRA model. Modifications were made that alter some of the above logic to account for accidents wherein some of the trip system cannot be credited. For instance, a large break in a pipe will lead to a reactivity insertion sufficiently fast that neither the LOCS nor the MRSR can prevent core damage. The logic of the RLH tree then must be modified to reflect this assumption. This is detailed in Section 4.3.3.

4.3.2 Description of the Reactivity Accident Fault Tree

This section discusses in depth the reactivity insertion fault tree (RLHIE). The RLHIE tree is structured so that events related to each of the six experiment loops are contained in their own subtree. Failure in the top event of any of these subtrees results in RLHIE failure (i.e., the subtrees are joined via an OR gate). This work focuses only on loop 2A; therefore, subtree EXT-2AC-AQU is the focus of the discussion in the rest of the section. Further, the subtrees representing other experiment loops are structured in the same way as EXT-2AC-AQU (but with different basic events).

Figure 4-2 shows the top part of the EXT-2AC-AQU. Solving this tree will yield all the events originating from loop 2A that will cause reactivity insertion. These events are categorized into three subtrees: failure of the flow equipment (EXT-2AC-FEQ), the temperature equipment (EXT-2AC-TEQ), and the pressure equipment (EXT-2AC-LPEQ).

The EXT-2AC-FEQ subtree models events that can cause low flow in loop 2A. This low flow condition increases the loop temperature that ultimately can lead to reactivity insertion via voiding. (ATR has a positive void reactivity coefficient.) For example, the “flow element FE-1 plugs” event will result in a low flow condition and, therefore, is modeled under the “flow equipment failure” subtree. The PRA model considers plugging at three locations (flow elements FE-1 and FE-2, and strainer-145); these three constitute three separate events. Similarly, EXT-2AC-TEQ looks at events that can directly increase the temperature; they include failure of the line heater control and the temperature control valve. Finally, the tree EXT-2AC-LPEQ looks at events that cause the loop pressure to drop, including pipe break and failure of the pressurizer heater. Table 4-1 shows all the events in each of these three subtrees; some events therein may be caused by several different failures. For example, the “temperature control component failure” event can be caused by a failure of the DPU pair, the analog input modules (AIMs), the analog output modules (AOMs), or other components of the temperature control system.

Some component failure causes multiple failures of the control functions and the protection functions. For example, failure of the DPU pair leads to a simultaneous loss of control of temperature, flow, and pressure. In addition, the DPU is supplied by a power system that itself is composed of many components such as transformers, buses, and batteries. The failure of these support components will lead to the loss of power to the DPU that will fail all functions of LOCS.

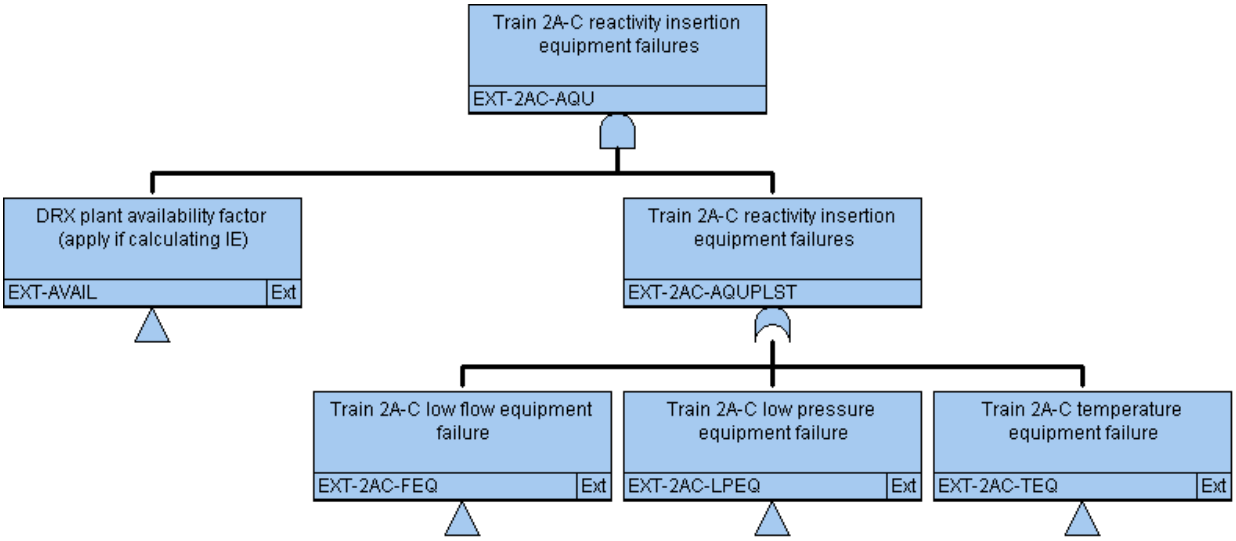


Figure 4-2 Fault tree model of failure events in loop 2A leading to reactivity insertion

Table 4-1 High level structure of the fault tree for loop 2A reactivity insertion (EXT-2AC-AQU).

Temperature Equipment Failure (EXT-2AC-TEQ)	Flow Equipment Failure (EXT-2AC-FEQ)	Pressure Equipment Failure (EXT-2AC-LPEQ)
Temperature control component failure (multiple cutsets)	Flow control component failure (multiple cutsets)	Pressure control component failure (multiple cutsets)
Insufficient secondary cooling – RFW 130 (multiple cutsets)	Loop 2A primary pumps failure (multiple cutsets)	Pressurizer heater failure
TCV-31 spuriously closes	FCV-1 spuriously closes	Loss of power to pressurizer heater (multiple cutsets)
	Flow element FE-1 plugs	
	Flow element FE-2 plugs	
	Pipe break	
	Strainer 145 plugs	

4.3.3 Modifications to the ATR PRA

Several modifications were made to the to the initial PRA model to meet the needs of the study. The following lists are the changes that were made.

<u>Changes to the RLH event tree (reactivity insertion originating from experiment loops)</u>

1. A Large LOCA (LLOCA) in the loop 2A piping can lead to a very fast reactivity insertion. The insertion can occur fast enough so that there is insufficient time for the LOCS to trip the reactor. Thus, only the PPS should be credited in the PRA analysis. Similarly, from the results of the RELAP5 runs, groups of cutsets were identified (discussed in the next section) that will lead to reactivity insertion within 3 minutes[11]. For simplicity, this study assumes that if trip must occur within 3 minutes, slow insertion will not be a valid means of reducing the reactor power (i.e., slow insertion takes more than 3 minutes, and therefore, cannot be credited in the PRA for these groups). To model these cases, the event tree modeling the experiment loop reactivity insertion event was modified. Specifically, the branch describing its consequences was broken down into three branches (Figure 4-3). Branch 1 (sequences 11 through 17) is the original branch. It represents the situation where the reactor has three mechanisms to trip, LOCS, PPS, and slow insertion. All initiating events that use this branch are assumed to cause the loop to reach the trip setpoint 3 minutes or more after the accident is initiated. Branch 2 (sequences 18 and 19) represents the LLOCA case. Here, neither the LOCS (which requires at least 0.3s to generate a trip signal) nor slow insertion is fast enough to trip the reactor in time to prevent core damage. The implicit assumption is that any LLOCA event will void the IPT, thereby generating a large positive reactivity insertion into the core and causing core damage, all within 0.3s. In this situation, only the PPS will be fast enough to trip the reactor before the core is damaged. Branch 3 (sequences 20 through 22) represents the case where both the LOCS and PPS (but not slow insertion) are fast enough to deal with the events. Events that use this branch cause the loop to reach the setpoint after 0.3s, but before 3 minutes. For all the cases, a SAPHIRE linkage rule was used to assign different cutset categories to one of the branches. Events that have multiple failure effects were assigned based on the failure effect with the earliest trip time. In generating test cases, only branches 1 and 3 were considered because only PPS can mitigate branch 2.

Table 4-2 shows the assignment of the cutset categories to branches 1 and 3 of the event tree (Figure 4-2). The categories are used in grouping failure effects in Section 4.4. Table 4-1 of Section 4.4 gives more information about each group.

Table 4-2 Assignment of cutset categories to branches 1 and 3 of the event tree.

Branch 1 (>180 s)	Branch 3 (<180 s)
Loss of heat exchanger cooling (gRFW130)	Flow control components failure – Input (gFctrlI)
Temperature control components failure – Input (gTctrlHI)	Flow control components failure – Output (gFctrlO)
Temperature control components failure – Output (gTcrlHO)	Plugging (gFlow)
	Primary pump failure (gPump)
	Pipe break (gPipe)
	Temperature control valve failure (gTcrtrlV)

[11] RELAP5 runs were made for 26 bounding cases using the upper and lower bounds for each of the 13 groups in Table 5.1-1. From these results, the earliest trip time was recorded for each group. If this time was less than 180s, then the group was assigned to Branch 3. Groups whose earliest trip time exceeded 180s were assigned to Branch 1.

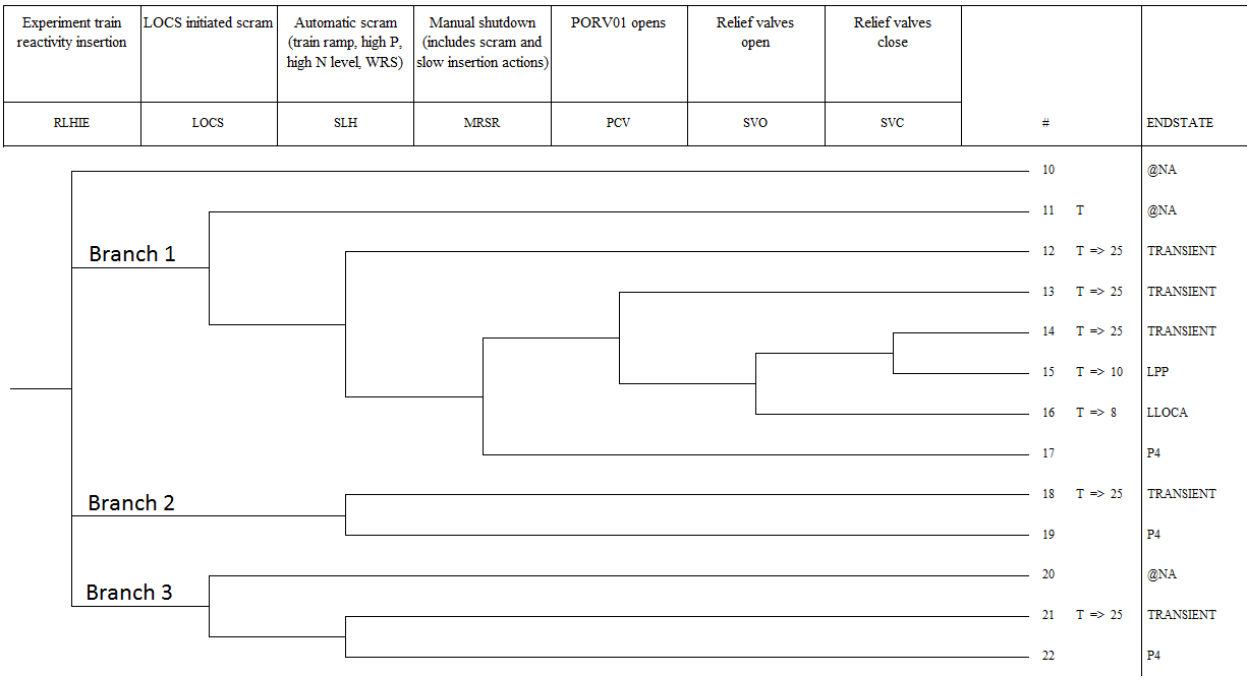


Figure 4-3 Branching of the event tree by the reactivity insertion events characteristics

Changes to the EXT-2AC-AQU fault tree (reactivity insertion originating from loop 2A)

1. In the original PRA model, every cutset of EXT-2AC-AQU has a basic event that effectively multiplies the cutset frequency by 365 to convert from a per-day basis to a per-year one. However, for cutsets containing multiple failure-to-run events, a multiplication by 365 implies that only one component needs to run for 1 year while the remaining components need to run for only 24 hours. This calculation is valid if the reactor is forced to shut down (and all component failures ceased to contribute to core damage) within 24 hours of the failure of the first component. Otherwise, the remaining components in the cutset must operate for more than 24 hours, entailing the need for additional multiplication factors. Therefore, additional 365 factors were added to account for additional exposure time beyond 24 hours. Events of the on-demand failure type (e.g., failure to start a pump) do not have the corresponding 365 factor.[12]

This change is made outside SAPHIRE 7 [Smith 2000]. For each basic event in the PRA model, manual determination was made whether an event is a mission time based (and needs the 365 factor) or probability based (does not need 365). After EXT-2AC-AQU was solved, its cutsets were extracted using SAPHIRE's MARD feature. A Python script [Jones 2001] was written that reads the cutsets, and for each basic event therein, decides whether a 365 factor is needed. The results were imported back into SAPHIRE using the MARD fault tree cutset import feature.

[12]It was conservatively assumed that a component failure will not be detected with the component repaired or replaced. Otherwise, if periodic tests are performed, then the mission time for the failure-to-run events could be shorter.

2. Common cause events (i.e., basic events so labeled in the SAPHIRE model) for analog input module and sensor failure, and sensor miscalibration events are included in the fault tree modeling the protection function of LOCS but not in the tree for the control function (EXT-2AC-AQU). To maintain consistency, these events also were added to the control function tree.

3. Analog output modules for flow, temperature, and pressure control and the DPUs were not included in the EXT-2AC-AQU fault tree for reactivity insertion. The argument for not doing so is that the system is set to use the last known good value on component failure, and this should not lead to reactivity insertion. However, with a perturbation while the control signal stuck at a steady state value, the system can be set on a trajectory away from the steady state condition that may lead to reactivity insertion in the long term. Thus, analog output modules were added to the fault tree.

4. Sensors (pressure, temperature, and flow) are critical in enabling LOCS to monitor the state of the experiment loop. However, sensors were not included in the original fault tree based on the same argument used for not including analog output modules. Therefore, based on the same counter-argument, they were added to the fault tree used in this study.

5. Distributed processing units (DPUs) are needed for the control function of LOCS. Like the analog output modules and sensors, they were not included in the original fault tree. DPUs were added into the fault tree used in this study.

6. Even though two of the analog input modules can be selected to process the sensor signals to be used for the control function of LOCS, only one input module is used at any given time [Marts 2012]. Also, there is also no automatic switching upon the failure of the module in use. Therefore, only one module should be credited (two modules were connected via an AND gate in the original model).

Changes to the EXT-2AC-CLLC fault tree (failure of loop 2A LOCS to initiate scram)

1. Digital output modules can fail in such a way that the LOCS generated trip signal is not properly transmitted, leading to failure of LOCS to trip the reactor. Therefore, the modules were added to the fault tree representing the protection function of LOCS.

2. The PRA model contains a fault tree to model a trip failure caused by the failure of the DPU watchdog to generate the trip signal. During normal conditions, the watchdog timer continuously checks that the DPU responds to its response request. If the DPU fail to respond in five seconds, the watchdog will initiate a trip signal. Since the LOCS has two DPUs for each experiment loop (an active DPU and a backup), a failure to trip from a watchdog will only occur if the currently active DPU, the DPU switchover mechanism (switching from the failed DPU to its backup), and the watchdog timer simultaneously fail. In the fault tree, this scenario is modeled as an AND gate joining the three failures. However, since there are two DPUs, there are two such AND gates. These AND gates were originally connected via another (top) AND gate. However, this top AND gate was changed to an OR gate to reflect fact that if the three failures occur, an operating backup DPU will not prevent a trip failure.

4.3.4 Quantitative PRA Results

The revised PRA model was used in generating the quantitative results summarized in this section. The SAPHIRE 7 code with a truncation limit of 10^{-15} was used unless otherwise stated.

Table 4-3 summarizes the results of PRA calculations. As described previously, we only modified the part of the PRA that is associated with Loop 2A and did not make similar changes to the similar fault trees associated with 5 other loops. Therefore, the results for the case with similar changes to other loops had to be estimated separately. The results of the PRA analysis are provided in Table 4-3. The rest of this subsection provides more discussions of the results.

Table 4-3 Summary of PRA calculations.

	Freq(reactivity accidents from experiment loops)/yr	P(LOCS failure)	CDF /yr
Total of ATR	0.97	$7.2*10^{-3}$	$2.4*10^{-6}$
Loop 2A's contribution	0.97	NA	$6.46*10^{-7}$
LOCS control function's contribution	$3.4*10^{-2}$	NA	$9.3*10^{-8}$
LOCS protection function's contribution	NA	NA	$3.03*10^{-13}$

Frequency of Reactivity Insertion Accidents

The frequency of reactivity insertion for loop 2A, calculated by solving the EXT-2AC-AQU fault tree (reactivity insertion from loop 2A), is 0.969 per year. It includes the failures of both LOCS components and that of the non-LOCS loop hardware (i.e., pipe clogging and failures of components originating from the secondary side). The frequency is dominated by the non-LOCS loop hardware failures.

As described in Section 4.3.3, the reactivity insertion events are divided into three groups. Group 1 contains events where the trip setpoint is reached after 3 minutes. Here, LOCS, PPS, and power setback can be credited for preventing core damage. Group 3 contains events where the trip setpoint is reached before 3 minutes; here, only LOCS and PPS can be credited. (Group 2 is for LLOCA and so only the PPS can be credited.) Including both LOCS failures and non-LOCS loop failures, the frequency of group 1 events is 0.8515 per year and that of group 3 events is $1.76*10^{-2}$ per year. Counting only LOCS failures[13], the annual frequency of a group 1 event is $1.64*10^{-2}$ per year and that of a group 3 is $1.76*10^{-2}$ per year. The event frequency for group 3 does not change when non-LOCS components are included because the dominant cutsets for this group are temperature sensor failure (26%), AIM failure (28%), and AOM failure (14%). By contrast, the failure of the secondary loop pump accounts for 87% of the total group 1 frequency. Excluding these non-LOCS events, the dominant cutset for group 3 becomes sensor failures (54%) and AIM failure (15%). Those cutsets of the fault tree that are associated with failures of LOCS control are 3.9% of the total frequency. The total reactivity insertion frequency caused by all 6 experiment loops is approximately 1.9 per year[14].

[13] This is done by using a Python script to remove all non-LOCS cutsets from the cutset list. The new list is then imported into SAPHIRE and the frequency re-quantified.

[14] Approximately 80% of the frequency is from cutsets involving failure of the secondary loop. These cutsets are shared among all 6 loops. Therefore, only 20% of the cutsets involve a loop-specific component such as sensors.

In this study, the first 200 dominant cutsets of the Loop 2A related reactivity accidents were used in generating test cases. The cutsets constitute 99% of the total frequency of 0.97 per year, and cover all the components of the primary cooling system of Loop 2A. Appendix A lists the 200 cutsets and describes of the basic events.

LOCS Hardware Failure Probability

A failure probability of LOCS protection functions due to hardware failures of $7.22*10^{-3}$ was obtained by solving the fault tree associated with LOCS protection failure (EXT-2AC-CLLC). The dominant cutset (42%) is a common cause DPU failure.

Total Core Damage Frequency

The modified ATR PRA was used in analyzing the risk significance of LOCS. The PRA has a total CDF of $2.40*10^{-6}$ per year given a truncation limit of 10^{-15}. This CDF value includes all initiating events (for instance, station blackout) in addition to failures in the experiment loops. The contribution of Loop 2A to the total CDF is $6.46*10^{-7}$ per year, calculated by quantifying the core damage sequences with Loop 2A causing reactivity insertion accidents. It includes the contributions from LOCS component failures (e.g., sensor failure), hardware failures of other components (e.g., pipe clog) of Loop 2A, and failures of the LOCS support system (e.g., power supply). The most dominant cutset (26%) associated with Loop 2A is strainer plugging (leading to a reactivity insertion) together with a common cause failure of the safety rod (leading to failure to trip). The safety rod failure means that all three systems that can trip the reactor (LOCS, RPS, and manual shutdown) fail to function. Thus, this is an anticipated transient without scram (ATWS) event which eventually results in core damage due to additional failures. The second most dominant cutset (6%) also is a strainer plugging but with a trip failure caused by a common cause failure of the trip division logic. (The division logic is used to transmit a trip signal to the rod clutch control system.)

The contribution of Loop 2A to the total CDF, i.e., $6.46*10^{-7}$ per year, also represents the contribution of the LOCS protection functions (including the associated non-LOCS component failures such as mechanical failures of the control rods). In these core damage sequences, the LOCS protection functions are failed (except for the large LOCA initiating event that cannot be mitigated by LOCS, and has a very small contribution to CDF of approximately 10^{-11} per year).

The preceding calculations of this subsection were done without modifying the other experiment loops. From the discussion in Section 4.3.3, it is evident that the changes made to the event tree associated with loop 2A were significant. Therefore, it is expected that if similar changes were made to the other five experiment loops, the increase would be comparable, assuming that the loops all have similar design. The overall effect then would be an increase in the total CDF, resulting in a lower percent contribution of loop 2A to it. If the same modifications were made to other loops, then the frequency of a reactivity accident would be approximately doubled, that is, 1.9 per year. It is expected that the CDF due to the 6 loops would be about twice that of Loop 2A, making the total CDF around $3*10^{-6}$ per year.

Assuming that all six loops are similar, the total frequency of reactivity insertion is approximated as 0.8*0.969+6*0.2*0.969=1.9 per year.

Contribution of LOCS's control function to total CDF

To calculate the contribution of the failures of LOCS control function to the total CDF, the failures of non-LOCS loop hardware were removed from the calculation of the contribution of loop 2A, described above, by setting their probability to zero and re-quantifying the cutset. The contribution to total CDF from loop 2A became $9.3*10^{-8}$ per year, corresponding to 4% of the baseline total CDF of $2.40*10^{-6}$ per year. Here, the dominant cutset (21%) is a failure of the temperature sensor together with common cause failure of a safety rod group. The next three dominant cutsets (11% each) involve the failure of the various analog input and output modules together with the common cause failure of the safety rod group.

The contribution to total CDF of failures of non-LOCS loop 2A hardware (e.g. pipe breaks, plugging) and LOCS failure from failure of the supporting system, assuming that the LOCS hardware is perfect, is $5.53*10^{-7}$ per year. The top two dominant cutsets here are the same as those in the second case described above (i.e., loop 2A contribution, including both loop 2A events and LOCS). By itself, the LOCS supporting system (i.e., power supply to the LOCS RPU) contributes $3.60*10^{-10}$ per year to the total CDF. The dominant cutset here is the failure of a transformer (leading to the loss of LOCS RPU) together with a common cause failure in the safety rod group.

Contribution of LOCS's protection function to total CDF

The LOCS protection functions always are backed up by the PPS making their contribution to the total CDF very small (~10^{-4} %)[15].

4.4 Risk-Informed Considerations

One benefit of risk-informed considerations is that overly conservative requirements or goals may be identified and relaxed. Section 5.3 of NUREG/CR-7044 [Chu 2013] provides some background discussion of risk-informed considerations for digital systems. In this study, risk-informed consideration is used to demonstrate that a reliability goal of 10^{-4} [INL 2008] is not needed to demonstrate the acceptability of the software of the loop operating control system (LOCS) of the Advanced Test Reactor (ATR), subject to limitations on the quality and scope of the probabilistic risk assessment (PRA).

RG 1.174 [NRC 2011] describes an acceptable method for the licensee and the NRC staff to use in assessing the nature and impact of licensing basis changes when the licensee chooses to support, or is requested to do so by the staff, the changes with risk information. Figure 4 of this regulatory guide specifies the risk-acceptance guidelines based on the CDF. Regions are established by a measure of the baseline risk metric, viz., the core damage frequency (CDF) along the x-axis, and the change in the metrics (ΔCDF) along the y-axis. The different regions of the acceptance guidelines require different depths of analysis; acceptance guidelines are established for each region.

[15] This is calculated by taking the difference of the frequency between the total loop 2A-initated core damage cutsets and the same cutsets but removing those involving LOCS protection failure.

Section 2.5 of RG 1.174 provides guidance on comparing the PRA results with the acceptance guidelines. In particular, for Region III in Figure 4, it is arguable that if the calculated value of ΔCDF is very small, a detailed quantitative assessment of the baseline value of the CDF and the large early release frequency (LERF) is unnecessary. The guidance is applied to the software of the LOCS as detailed in the next paragraph.

Based on the PRA analysis of the ATR PRA of Section 4.3, the CDF from internal events is approximately $3*10^{-6}$ per year, and the contribution of the protection functions of the LOCS is less than 10^{-4}%. In addition, the probability of hardware failure of the LOCS protection functions was estimated to be $7.22*10^{-3}$. If the probability of software failure, which is not modeled in the PRA, is the same as that of the hardware failure, then it would make very small contribution to the total CDF (i.e., less than 10^{-4}%). Therefore, a reliability goal of $7.22*10^{-3}$ should be adequate. As calculated in Section 7, the results of one failure in 10,000 tests more than suffice to demonstrate the acceptance of the software of the LOCS. In addition, the PRA analysis of a hardware failure probability of $7.22*10^{-3}$ for the LOCS is good enough.

4.5 Assumptions and Limitations of the Application

The key assumptions and limitations in using the ATR PRA are summarized below. They mainly concern the realism of the PRA model and the RELAP5 model, and are not limitations of the method.

1. BNL does not have the documentation for the ATR PRA, which is proprietary, nor the design information needed to undertake a detailed review of it. Thus, BNL worked with the SAPHIRE7 model and concentrated on that part of it related to the LOCS. A few conference calls were held with INL's staff who are familiar with the PRA and RELAP5 model to resolve some questions BNL had. Thereafter, BNL made some changes based on BNL's understanding of the system and the reactor. The most significant one is the success criteria associated with those systems that can be used to generate a reactor trip signal. In particular, the strainer plugging model is an important reason for the large increase in CDF resulting from the changes.

2. BNL did not change the modeling of other experiment loops that were modeled in the same way in the PRA. Approximations were used in estimating the effects if the loops had been modified.

3. The PRA assumes that the LOCS designed to protect the experiment also can mitigate reactivity insertion accidents. That is, the LOCS trip set points selected for protecting the experiment also are effective in mitigating reactivity insertion accidents.

4. The PRA assumes that any failure of the modeled protection functions would cause a failure to trip. Therefore, some CDF cutsets may include a reactivity insertion event with failure of an irrelevant protection function of the LOCS. On the contrary for each reactivity insertion accident, there may be more than one protection function that would generate a trip signal. In this study the simulation of the test cases was terminated after the generation of the first trip signal.

5. The basic events and cutsets were grouped according to their failure effects mainly because of the limitations of the RELAP5 model in simulating those effects. That is, more realistic failure effects could have been used if the RELAP5 model had been improved further.

6. Development of 13 probabilistic failure models was necessary to capture the variability of the failure effects by characterizing them in terms of parameters with uncertainties. The choice of parameters and their probabilistic distributions can be improved by performing engineering analyses and possibly collecting data on the effects of failure.

7. BNL used the first 200 cutsets of the fault tree for reactivity insertion accidents involving Loop 2A. The cutsets contributed 99% to the top event frequency and covered all primary components modeled in the RELAP5 model. In general, the approach can be extended to a larger number of cutsets that may contain more challenging conditions to the LOCS.

5. USING THE RELAP5 MODEL TO GENERATE TEST CASES

This section describes how the RELAP5 [NRC 1995] model of Loop 2A was developed and used to generate the test cases for the LOCS. The RELAP5 model provided by Idaho National Laboratory (INL) was improved to meet the needs of this study to simulate the PRA scenarios and their associated variations (e.g. LOCA sizes and locations). The INL model was used at INL only to simulate a large loss of coolant accident (LOCA); thus, it lacks the detailed models of the loop components that are necessary to fully analyze the operational contexts defined by the probabilistic risk assessment (PRA) model. For example, the secondary side that supplies cooling to the loop through a heat exchanger was omitted despite the secondary side problems being the dominant contributors to the reactivity insertion scenarios to be simulated with the RELAP5 model. Brookhaven National Laboratory (BNL) did not have the required detailed design information to modify the RELAP5 model, and so had to make some modifications, using assumed parameters, to make it more realistic and also to approximately simulate the scenarios using this modified version. In, addition, the cutsets from the ATR PRA do not specify exact how the failures would affect the physical condition of Loop 2A. We developed probabilistic failure models that are used in specifying the exact failure effects and their possible variations.

Section 5.1 describes the RELAP5 model obtained from INL and the changes that BNL made to the RELAP5 model to facilitate simulation of the PRA scenarios. Section 5.2 describes how failure events defined in the PRA are simulated and how they can be grouped into a few groups based on their failure effects. It also describes how probabilistic failure models are used in modeling variations of the scenarios. Section 5.3 summarizes the key assumptions and limitations of the RELAP5 simulation.

Section 6 describes how test cases are sampled from reactivity insertion cutsets generated in Section 4.3 and how the RELAP5 input decks were automatically prepared for each of the test cases. The outputs of the RELAP5 runs then were used as input to tests of the LOCS described in Section 7.

5.1 RELAP5 Model of Experimental Loop 2A

This section describes the original RELAP5 [NRC 1995] model as provided by INL for use in the project, the changes that were made by BNL to partially improve the model, and the limitations of the resulting model.

The RELAP5 model of the pressurized water loop 2A includes both the in-pile tube (IPT) located in the reactor core and out-of-pile (located outside the core) facility. The model includes some of the control variables representing safety-related signals used by the loop operating control system (LOCS) and includes the associated reactor trips with scram set points. The signals include the measured loop coolant temperature, pressure, and flow rate. Additional control variables representing the control functions of the LOCS are also included. The trips represent reactor scram points for low and high temperature, low pressure, and low flow rate. The RELAP5 nodalization of the out-of-pile loop piping is shown in Figure 5-1. The IPT is modeled as a long annulus and is not shown in the figure. The RELAP5 model of the reactor primary side itself is not available to BNL and is modeled as a constant heat source to the IPT. This heat source represents gamma heating of the IPT components and moderator heating from neutrons. Hydraulics components (e.g., piping) for the primary side are not modeled which means that any feedback from the experimental loop to the primary loop cannot be represented.

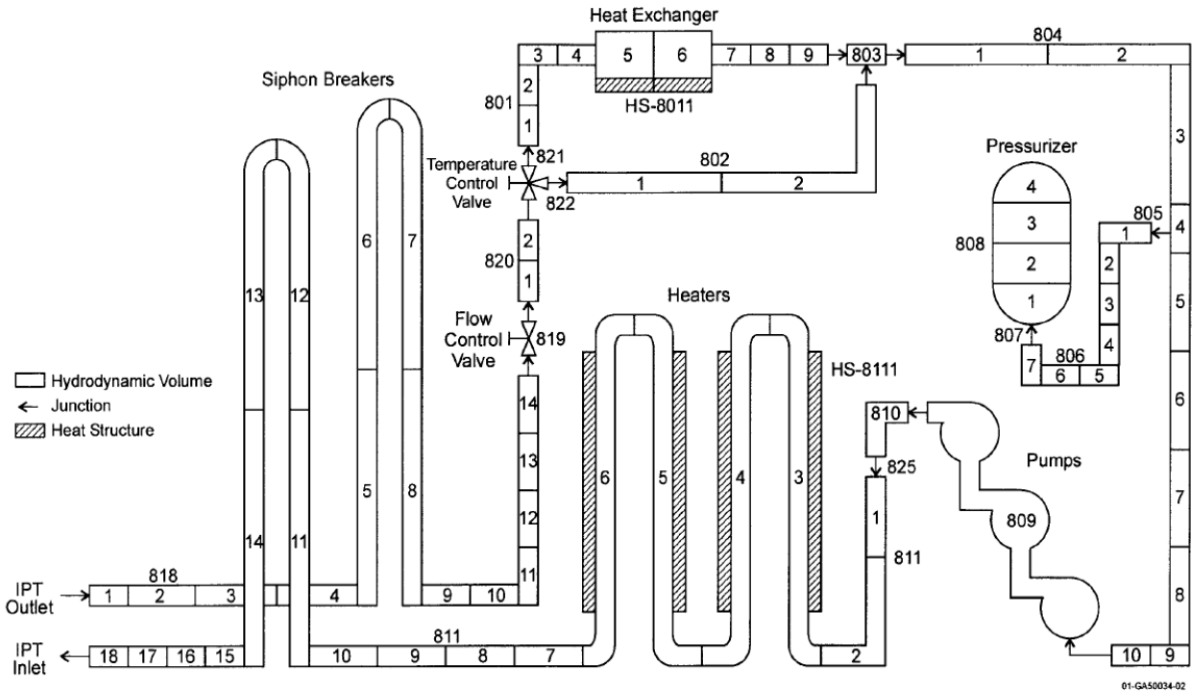


Figure 5-1 RELAP5 nodalization of the original model for the out-of-pile loop piping.

The RELAP5 model of Loop 2A was originally used by INL to simulate a large loss of coolant accident (LOCA) in the loop and was not designed for generating test cases for statistical testing. For a large LOCA, the accident progresses rapidly so the control systems do not have time to react. This means that control systems do not have to be modeled for the model to accurately predict the post-accident behavior. However, for slower transients as is the case for many of the reactivity insertions events modeled in the PRA, it is important for the control systems to be present since these systems will try to correct any deviations from steady state. Therefore, the model as obtained from INL was enhanced to address these limitations. Specifically, the original RELAP5 model misses the following control functions:

1. Coolant pressure control. In addition, both pressurizer heater and pressurizer spray are not modeled,

2. Pressurizer level control,

3.Loop 2A has two methods of temperature control: line heater and temperature control valve (which controls the heat exchanger bypass fraction). The RELAP5 model has a line heater control system but the temperature control valve only provides constant mass flow.

4. Other control functions such as loop degassing flow control, ion exchange flow control, and makeup system storage tank level control.

The model contains trip function for coolant temperature at the IPT inlet and outlet, IPT inlet coolant flow rate, and IPT inlet coolant pressure. The test specimen temperature and IPT coolant temperature delta-T are not modeled.

In addition to the control functions above, the secondary side (of the heat exchanger) is simply modeled with a constant temperature boundary condition and the reactor primary loop is only modeled in a very simplified way as described earlier.

Because the RELAP model is being used for a different purpose than initially intended, additional control functions were added to better model control system failures that are important for this study.

Specific enhancements include the following::

1. An additional cell was added to the top of the pressurizer. The pressurizer in the original model is composed of three nodes (component 808 in Figure 5-1) and all are filled with water during stead state and has no room for steam. During a transient run, the original model adds additional node containing steam to the pressurizer. To avoid having to modify the pressurizer for each transient run, the model was changed to that three additional nodes were added to component 808 in the steady state input deck. These nodes contain gas (steam) to allow for water expansion.

2. Scaling factors of a control variable that evaluates the amount of heat transferred from the IPT to the reactor were adjusted to make them consistent with the heights of the hydrodynamic nodes.

3. Reactor scram logic was added to the main input deck so it does not have to be added to the transient deck for transient runs. This improves the efficiency of the model for generating test cases for the STM.

4. Control variables were added to output both the engineering unit and electric current (mA) unit of the pump inlet pressure. These outputs were requested by INL for their simulation runs.

5. A control logic system was added to terminate the transient runs 30 seconds after any trip signal.

6. A valve and a time-dependent volume were added at two locations (at the outlet of the pump and at the inlet of the flow control valve) to simulate small break loss-of-coolant accidents (SBLOCA).

7. To simulate pipe plugging, PIPE components were modified by adding a single-junction at three locations (at the IPT inlet and outlet and at the strainer. Pipe plugging was simulated by reducing the flow area of a specific single junction during a transient run.

8. In order to facilitate some sensitivity calculations, a control logic was developed to terminate transient runs to avoid running transient cases for a very long time. This control logic stops RELAP5 running 1800 seconds after an important variable changes by 10% from its initial value and a reactor scram signal is not generated.

9. RELAP5 trip systems were developed to initiate transient events.

The modifications above do not attempt to add control functions for the loop pressure and the temperature control valves. In addition, components for the secondary loop were not added. The main reason is that BNL does not have detailed design information that will be needed to model these components and control functions, so including them into the model will involve assumptions that may not reflect the actual system.

Modeling loop 2A without the appropriate control functions means that any possible interaction between the different functions will not be accurately predicted. For any one accident scenario, more than one control function[16] may respond to compensate the deviation from steady state. For example, an accident leading to low flow will most likely see the flow control function opening the flow control valve in an attempt to increase flow. If the low flow situation also leads to a pressure increase, then the pressure control function will also respond. The simultaneous responses from these two control functions may take the system in a trajectory that is different from the one the system will take if only one control function responds. In this way, the lack of the pressure control function in the model limits the range of scenario that the model will accurately predict the system behavior.

In addition to the limitation of the control functions, the lack of secondary side modeling further restricts the type of scenario that the model can represent. A majority of the cutsets of events leading to reactivity insertion from loop 2A events are events involving failure of secondary side components (e.g., secondary flow control failure, secondary coolant pump failure, and loss of secondary inventory). The exact trajectory of the primary loop state will vary with the type of secondary failure. Specifically, the rate of temperature increase of the primary coolant differs for different scenarios involving secondary components. However, the use of a boundary temperature to represent the secondary side means that all scenarios have to be approximated using this representation. For example, the scenario where there is a pipe break in the secondary side loop is expected to evolve differently than the case where a secondary pump fails. Yet, the lack of secondary side representation means that these two scenarios are both modeled through boundary heat transfer coefficient changes. It is difficult to judge how much error the approximation introduces without knowledge of the construction of the secondary loop and without studies using models that do include these components.

Similarly, the absence of the reactor primary loop in the model makes it difficult to judge the severity of the different scenarios. For example, it is not clear how much flow will need to be reduced for the reactor to see a reactivity insertion. For this project, it is assumed for simplicity that any scenario leading to voiding in the IPT will introduce enough reactivity for LOCS to not be able to react in time to trip the reactor. It is also assumed the trip setpoint contained in the RELAP5 model and used in the LOCS logic was determined taking into consideration the LOCS's cycle time such that LOCS is capable to generate a trip signal in time.

The assumptions described in the preceding paragraphs were used in the following ways. They are associated with determining if the LOCS can be used to mitigate different reactivity insertion

[16] A control system refers to one of the flow, temperature, or pressure control system. Being part of LOCS, these systems share some common component such as the DPU but also contain distinct component such as the sensors.

scenarios. Only those scenarios that the LOCS can mitigate were used in the simulation with the results defining the test cases to be performed.

1. For each scenario, if a trip setpoint is reached in at least 0.3s after the start of the reactivity insertion event, then LOCS is credited. (According to discussion with INL, LOCS needs at least 0.3s to process a trip signal.) Scenarios in this group were simulated.

2. For a SBLOCA case, if a scenario occurs where the setpoint is reached before 0.3s after the initiating event, then voiding of the IPT is checked. If no voiding occurs (void fraction < 10%), then it is assumed that no significant reactivity insertion occurred so that LOCS is allowed to trip at or after 0.3s. Scenarios in this group were simulated.

3. If a SBLOCA case occurs where the setpoint is reached before 0.3s and voiding of the IPT occurs within that 0.3s, then LOCS cannot be credited with preventing core damage. Scenarios in this group are not simulated.[17]

5.2 Modeling of Reactivity Insertion Cutsets with RELAP5

There are a few issues associated with modeling of the PRA-defined reactivity insertion scenarios (cutsets) using the RELAP5 model. They are discussed in Section 5.2.1 along with how the issues were addressed in this study. Section 5.2.2 describes the 13 failure effect categories and their associated probabilistic failure models.

5.2.1 Issues Associated with Modeling of PRA-Defined Reactivity Insertions

Modeling of PRA Failed Components that are not in the RELAP5 Model

The original RELAP5 model of experiment loop 2A does not support the direct modeling of many component failures that appeared in the cutsets. For them, alternate means of modeling were needed, based on the knowledge of the roles that these components play in the system. The approach used in this study was to include failure events with similar effects on the system in groups that could be modeled generically. This section discusses how these groups, briefly mentioned in Section 4.4, were constructed. Using these groupings allowed simulations of the failures of components that were not explicitly included in the RELAP5 model by failing other components that were modeled. As an example, the following paragraphs describe how failure of pressure control was modeled using the RELAP5 model. Other component failures that are not explicitly modeled in the RELAP5 model were simulated similarly. Thirteen groups/categories of failure effects were developed and represented by 13 probabilistic failure models of the failure events; they are described in Section 5.2.2.

The lack of control systems for the loop pressure in the RELAP5 model precludes the direct modeling of cutsets involving the failure of the pressure control component (e.g., loss of pressure sensor). For pressure sensors, the failure mode that leads to reactivity insertion is the one where the sensor gives a false high reading (i.e., fail high) when the actual pressure in the

[17] In the PRA model, it is assumed that the LOCS is capable of mitigating a SBLOCA. In reality, this type of SBLOCA occurs too quickly for the LOCS to be effective and should be treated as a large LOCA in the PRA.

loop is low. This scenario will leave the initial low pressure uncorrected and may prompt the pressure control system to reduce it further. Since loop 2A is a pressurized loop that can operate at temperatures well above the boiling temperature at atmospheric pressure, depressurizing it may lead to voiding at the IPT. This, in turn, causes a reactivity insertion due to positive void coefficient of the reactor. Therefore, it is important to find a method to simulate the pressure control system in the RELAP5 model to enable it to analyze scenarios involving the failure of pressure control components.

One way to model a pressure sensor failure in its absence in the model is to introduce a pressure drop into the loop and disable any mechanism that may try to compensate for the pressure drop. In the RELAP5 model, since the pressure control system is not modeled, it is sufficient to only initiate a pressure drop that is initiated by introducing a randomly sized pipe break (to simulate a random rate of pressure decrease) at a pre-specified location. Notably, this method of approximating the effect of failure of a pressure sensor means that modeling this failure scenario and one of a small pipe break in the loop are identical. Accordingly, both the failure of the pressure sensor and the pipe break belong to the same group even though at first glance, the two are very different.

Mapping PRA Failure Events to the RELAP5 Model

A PRA model typically only specifies a general failure mode of a component, for example, a pump may have a failure mode called “pump fails to continue running”. In some cases, a failure mode may be simply “the component failed”. Once a component failure event has been selected to be simulated in the RELAP5 model, it is necessary to specify how exactly the component fails in the model. For example, if a valve spuriously closes, the position of the valve (which determines the flow area through it) as a function of time must be specified. In general, the flow area may vary, representing different possible scenarios to be simulated. For example, a fully opened valve may spuriously close to a half-open position in one scenario and to a fully closed position in another. Therefore, a random variable representing the flow area is suitable for modeling the valve closure event, and each time this event is simulated, a sample from the random variable is taken. (In the RELAP5 model, the valve area is not changed directly but via a control variable whose value is proportional to the valve area.) In this study, thirteen categories of failure events were developed and a uniform distribution is assumed for the random parameters used in defining the random variables. Engineering considerations and judgment were used in assessing the parameters. Each category is characterized by a probabilistic failure model of the failure events. Examples of the random parameters are time to close, pump stop time, and flow plugging fraction. The assessments of the random parameters for each category are discussed in Section 5.2.2.

PRA Cutsets May Include Failures with Multiple Failure Effects

In the PRA model of the reactivity insertion events, some of the cutsets may contain failure of components of support system that may cause a failure of multiple control functions, each with a different effect on thermal hydraulic condition of the loop. Then, the failure effects of the failed components will include more than one category of the 13 categories. The multiple failure categories were applied in the RELAP5 model in simulating the cutsets.

5.2.2 Categories of Failure Effects and Their Associated Probabilistic Failure Models

In this section, these 13 categories of failure effects and their associated probabilistic failure models are detailed. Table 5-1 shows the 13 categories. Appendix A provides a mapping of the 200 reactivity insertion cutsets used to study the category or categories of failure effects.

Note that some of the following groups contain subgroups specifying how a component fails (i.e., if a pump fail in a “trip” mode so that it coasts down normally or in a “seizure” mode so that it suddenly stops spinning). Each individual failure mode should associate with a unique subgroup. Depending on the specified failure mode in the PRA model, a particular subgroup should be used to model it. If a failure mode does not specify a subgroup, then when sampling from its associated group a subgroup was selected randomly from the possible subgroups, for example, in the case of a pipe break, two subgroups representing pipe break at two different locations are assumed to be equally likely.

(1) Loss of Heat Exchanger Cooling

A majority of the cutsets for reactivity insertion involved failures that cause a loss of heat exchanger cooling (i.e., loss of heat transfer to secondary loop) for the loop 2A heat exchanger. These cutsets account for approximately 80% of the total loop 2A annual reactivity insertion frequency. The heat exchanger is the primary means by which loop 2A cools, and its loss eventually leads to an increase in the coolant temperature. A variety of failures can cause the loss of cooling. For example, the secondary loop may have lost its makeup water, the secondary pump may have failed, the flow control valve of the secondary side may have failed close, or the control system responsible for secondary flow may have failed.

Since the RELAP5 model does not model the secondary side, it is impossible to directly represent these secondary side component failures. Instead, modifications to the existing parameters were made to approximate them. For this study, it was decided that the appropriate approximation was to decrease to zero the heat transfer coefficient (HTC) between the primary and secondary sides. This decrease is not a jump drop but, rather, is a linear decrease from the initial steady state value to zero over some period. The time over which the decrease occurs is a random number within a certain interval (see Tables 5-1 and Table 5-2). This randomness of the time to reach zero was intended to simulate the different effects that the different secondary side components exert when they fail. The lower bound of zero on the random number means a simultaneous termination of heat transfer to the secondary and represents events such as large pipe break in the secondary loop. The upper bound was chosen so that the trip setpoint would be reached within 30 minutes of the start of the transient and was determined from RELAP5 sensitivity calculations. For all cutset groups used for this project, 30 minutes was the maximum time for which the cases were analyzed; events leading to a trip setpoint after 30 minutes were not considered.

(2) and (3) Pump Failure

Cutsets that result in the stoppage of the loop 2A pumps were assigned to the pump failure group. These cutsets further were placed in one of two subgroups (i.e., the Trip and Seizure subgroups), depending on how they affect the pumps. An event such as a loss of power will lead to a different behavior of the pump than does a stuck pump shaft. The Trip subgroup of the pump failure group represents events that cause the pump to stop gradually. In RELAP5, the pump was allowed to coast down from its initial rotation frequency to zero, following its natural coast down curve. To simulate the variation in the trip coast down curve, randomness was introduced by multiplying the curve by a random number.

By contrast, the Seizure subgroup represents events that cause the pump to come to a sudden stop. It was modeled by assigning a linear coastdown curve to the pump. Here, the variation in the pump coastdown behavior was simulated by varying the slope of the coastdown function. The linear coastdown function starts at the pump initial velocity and reaches zero at a random time between t=0 (instant drop), and an upper bound. This upper bound was determined by drawing a line starting at the pump initial velocity at t=0 and, using a slope calculated from using the t=0 s and t=1 s data of the original coastdown curve, determining the time axis-intercept. The probability of the trip and of the seizure subgroups is 49% and 51%, respectively. The PRA model does not specify the failure modes of these subgroups so their frequency is assumed to be similar.

(4)-(6) Pipe Plugging

In the PRA model, there are three locations in loop 2A where flow may be plugged: flow element 1 (FE1), flow element 2 (FE2), and strainer 145 (S145). For all three, the plug was modeled in RELAP5 by inserting a single-junction at the plug location and reducing the flow area of this single-junction. The final area of the junctions (i.e., the flow area after the plugging) is a random number ranging between zero (complete plug) and an upper limit, chosen so that the flow rate remains below the trip setpoint for longer than 1 second. For flow area above this upper limit (i.e., for plugging that is less severe than this limit), the RELAP5 simulation predicted that the system would reach a new steady state that will not cause a trip. In some cases, the flow rate as calculated from RELAP5 oscillations near the trip setpoint and it does not stay below the setpoint for more than 1 s. These cases were excluded by setting the upper limit as described here. The lower limit of the flow area is 0, corresponding to complete plugging.

(7) and (8) Pipe Break

In the PRA model, there is only one pipe break event. However, based on physical considerations, its impact is expected to differ depending on the break location. Therefore, two locations were considered: at the IPT inlet, and at the IPT outlet. For simplicity, the probability that the break occurs at either location was assumed to be identical (i.e., 50% probability that the break occurs at the IPT inlet, and 50% probability that it occurs at the IPT outlet). The break was modeled by adding a valve at the location with a valve that is normally closed in the other transient runs. The valve is opened to initiate the break. The random parameter is the valve flow area, representing the size of the break. The lower limit for the parameter (i.e., break size) was chosen so that, based on the RELAP5 sensitivity study, a trip signal is generated within 30 minutes of the start of the break. The upper limit to the break is the largest break size such that voiding in the IPT occurs at least 0.3 s after the start. Note that for break size near the upper limit, the low pressure trip setpoint is reached before 0.3 s. However, LOCS still can be credited for generating a trip provided that IPT voiding does not occur.

(9) Loss of Flow Control-Input

Events that were assigned to this group are those that affect the input to the LOCS flow controller that include failure of the flow sensor failure and of the analog input module (AIM). The PRA model does not specify the mode of failure for these components. Therefore, it was assumed here that the failure mode is the one leading to the most severe consequence. Flow sensors were assumed to fail high, causing the controller to (incorrectly) reduce the flow rate. The lower rate eventually will cause high temperature in the loop, and if a high-temperature trip

does not occur, eventually to boiling in the IPT. IPT voiding causes reactivity insertion due to the positive void coefficient. Similarly, the AIM was assumed to fail by generating a false low flow output.

All cutsets in the "loss of flow control-input" group were modeled in RELAP5 by modifying control variable 240 (CV-240). CV-240 normally takes as input the mass flow rate and processes it to generate an output variable that determines the position (i.e., flow area) of the flow control valve. To simulate events in the group, the input connection from the mass flow rate to CV-240 was removed and replaced by a random number to directly set the value of CV-240. This random number lies in a range that ensures that the trip setpoint occurs within 30 minutes and that the RELAP5 case does not fail (the model was built such that RELAP5 would fail if the valve flow area was near 0).

(10) Loss of Flow Control-Output

Cutsets assigned to this group are those that affect the output of the LOCS flow controller. They include the LOCS DPU and digital output modules (DOM). Like the case of the "loss of flow control-input" group, the PRA model does not specify the exact ways the component fails. They were assumed to fail in a way that causes the most severe consequence. Both the DOM and DPU were considered as failing by incorrectly instructing the flow control valve to close. Events in the group are modeled in RELAP5 by directly modifying CV-24. This control variable is part of the mechanism by which the flow controller determines the flow area of the flow control valve (FCV) based on the value of CV-240. By setting CV-24 to a random number, the position of the flow control valve no longer responds to the actual flow rate. The random number was selected from a range determined so that the trip setpoint is reached rather than the model reaching a new steady state above the setpoint. One cutset in the PRA involves the FCV spuriously closing. This cutset also was assigned to this group since its effect is the closing of the FCV, same as the other cutsets in this group.

(11) Loss of Line Heater Control-Input

This group is similar to the "loss of flow control-input" group but with the line heater controller instead of the flow controller. Events in this group were modeled in RELAP5 by modifying CV-1 that normally takes as input the signal from a temperature sensor. Setting CV-1 to a random number simulates the failure of the input portion of the line heater controller. The interval from which the random number is drawn was determined based on sensitivity analysis so that the trip setpoint is reached within 30 minutes.

(12) Loss of Line Heater Control-Output

This group is similar to the "loss of flow control-output" group but with the line heater controller instead of the flow controller. Events in this group were modeled in RELAP5 by modifying CV-4. The line heater directly reads the value of CV-4 and adjusts the heater power accordingly. To simulate the output portion of the line heater controller, CV-4 was directly modified by setting it to a random number, drawn from the interval based on sensitivity analysis such that the trip setpoint is reached within 30 minutes.

(13) Loss of TCV control

There are two temperature control mechanisms in LOCS: adjustment of the line heater power and the TCV. The latter controls the ratio of flow that bypasses the heat exchanger. Cutsets in this group are those that lead to the loss of temperature control via problems with the temperature control valve (TCV). Examples include the TCV spuriously closing and the loss of DPU. These cutsets were modeled by completely closing the TCV with various times to full closure. The time to close was a random number drawn from the interval determined from the valve closing time, based on engineering judgment.

Several assumptions were made about the operation of the LOCS that directly determined the choice of the range used in sampling:

1. LOCS has a 0.3 s cycle time. Thus, the longest delay between the time that the trip demand occurs (threshold is exceeded) and the time that trip signal is generated is 0.3 s. The nonzero lower limit on the delay implies that the LOCS protection system cannot mitigate any accident scenario that needs a trip to occur faster than 0.3 s (as determined from RELAP5 sensitivity analysis). Assuming this, the range for the parameter (e.g., upper limit for the pipe break size) was determined so that all test cases generated do not require a trip before 0.3 s.

2. After the occurrence of an event, it was assumed that the operator would initiate mitigation actions to terminate the reactivity insertion no later than 30 minutes after the event occurs. This assumption limits how long the simulation with RELAP5 will last, and thus, the range for the parameter. For example, this assumption led to a lower limit for the size of the pipe break; for sizes below it, no trip demand will be generated within 30 minutes of the break.

Table 5-1 lists the ranges of the uniform distributions for all the cutset groups as determined from sensitivity study runs. These runs basically used the two assumptions above to determine the appropriate limits for the parameters. Within these limits, a uniform sampling was made to select the value of the parameter to be used in a single run. As an example, for the cutsets involving the loss of heat exchanger cooling, the model was constructed by decreasing the heat transfer coefficient from the steady state value to zero over a period between 0 and 1670 s. During the generation of the RELAP5 input case, a random number between 0 and 1670 also was obtained. This number then represented the time over which the heat transfer coefficient would drop to zero. During the simulation, if the loss of the heat exchanger cooling group was selected again, then another random number between 0 and 1670 would be used. As Table 5-2 shows, the upper limit of 1670 s was obtained by the sensitivity study as the largest number that could be used and still have a trip demand generated within 30 minutes. If the heat transfer coefficient takes longer than 1670 s to drop to zero, then a trip signal will not be generated within 30 minutes, and by assumption 2, the operator will have noticed the problem and corrected it.

Table 5-1 Bounds for probabilistic modeling of cutset groups.

No.	Cutset Group Description	Subgroup [Frequency of Subgroup]	Parameter	Lower Bound	Upper Bound
1	Loss of HX cooling	-	Time at which heat transfer coefficient reaches zero. [s]	0	1670
2	Pump Failure	Trip [49%]	Multiplication constant to the time variable for pump coastdown curve	0.5	1.5
3		Seizure [51%]	Time for pump to reach	0.001	2.04

			complete stop [s]		
4	Pipe Plugging[18]	Plugging at FE1 [33.3%]	Flow area at junction 855 [ft^2]	1.00E-08	6.3580E-04
5		Plugging at FE2 [33.3%]	Flow area at junction 856 [ft^2]	1.00E-08	6.5630E-04
6		Plugging at S145 [33.4%]	Flow area at junction 857 [ft^2]	1.00E-08	6.3580E-04
7	Pipe Break	Break at IPT Inlet [50%]	Flow area at valve 851 [ft^2]	6.3840E-06	7.5100E-04
8		Break at IPT Outlet [50%]	Flow area at valve 853 [ft^2]	6.1500E-06	9.4300E-04
9	Loss of flow control - input	-	CV-240 (Flow sensor input) [gpm]	30.06	35.1
10	Loss of flow control - output	-	CV-24 (Flow controller output)	0	0.382423
11	Loss of line heater control – input	-	CV-1 (Temperature sensor input) [^oF]	45	490
12	Loss of line heater control – output	-	CV-4 (Line heater controller output)	1.799637E +05	2.16E+05
13	Loss of TCV control	-	Time for valve TCV-3-1 to be fully closed. [s]	15	45

[18]Based on the PRA model, plugging at strainer 145 accounts for about 97.3% of all plugging cases. Plugging at flow elements 1 and 2 account for about 1.35% each. For the simulation, we assumed that plugging at all three locations can occur with equal probability.

Table 5-2 Justification of bounds for probabilistic modeling of cutset groups.

No.	Variable	Rationale for Lower Limit	Rationale for Upper Limit	Trip reason
1	Time at which heat-transfer coefficient reaches zero. [s]	Instantaneous termination of heat transfer	Trip signal generated within 30 minutes	High-temperature at IPT inlet
2	Multiplication constant to the time variable for pump coastdown curve	Engineering judgment	Engineering judgment	Low mass flow rate at IPT inlet
3	Time for pump to reach complete stop [s]	Instantaneous drop	Time axis intercept assuming linear drop with slope calculated using t=0 s and t=1 s data	Low mass flow rate at IPT inlet
4,5,6	Flow Area [ft^2]	Complete plugging	Flow rate remains below trip setpoint for $\geq$ 1 second	Low mass flow rate at IPT inlet
7,8	Break size [ft^2]	Trip signal generated within 30 minutes	Maximum break size such that voiding in IPT occurs after 0.3s	Low pressure at IPT inlet
9	CV-240 (Flow controller input)	Trip signal generated within 30 minutes	Largest flow area that RELAP5 runs without failure	High temperature at IPT outlet
10	CV-24 (Flow controller output)	Fully closed	Trip setpoint is reached instead of new steady state	Low mass flow rate at IPT inlet
11	CV-1 (Line heater controller input)	Trip signal generated within 30 minutes	Maximum allowable temperature difference between IPT inlet temperature and reference temperature of 490 K	High temperature at IPT outlet
12	CV-4 (Line heater controller output)	Trip signal generated within 30 minutes	Maximum heater power	High temperature at IPT outlet
13	Time for valve TCV-3-1 to be fully closed. [s]	Engineering judgment	Engineering judgment	High temperature at IPT inlet

5.3 Simplifications, Assumptions, and Limitations of the RELAP5 Simulation

The purpose of the RELAP5 simulation is to realistically simulate the reactivity insertion accident conditions under which LOCS operates. Such accident scenarios are identified by the PRA and further characterized by the probabilistic failure models that capture the potential variability of the scenarios. Each RELAP5 run can be used to generate the inputs of LOCS test cases. This is a part of the characterization of operational profiles described in Section 2.8 where some wider-scope limitations associated with the characterization are discussed. This section summarizes the simplifications and assumptions that were adopted in the RELAP5 simulation.

1. RELAP5 model limitations

The RELAP5 model that INL developed was originally used to simulate short duration reactivity insertion events. Because this project used the original RELAP5 model for a different purpose, some modeling needed to fully represent that the PRA context was not modeled, or was modeled in a simplified way. For example, the secondary side that provides cooling to the loop is modeled only in terms of the heat transfer coefficient at the heat exchanger. On the other hand, the failure events identified in the PRA may be much slower than short duration reactivity insertion events, and some involve failure of specific components on the secondary side. Hence, BNL approximated the failures by varying the heat transfer coefficient. In some cases, BNL had to modify the RELAP5 model with assumed parameters so that some specific failures could be more realistically modeled. For example, BNL added a steam volume to the pressurizer model, and also made some modifications, such that some failure events can be modeled. For example, a valve was added to simulate a LOCA at a specific location.

An interesting issue is associated with the fact that the system under test, LOCS, also performs control functions that could be included in the RELAP5. Including these control functions improves the ability to more realistically characterize the operational context. However, some of these control functions were modeled in a simplified manner. It should be noted that these simplifications can introduce inaccuracy in simulating accident scenarios in which the control functions attempt to maintain the loop in a steady state condition. Additionally, as described in Section 3.4, LOCS performs several protection functions. In order to prevent the actuation of a protection function from interfering with the characterization of the testing operational profile, the LOCS protective functions in the original RELAP5 model were turned off.

In summary, a RELAP5 model that was initially developed to support specific safety analysis reviews can be adapted to the needs of the statistical testing approach. For example, in order to better capture the PRA context for statistical testing, it may be necessary to add additional control functions, adjust boundary condition assumptions, and disable protective function under test. These changes will serve to relax some of the bounding assumptions used for deterministic safety analysis and provide a more realistic PRA context for characterizing the digital system operational profile. However, a more general question is how far one can go in trying to make the TH model realistic. For Loop 2A, it has a secondary cooling system, cooled by a tertiary system that depends on the weather which changes often. These are practical limitations of the simulation.

2. Modeling of variability in the plant initial condition

In this study, the initial condition of Loop 2A was the one defined in the RELAP5 model. For example, the reactor is assumed to be operating at 100% power and no variability in the condition was considered. This often also is the assumption made in a PRA, but in general, the reactor may operate under different conditions, for example, at a level lower than 100% power. Given that the reactor is operating at a power level, Loop 2A may operate in different conditions in terms of its TH condition.

3. Modeling of PRA failure events

The failure events modeled in a PRA often are at a high level and lack the details needed to specify a RELAP5 run. Therefore, thirteen probabilistic failure models were developed for thirteen categories of failure effects with the parameters needed in defining the failure effects to be modeled using RELAP5 and probability distributions to characterize the variability of the failure effects. Each cutset was assigned to have one or more of the 13 categories of failure effects. The assessment of the probability distributions involved engineering considerations (e.g., in deciding the upper and lower bounds of a distribution) and assumptions on the type of distributions (i.e., the choice of uniform distribution). In some cases, the bounds of the distributions were selected without strong bases. Engineering analyses of the failure modes potentially can offer better bases for the distributions. In addition, some failure events either do not have their associated components modeled in the RELAP5 model (e.g., secondary component failures) or only indirectly affect the TH condition of the loop, for example, loss of a bus that supplies power to some components of the LOCS. Therefore, the failure effects of these failures are approximated by one or more of the 13 failure categories.

The development of probabilistic failure models to capture the variability in the thermal hydraulic effects of PRA-postulated failures is an innovative approach that is needed in the study and any other similar studies. It also can be used in dynamic PRA modeling. In general, data can be collected and experiments and engineering analyses can be performed to further support the development of the models.

4. Assigning equal probability to subcategories of failure effects

As described in Section 5.3, samples were taken from the cutsets that resulted in a reactivity insertion based on the cutset probabilities. Once a cutset is sampled, its failure effect is represented by one or more of the 13 categories of failure effects. For some categories, there are subcategories representing different failure effects or locations (Table 5-1), and when used in sampling, the subcategories are assumed equally likely. For most of these categories (i.e., pipe plugging and pipe break), the assumption of equal likelihood may be reasonable because they represent failure occurring at different locations which the PRA model does not specify. However, for pump failure, the two subcategories, pump trip and pump seizure, do not have the same likelihood; the former is expected to be much more likely than the latter. This is an error of the sampling that can be corrected by mapping individual cutsets directly to the subcategories.

6. TEST CASE GENERATION

6.1 Grouping of Cutsets for Generating Test Cases

The PRA model described in Section 4 was used to generate cutsets from the fault tree representing the reactivity accidents associated with Loop 2A. The cutsets were sampled based on their frequency, and each one defines a test case to be simulated with the RELAP5 model. Furthermore, each cutset includes one or more component failure events whose effects must be simulated.

This study requires that the RELAP5 model of the Loop 2A is able to simulate reactivity insertion events (RIE). For the sake of simplicity, each RIE cutset was grouped according to its failure effects in this study. Section 6.1.1 details the general paradigm used for grouping the cutsets and briefly describes the type of effects that each failure effect group represents. Section 6.1.2 discusses a semi-automated method of classifying a cutset to one or more failure effect groups. Finally, Section 6.1.3 describes how the probabilistic failure models (See Section 5.2.2 for more detailed descriptions of the RELAP5 simulation strategy for each group.) associated with the failure effect groups were used to capture the variability in these effects within the group and then used in generating test cases to be simulated with RELAP5. Appendix A shows the top 200 cutsets that were used in this study in generating test cases and their failure effect group assignment.

6.1.1 Grouping of Cutset by Failure Impacts

Solving the probabilistic risk assessment (PRA) model yields a list of cutsets representing events that will result in reactivity insertion. Each cutset consists of either a single failure event or multiple failure events. These events define the LOCS execution environment and also the RELAP5 model simulation boundary. Ideally the RELAP5 model covers all failure events. If this cannot be accomplished, which is the case in this study due to a simplified RELAP5 model, the failure effects of some failure events can only be approximately simulated. For instance, the RELAP5 model of loop 2A does not contain a secondary loop. If a cutset involves failure of components in the secondary loop, explicit modeling of the secondary loop failure components becomes impossible. However, such components' failures lead to reduction in secondary loop flow rate, and that in turn reduces cooling of the primary (i.e., loop 2A) side. Therefore, by manipulating the heat transfer rate of the heat exchanger, the secondary side failure events can be modeled in RELAP5.

There are other failure events that may lead to the heat exchanger performance degradation. From the example described above, it is reasonable to group such cutsets into one group and model them in the same way within the RELAP5 model. This approach is able to group all the cutsets obtained from the PRA analysis into limited number of bins and ease the RELAP5 modeling effort.

Table 6-1 shows 13 failure effect groups developed to represent the impact of the failure events in the cutsets. A majority of the cutsets belong to the RFW130 group. They represent a failure of combination of failures that affects the secondary side of the heat exchanger. This group represents the failure effect of a reduction in the rate of the heat removal rate of from the primary loop side. In the RELAP5 model, the secondary loop is modeled as a boundary condition with a fixed temperature. Therefore, the reduced coolant flow rate in the secondary

side cannot be modeled directly. However, there are multiple ways to approximate its effect. For example, the boundary temperature can be increased, the heat transfer coefficient at the heat exchanger can be lowered, or the heat transfer area can be decreased. Some of these approximate methods have side effects. For instance, increasing the boundary temperature can lead to scenarios where heat is transferred from the secondary to the primary side, resulting in the system behaving unrealistically. Using engineering judgment, it was decided that lowering the heat transfer coefficient leads to the most realistic approximation of the reduced flow scenario. The selections of the approximation technique for the failure effect groups are shown in the last column of Table 6-1.

Another example of the use of the groups is the modeling of the pressurizer. The RELAP5 model does not contain the pressurizer heaters and sprays, which are the major means to control the pressure. To simulate the loss of pressure control, a pipe break transient was used to initiate a drop in pressure. All cutsets leading to a loss of pressurizer heater were assigned to the gPipe group and simulated the same way as the small-break loss of coolant accident (SBLOCA) cutset even though the two scenarios clearly differ. This grouping practice is based on the same effects of the cutsets on the system.

Table 6-1 also shows that some groups are further divided into subgroups. The gPump group represents all cutsets that ultimately cause the pump to fail. However, there are multiple ways (failure modes) that a pump can fail and the different ways may lead to different reactor transients. It may trip, for example, resulting in a flow rate that follows the pump coastdown curve. A pump also may seize, resulting a more abrupt reduction in flow. The PRA analysis does not always specify the failure mode (i.e., a cutset may only show that a pump failure occurs, but not the mode of the failure). For the purpose of modeling in RELAP5, however, the failure mode is important since it will determine how the failure should be represented. For this study, two modes (trip and seizure) were considered; they consist of subgroups that are shown in the third column of Table 6-1. Other examples of subgroups are gFlow (flow blockage group, subgroups are block location) and gPipe (pipe break group, subgroups are break location).

It is noted that some cutsets or failure events have wider impact on the system and may belong to multiple groups. An example is a loss of power event that leads to loss of the loop operating control system (LOCS) distributed processing unit (DPU). Since the DPU controls all the LOCS control functions, its loss would lead to a loss of control of flow, pressure, and temperature. Therefore, this loss of power event was assigned to both the gFCtrlO and gTctrlHO groups. Table 6-2 shows the assignments of a few cutsets to different groups. A complete list is given in Appendix A.

Table 6-1 Failure effect groups and their modeling in RELAP5.

#	Group	Description	Effect of Failure (for modes leading to trip demand)	Modeling in RELAP5
1	RFW130	Loss of heat-exchanger cooling	The heat exchanger is unable to remove heat from loop 2A, leading to rise in the loop temperature.	Decrease the heat transfer coefficient at the heat exchanger to zero over a variable time.
2	gPump	Primary pump failure – Trip	Forced circulation in loop 2A ends.	Shift (in time) the coastdown curve by a variable multiplicative constant.
3		Primary pump failure – Seizure	Forced circulation in loop 2A ends.	Linearly reduce pump speed to zero over a variable period.
4	gFlow	Plugging – flow element 1	Flow area at flow element 1 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at flow element 1 by a variable amount.
5		Plugging – flow element 2	Flow area at flow element 2 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at flow element 2 by a variable amount.
6		Plugging – strainer 145	Flow area at strainer-145 decreases, leading to reduced flow rate in loop 2A.	Reduce flow area at strainer-145 by a variable amount.
7	gPipe	Pipe break – IPT Inlet	Volume and flow rate of loop 2A coolant decrease.	Introduce a pipe break of a variable size at the IPT inlet.
8		Pipe break – IPT Outlet	Volume and flow rate of loop 2A coolant decrease.	Introduce a pipe break of a variable size at the IPT outlet.
9	gFctrlI	Flow control components failure (sensors and analog input module)	Loss of ability to increase loop flow rate in response to transients resulting in flow rate reduction.	Reduce flow rate by a variable amount by adjusting input to the flow controller by a variable amount.
10	gFctrlO	Flow control components failure (DPU and analog output module)	Loss of ability to increase loop flow rate in response to transients resulting in flow rate reduction	Reduce flow rate by a variable amount by adjusting output from the flow controller by a variable amount.
11	gTctrlHI	Temperature control components (line heater) failure (sensor and analog input module)	Loss of ability to decrease coolant temperature via line heater output reduction in response to transients resulting in temperature increase.	Increase coolant temperature by increasing line heater output by a variable amount by adjusting input to the controller (CV-1).
12	gTctrlHO	Temperature control components (line heater) failure (DPU and analog output module)	Loss of ability to decrease coolant temperature via line heater output reduction in response to transients resulting in temperature increase.	Increase coolant temperature by increasing line heater output by a variable amount by adjusting output from the controller (CV-4).
13	gTctrlV	Temperature control components (TCV-3-1) failure	Loss of ability to decrease coolant temperature via increasing flow to heat exchanger in response to transients resulting in temperature increase.	Increase coolant temperature by fully closing TCV-3-1 over a variable period.

Table 6-2 Sample cutset showing failures leading to reactivity insertion and their group assignment.

#	Probability	Basic Event ID	Basic Event Description	Group ID Code
3	1.86E-01			gRFW130
	8.15E-04	ASW-STF-FF-0000FE42-0000	Flow element FE-4-2 fails (plugs)	
	0.625	DRX-GEN-AD-000OPPOS-0010	DRX plant availability factor	
	365	DRX-GEN-AD-DAYTOYR	Day to year conversion	
4	4.04E-02			gFlow
	0.625	DRX-GEN-AD-000OPPOS-0010	DRX plant availability factor	
	1.77E-04	EXT-SNR-PG-02ACT145-0000	Train 2A-C strainer 145 plugs	
	365	DRX-GEN-AD-DAYTOYR	Day to year conversion	
5	1.56E-02			gRFW130
	6.84E-05	DCS-DOM-FF-2NE2F1_A-0000	Digital output module 2NE-2F1 fails to function/operate	
	0.625	DRX-GEN-AD-000OPPOS-0010	DRX plant availability factor	
	365	DRX-GEN-AD-DAYTOYR	Day to year conversion	
6	5.48E-03			gPipe
	0.625	DRX-GEN-AD-000OPPOS-0010	DRX plant availability factor	
	2.40E-05	EXT-HTR-FF-000002AC-0000	Pressurizer heaters fail to function	
	365	DRX-GEN-AD-DAYTOYR	Day to year conversion	

6.1.2 Automation of Cutset Group Assignment

Manually grouping all the cutsets would be very time consuming. A Python [Rossum] script was developed to semi-automate the process. This automation was made possible due to two properties of the PRA model. First, although 200 cutsets were considered, there were only 44 unique basic events. Most cutsets merely are various combinations of these basic events. Second, many of the basic events are already grouped according to their impact on the system in the PRA model. For instance, those basic events that ultimately lead to a loss of power to the pump are all under their own fault trees. These fault trees appear as transfer gates (subtrees) in the reactivity insertion tree (Section 4.3 describes the PRA model details). Another example involves failure of the secondary system components that appear under a transfer gate, viz., “insufficient cooling flow from RFW header” (RFW130). Those that cannot be categorized in these ways were manually assigned to the groups in Table 6-1 according to the impact of their failure. The script contains a database linking these basic events to the groups. Detailed algorithm is described below. The algorithm is based on the fact that unlike the cutsets in the main fault trees (fault trees for loss of pressure, loss of temperature, and loss of flow controls), which may belong to many different failure effect groups, all the cutsets for a subtree belong to the same group.

For those fault trees that contain subtrees, the subtrees (e.g., DPU power supply, secondary system components, pressurizer heater power supply) were solved individually and their cutsets were read by the script. The cutsets for each subtree were stored in a list variable[19]. This way, when the cutsets for the main tree were read during a test case generation, the script can appropriately group the cutsets by identifying the list variables containing the cutset. For example, if a cutset for the "loss of pressure control" fault tree (the parent fault tree) was found in the list variable for "loss of pressurizer heater power supply" (the subtree), the script assigned this cutset to the appropriate failure effect group (Table 6-1). The procedure described in this paragraph was used in EXT-2AC-PMP (loss of loop 2AC coolant pump), EXT-2AC-PRZZPWR (loss of power to pressurizer heater), RFW130 (insufficient coolant flow from RFW header) and EXT-2AC-RPU (loop 2AC RPU failure).

Fault tree basic events that are not part of any above subtrees (i.e., those that appear as basic events in EXT-2AC-TEQ, Ext-2AC-LPEQ, or EXT-2AC-FEQ) were manually assigned to groups. As an example, the fault tree basic event "analog input module 1E3" appears in EXT-2AC-TEQ. Based on the fact that this input module is part of the heat exchanger bypass valve control, this failure event was manually classified into the gTctrlHI group. About 12 basic events were handled manually, and this rule were hard-coded in the script

The algorithm used in the script is shown in Figure 6-1. The script first reads the output file from the SAPHIRE model containing a list of cutsets for core damage. Each cutset in the list has the basic event identifier, the basic event description, and either the occurrence frequency or probability. Next, the script populates *component_list* (this is a list variable) with a list of either subtrees or intermediate gates in a fault tree that determine the failure behavior. These subtrees or gates (which will be referred to as *component* in this discussion) model the loop primary pumps, pressurizer heater power source, secondary cooling system, and the remote processing unit (RPU) and its power sources. Each component is considered belonging to one or more group based on its failure effect. The final step in the script is to iterate through each cutset (read in the first step) and assign that cutset to the appropriate groups.

1. *CS* ← list of cutsets read from SAPHIRE output file
2. *component_list* ← list of component subtree
3. For each *component* in *component_list*:
   a. *component_cs*[*component*] ← list of cutset of *component*
   b. *group*[*component*] ←list of group assigned to *component*
4. For each *cutset* in *CS*:
   a. For each *component* in *component_list*:
      i. if *cutset* issuperset(*component_cs*[*component*]):

Figure 6-1 Algorithm for the script used to classify cutsets

[19] In Python, a list variable is an array whose elements can be of mixed data types.

As discussed in Section 6.1.1, some cutsets were assigned to multiple groups. For any cutset, the script checks each group in Table 6-1 to determine whether the current cutset is a superset of the group cutset. If so, then the cutset is assigned to that group. Note that the assignment is not exclusive. The script maintains a variable for each cutset that represents a list of groups assigned to the cutset. This list may just contain one or multiple groups. This list of groups to which a cutset belongs will dictate how the RELAP5 model is used to simulate that cutset, as discussed in Section 6.1.3.

6.1.3 Use of Probabilistic Failure Models of Failure Effect Groups in Generating Test Cases

This section briefly discusses how probabilistic failure models were used in capturing the variability of failure effect groups, how test cases were sampled, and how a Python script was used to automate the generation of the RELAP5 input. A more detailed discussion is provided in Section 6.2.

The cutsets that were obtained from solving the PRA model represent one or more failures events that can lead to a reactivity insertion. However, the cutsets may not specify exactly how or where a component fails, which the RELAP modeling needs. For example, failure events such as pipe plugging or pipe breaking may occur at any location in the loop while a pump failure may lead to different coast down rates. In Section 6.1.2, the cutsets are grouped into 13 groups based on high level information of their effects, as is shown in Table 6-1. Appendix A has a complete list of the top 200 cutsets that were used in this study and their failure effect group assignment. These groups must be developed further to capture the variability within each of them. Section 5 has detailed descriptions of the probabilistic failure models of the groups of failure effects. Each probabilistic failure model uses a probabilistic distribution of a parameter to represent the variability. For example, in a valve failure, given that the failure mode is spuriously closing, the random parameter may be the time over which the valve closes, or the final area to which the valve closes. This random parameter is important because in the RELAP5 input file, the position of the valve as a function time must be specified. It is assumed that a random parameter is distributed uniformly over a certain range so that to specify the state of a component, the parameter is drawn from a uniform distribution over a fixed range as discussed in Section 5.2.2. The range itself is determined on either physical consideration or sensitivity analysis. A sample taken from the distribution would define a test case to be simulated using the RELAP5 model. It is noted that cutsets that belong to more than one failure effect groups will have multiple associated random parameters.

For a component with multiple failure modes (e.g., a pump may seize or trip), not only must the failure mode be known, but also how frequently each mode occurs should be known. In most cases, these failure mode frequencies are either assumed or are estimated from the literature. Section 6.2 discusses in more detail the failure mode frequency.

To create the RELAP5 input file for a test case, a Python script was used to (1) sample a cutset from the cutset list based on the cutset frequency, (2) determine the failure effect group(s) of the cutset, (3) sample the relevant parameters (e.g., break size or valve closure rate) from its probabilistic failure model, and (4) modify the base case RELAP5 input deck to simulate the failure(s). Section 6.2 gives a detailed description of the Python script.

6.2 Sampling and Simulation of Test Cases

6.2.1 Sampling of Cutsets

Section 4.3 described how the list of cutsets of the reactivity insertion accidents was generated from the PRA analysis. Section 6.1 detailed how each cutset was assigned to one or more groups of failure effects (and the associated probabilistic failure models). Section 5.2.2 further described how the 13 groups of failure effects were modeled in RELAP5 and the assumptions associated with each one. This section describes the Python script that was used to automatically sample the cutsets while Section 6.2.2 discusses how the RELAP5 input decks were automatically generated after a cutset (sample) was selected for the simulation.

From the PRA analysis, each reactivity insertion cutset has an associated occurrence frequency. In selecting a sample for the simulation, the probability of a selected cutset is the ratio of its occurrence frequency to the total reactivity insertion frequency. For this study, 10,000 sampled cutsets (referred as "samples" in the following discussion) were used for the simulation. These samples were generated by a Python script, with each sample (i.e., cutset) selected according to its probability. The script took the cutset list described in Appendix A, the probability of each cutset in the list, and a flag designating that the sampling was to be done with replacement (i.e., each cutset may be selected multiple times) as its inputs. The output was 10,000 random cutsets, drawn from this list according to their probability.

For each cutset, the Python script internally maintains a list data structure that contains the groups to which the particular cutset belongs. Some groups such as pipe plugging contain multiple subgroups (e.g., for the pipe plugging groups, the subgroups represent the blockage location). In these cases, the script selected one subgroup randomly according to the subgroup probability. For this study, all subgroups were assumed to have an equal probability so that each one has an equal chance of being selected. The subgroup that was selected for the sample then was added to the list data structure.

Next, the script determined the parameters associated with each group. As shown in Table 5-1, each group or subgroup has an upper and lower bound. The script assumed a uniform distribution and selected a random number between these bounds. For example, for the loss of heat exchanger cooling group (group 1 in Table 5-1), the script picked a random number between 0 and 1670. This number then represents the time at which the heat transfer coefficient reaches 0 for this sample. The script used this time later to generate the RELAP5 case (Section 6.2.2).

For all samplings (cutset list sampling, subgroup sampling, and parameter sampling), the Python SciPy [Jones 2001] library was used. SciPy is a scientific library that allows Python to perform routine operations (such as sampling from different distributions) without extensive programming by the user. To assure reproducibility of the results, a fixed seed was used for generating random numbers, allowing the output to be replicated in subsequent runs.

6.2.2 Generation of Input Decks

This section discusses the automation of the RELAP5 input file generation, the addition of noise to the RELAP5 output to simulate the sensors noise, and finally, the actual simulation of the cases at INL.

Automating the generation of the RELAP5 input file facilitated the conversion of the Monte Carlo sample (i.e., the accident scenario) into the corresponding RELAP5 file. For each accident scenario (cutset), the RELAP5 case was constructed by copying relevant sections from a RELAP5 template file to reflect the changes from the steady state condition. For example, a pipe break cutset was modeled by constructing an input file that contained the location and the size of the break. This information was entered in the "transient" input deck that listed all the changes from the "steady state" input deck. The script achieved automation by generating these transient decks based on the samples that were selected from the list of cutsets shown in Appendix A.

Each sample contained information on the components that failed and the numerical parameters associated with that failure. As discussed in Section 6.2.1, these parameters were generated by sampling from a uniform distribution within a predetermined range. Table 6-3 shows a portion of the sample file. Each line represents one failed component. The columns, from left to right, are the following: sample number, cutset number, failure effect group, first random parameter, and second random parameter.

Table 6-3 Portion of the sample file.

Sample No.	Cutset No.	Group	Parameter 1	Parameter 2
1	2	gRFW130	5.902E+02	NA
2	4	gFlow	FE2	2.813E-04
3	4	gFlow	S145	3.876E-05
4	3	gRFW130	2.396E+02	NA
5	1	gRFW130	1.140E+03	NA

The algorithm of the script is shown in Figure 6-3. The high level description of the script is as follows:

1. Read the sample information from the sample file into *sample_list*. The sample file also contains the failure effect group(s) of the cutset. This is read into *sample.group* which is a list variable containing all the cutset groups (Table 5-1) assigned to a cutset.
2. Read the template file to determine what information must be included in the transient RELAP5 input file. These lines, stored in *b_common* and *b_specific*, are copied to the transient deck, with the appropriate random parameter.
3. Write the transient deck with a filename, specifying the type of the sample.

The template file that was used by the script was a template that contained information on how the transient deck should be constructed given the type of cutset to be simulated. Since there are only 13 failure effect groups, the template file was constructed manually with notations to indicate which portion of the template file was to be used for which cutset group. The script then read the appropriate section of the template file and modified the appropriate parameter to reflect the random parameter. A portion of the template file is shown in Figure 6-2. The lines preceded by an asterisk denote a comment and are used to identify appropriate sections to copy to the transient input file.

```
*  To simulate Line Heater Input Failure ----------------------------
*              name         type         value
20500010    "TempDiff"      constant        490.0
*  To simulate Line Heater Input Failure ----------------------------
*
*  To simulate Line Heater Output Failure ---------------------------
*              name         type         value
20500040    "HtrPower"      constant      177326.9
*  To simulate Line Heater Output Failure ---------------------------
*
*  To simulate FCV Controller Input failure-------------------------
*             name         type         value
20502400    "InFlow"      constant        35.1
*  To simulate FCV Controller Input failure-------------------------
```

Figure 6-2 Portion of the template file

1. *b_Common* ← list of common block read from master file
2. *b_Specific* ← list of group-specific block read from master file
3. For each *sample* in *sample_list*:
   a. Write *b_Common*
   b. For each *group* in *sample.group*:
      i. Generate random parameter
      ii. Write *b_Specific*[*group*]

Figure 6-3 Algorithm for the script used to generate RELAP5 input file

After the output files were constructed for the 10,000 cases, they were separated into four groups to be run on four computers. The grouping was done on the basis of the estimated runtime for each file; each group was designed to have similar runtime. A Fortran program was used for each group to extract relevant information (e.g., sensor output) from the RELAP5 restart files. (The restart file is a binary file that contains all the output from a RELAP5 run.) The final output was a text file that contained, for each time step, the value of the parameter (in both engineering units and miliamps) for each sensor (e.g., pressure, temperature, and mass flow rate). With four personal computers running in parallel, the cases were completed in few days.

This output file contains the RELAP5 simulation results of the physical parameter at the sensor locations. These numbers are calculated deterministically, based on appropriate physical laws or correlations, and do not account for variability due to sensor noise. To account for the sensor inaccuracy, white noise was added to the output. INL provided BNL with the error range for each sensor that is part of the LOCS protection functions (Table 6-4). The amount of noise therefore was obtained by sampling from this error range and assuming a uniform distribution. This noise, calculated for each sensor, was added to the RELAP5 value to account for the variability among different sensors. Since, for control functions, there are three sensors in the system, each physical parameter (e.g., pressure) is added to an individual white noise. For example, to find the noise associated with the three IPT inlet flow sensors FT-1A, FT-1B, and FT-1C, three samples were taken from a uniform distribution between -1.03 and +1.03. Each of

these three values, representing the noise for each sensor, was then added to the RELAP5 output for the IPT inlet flow to obtain the readings for these three flow sensors.

Table 6-4 Accuracy of sensors modeled in RELAP5 Loop 2A Model.

Sensor	Unit	Accuracy
IPT Inlet Flow FT-1	GPM	$\pm$ 1.03
IPT Inlet Pressure PT-2	PSIG	$\pm$ 8.1
IPT Inlet Temperature TT-41	^{o}F	$\pm$ 1.12
IPT Outlet Temperature TT-32	^{o}F	$\pm$ 1.12

In Section 7, INL developed a configuration to execute the tests using the LOCS hardware and software, and used the RELAP5 output file that contains the sensor reading (with noise added) as the input. The outputs of these tests are then evaluated by BNL to determine the success/failure of the protection system to generate a reactor trip (Section 8).

7. TEST CONFIGURATION, EXECUTION, AND EVALUATION

7.1 Introduction

This section describes (1) the establishment of the test configuration used in testing the loop operating and control system (LOCS), (2) the procedure followed in validating the test configuration and in executing the test cases, and (3) the evaluation of the test results. The work was done jointly by staff at Brookhaven National Laboratory (BNL) and Idaho National Laboratory (INL).

Figure 7-1 gives a high level view of the testing process. As described in Section 6, test cases were generated via RELAP5 simulations of reactivity insertion scenarios derived from a probabilistic risk assessment (PRA). Each test case consists of time-stamped records with values of physical parameters that were generated by the RELAP5 simulation. The Testing Host Computer takes test cases, converts the values of the physical parameters into analog signals, and feeds them into the LOCS. The Testing Host Computer then receives the trip signals as test results. The host computer then generates time-stamped records of these outputs, saving them in a file with the test results. Next, these results are evaluated to determine if a trip signal is generated in time based on a predefined success criterion. The successes and failures of the tests are then used in estimating the system failure probability.

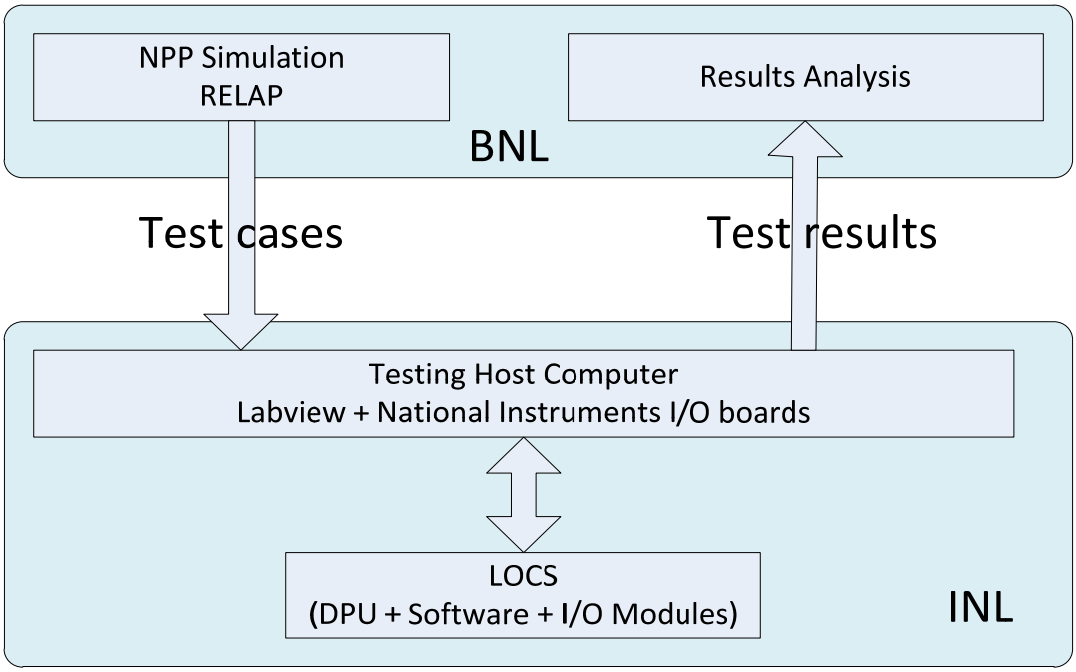


Figure 7-1 Work flow associated with performing the tests

7.2 Establishment of a Test Configuration

The Loop 2A Distributed Control System (DCS) has 183 analog inputs, 52 digital inputs, 7 analog outputs, and 39 digital outputs, all of which interface with the loop Remote Processing Unit (RPU). Simulating all 235 input signals would necessitate having a large, complex, and costly system. While most loop parameters are not considered safety related, a few are and they directly drive the loop safety SCRAM output channels. Therefore these safety related instrument signals were the only simulated signals required to exercise the safety functions of the DCS software. During the test, the remaining loop input channels were configured (placed in simulation mode) to hold a software setpoint value that does not contribute to off-normal conditions nor produce non-safety alarms that would require an operator actions.

The LOCS inputs and outputs that INL identified as safety-relevant were provided to BNL. All other DCS RPU input/output (I/O) for loop 2A were placed into the "simulate mode", and each channel was set with a "dummy" signal value. None of these I/O signals could trigger a SCRAM and so were ignored by the Control Software Failure Test Signal Simulator (CSFT-INL-SS), that is, the host computer, throughout the entire execution of the test.

Based on the preceding discussions, INL developed a computerized system for simulating signals that produces 14 analog current output signals that represent the instrument signals in the normal real world plant. Figure 7-2 is an overall diagram of the CSFT testing system and environment; it gives a better understanding of the integration of the equipment. This Signal Simulator is closely connected to the Loop 2A DCS RPU development and test system, the primary purpose of which is to test the code and configurations before their deployment to the Advanced Test Reactor (ATR). The software configuration was identical to the version running at the ATR.

The CSFT-SS (host computer) also monitors and collects the response of the LOCS digital SCRAM channels (A, B, C). Each simulated level of the analog output channel is driven by values obtained from the output of runs of the RELAP5 model, each representing a test case. The values for each case are organized into a scenario file containing a set of time-stamped records that include information on steps and timing along with the 14 signal values. The hardware and software of the test configuration is described below.

Hardware

The test configuration shown in Figure 7-2 allows testing of the protection functions of the LOCS of ATR loop 2A; its input instrumentation is replaced with simulated analog input signals whose values were generated using a RELAP5 model of the loop. The CSF-SS (the host computer) is a personal computer with a National Instruments analog output and digital input system. Output data from the RELAP5 model at BNL was collected in scenario event simulation files that then are used to drive CSFT-SS signal simulator with all 12 safety related sensor inputs plus 2 other critical control input values of the LOCS DCS at INL.

To provide the needed real time simulation function, this signal simulator uses National Instruments (NI) Compact cDAQ rack and module hardware in conjunction with the Lab View software Development system. Simulator analog output channels were connected to proper

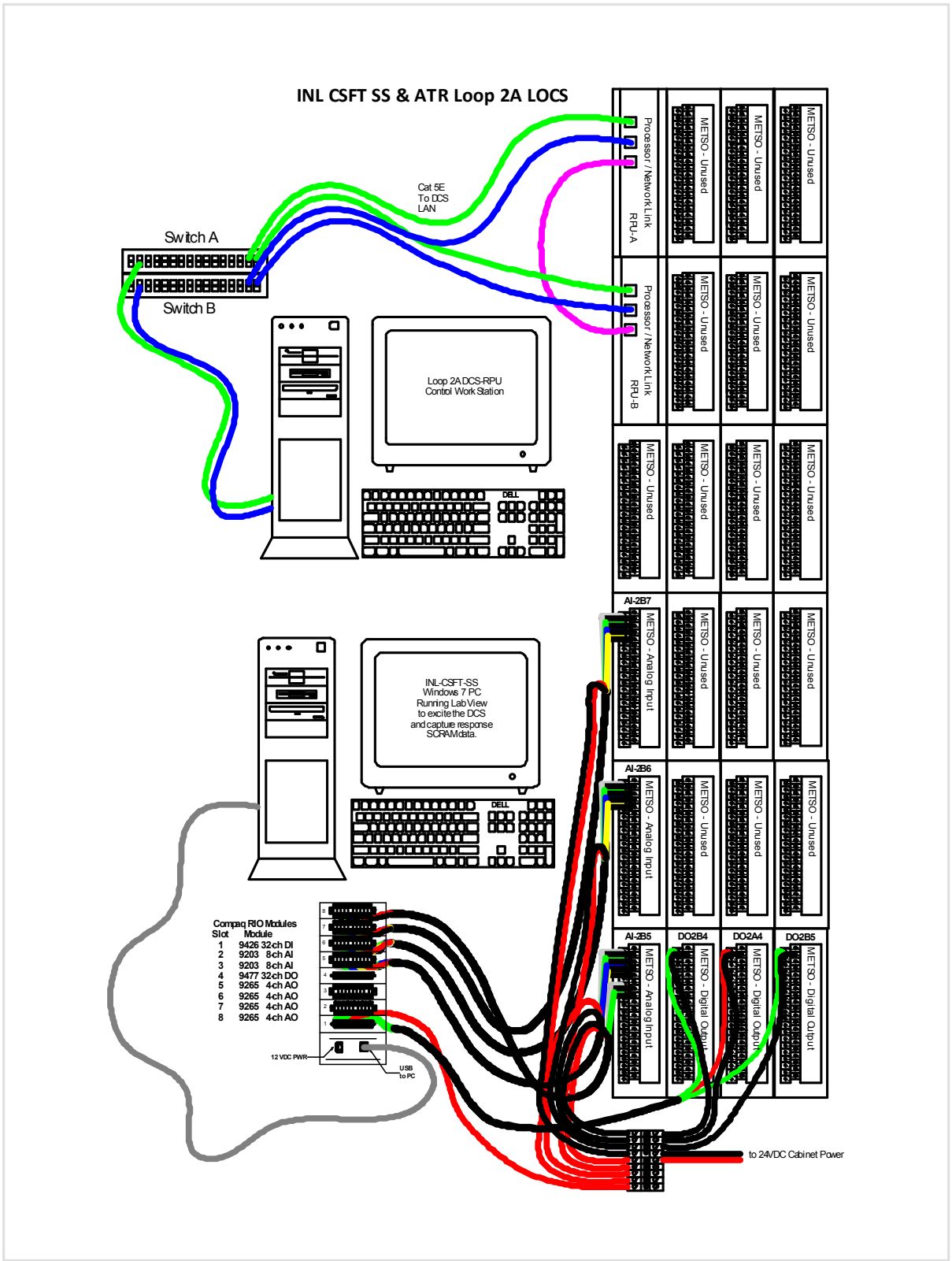


Figure 7-2 CSFT-SS testing environment

DCS Loop 2A input channels using copper wire cables made for this application. Below is a listing of items that compose the testing system; they were purchased or were on hand. .

Manufacturer	Item Description
National Instruments	9203 CompactDAQ 8-ch. 16 bit +20 mA Input module
National Instruments	9265 CompactDAQ 4-ch. 16 bit +20 mA Output module
National Instruments	9477 CompactDAQ 32-ch. (sinking) Digital Output module
National Instruments	9426 CompactDAQ 32-ch. (Sourcing) Digital Input module
National Instruments	cDAQ9178 CompactDAQ, 8-slot USB Chassis
National Instruments	LabView, Full Development System.
Dell	Dell PC running Windows 7, w/ DVD writer

Software

A Lab View [LabVIEW] application program was developed that reproduces BNL's RELAP5-derived analog signals on NI Compact Rio cDAQ output channels in near real time. The CSFT-SS (host computer) reads an entire scenario file into a memory array and then uses the in-record timing information to schedule and implement each record of the values of 14 channel outputs. Normally, a scenario file contains from 100 to 18,000 records. Sequentially, each record of 14 values is loaded into 14 output channel buffers and activated for the hold time period specified in the record. Hold time for these scenarios is typically 0.1 seconds. Near the end of the hold time, the digital input channels for SCRAM A, B, and C are sampled and recorded in the output array along with the time, and the current input record number. This iterative process is repeated until the entire array has been run once; then, the output array is written to a file using the same input name with "-out" appended to its name. The next scenario file is then read into memory and run until all files have been run once.

The bulk of the project's calendar time was taken up by the unattended monitoring of this automated system while it executed BNL's RELAP5 test data cases and collected the resulting output data. Each of BNL's input files was renamed by appending "_in.csv" to it. The corresponding output file is similarly named but ends with "_out.csv" instead. All CSFT SS response (output) data files produced at INL have the following content: Date/time, record serial#, SCRAM-A, SCRAM-B, SCRAM-C.

Lining up the input files to the output files is facilitated by using the record serial# for any variable interval scenario. The record serial# is included for this purpose.

Figure 7-3 is a view of the CSFT-SS main window. Analog output values appear across the middle in the 14 numerical boxes; the SCRAM A, B, & C status block of round green buttons is on the bottom.

Table 7-1 shows the ATR Loop 2A safety relevant signals that were simulated via the RELAP5 model and used as input to the CSFT-SS. The RELAP5 scenario outputs are used as test case inputs to the LOCS. The content of each file (scenario) consists of Elapse Time starting at 0.0, an Interval time for the step (both in seconds), and the 14 instrument values. This time sequence information was organized in time step records, each consisting of the above items. Each test case is a single file containing a series of these records. Two different versions of a scenario were produced, one that contains engineering units for the 14 instrument values, and a second version with milliamp units that are equivalent to the engineering units. This second scenario file has the milliamp values and was the actual file type used as input to the CSFT-SS test. The engineering unit file was used only if it were necessary to check the validity of a milliamp value.

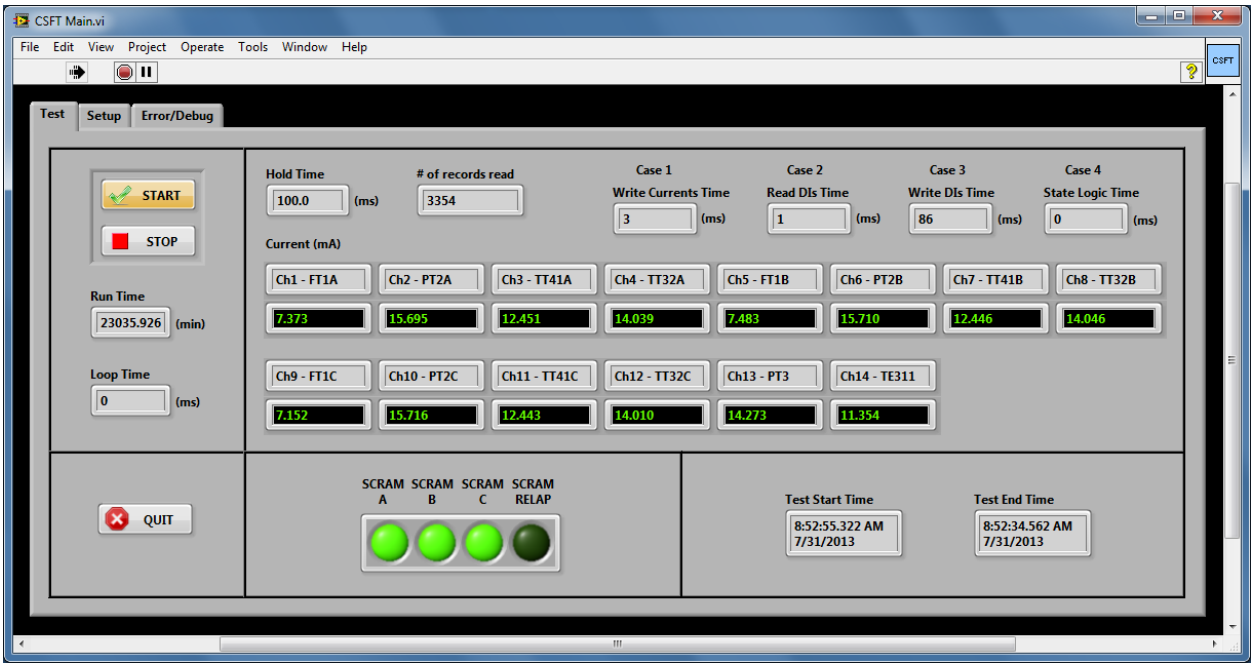


Figure 7-3 A view of the CSFT-SS main window

Table 7-1 ATR Loop 2A signals simulated with the RELAP5 model and used as input to the CSFT-SS.

Field #	ID or Tag Name	NI Output Channel	Data Type	Format	Eng. Units	Range	DCS Trip Point
1	Time, running	No output	Real	xxx.xxx	Seconds	0-max	none
2	Step Interval	No output	Real	x.xx	Seconds	0-max	none
3	FT-1A	Mod5-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
4	PT-2A	Mod5-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
5	TT-41A	Mod5-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
6	TT-32A	Mod5-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
7	FT-1B	Mod6-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
8	PT-2B	Mod6-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
9	TT-41B	Mod6-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
10	TT-32B	Mod6-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
11	FT-1C	Mod7-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
12	PT-2C	Mod7-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
13	TT-41C	Mod7-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
14	TT-32C	Mod7-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
15	PT-3	Mod8-Ch-0	Real	xx.xxx	milliamps	4 - 20	No Trip
16	TE-31-1	Mod8-Ch-1	Real	xx.xxx	milliamps	4 - 20	N0 Trip

Table 7-2 Output record data collected in the CSFT-SS scenario output files.

Field Number	NI Input Channel	Item Identifier	Data Type	Format	Engineering Units	Value Range
1	none	time	real	xxxxx.xxx	Seconds	increasing
2	none	Rec #	integer	xxxxx	Input rec #	0-n
3	DI-0	SCRAM-A	Logical	x	0=true, 1=false	0 or 1
4	DI-1	SCRAM-B	Logical	x	0=true, 1=false	0 or 1
5	DI-2	SCRAM-C	Logical	x	0=true, 1=false	0 or 1

7.3 Execution of the Test Cases

Since testing required that the work between BNL and INL be coordinated, the process followed a phased approach. That is, some test cases had to be run before undertaking the production runs of 10,000 cases such that a workable process could be established and ensured for those runs. For example, the content and format of the files exchanged between the two laboratories needed to be determined, as did the size of the time step, the duration of the tests, and the cycle time constraint of the CSFT-SS. More importantly, the earlier test runs also served as a validation of the test configuration by ensuring that the results were consistent with those expected.

Initial test runs

The RELAP5 model originally was developed to simulate two scenarios, a large LOCA and heat exchanger bypass. Accordingly, a few RELAP5 runs were performed first to decide upon the time steps needed to properly simulate these scenarios and to determine how long the tests should last. These test cases were sent to INL to aid its design of the Lab view software of the CSFT-SS. It was recognized that very short time steps (i.e., 0.01 second) are needed for a large LOCA that, in turn, requires a short cycle time of the CSFT-SS. On the other hand, the LOCS has a cycle time of 0.3 seconds and will not be able to recognize/capture the changes in very small time steps. Therefore, the RELAP5 model does not have to generate one output record every 0.001 second; hence, that eases the cycle time constraint for the CSFT-SS. In addition, it was recognized that the input records to the CSFT-SS can be read into memory before a test case is started and that the output records of CSFT-SSS can be saved in the memory before the test end such that the input and output operations do not affect the CSFT-SS cycle time. It later was decided that large LOCAs would entail voiding in the core, causing a very fast reactivity transient that cannot be mitigated by LOCS and thus does not need to be simulated. Based on the LOCS cycle time of 0.3 second, it was decided that a time step of 0.1 second should be adequate. Depending on the reactivity scenario, the time when a physical parameter exceeded the threshold such that a reactor trip signal would be generated is determined by the RELAP5 model. It was decided that a RELAP5 simulation can be terminated 30 seconds after the generation of a trip signal. In fact, after the trip is generated, the RELAP5 model no longer produces realistic results compared to the situation without a reactor trip signal.

Test runs of 26 bounding cases

As described in Section 5.2, the failure effects of reactivity insertion accidents can be captured by considering 13 categories of failure effects; accordingly, a probabilistic failure model was developed for each category so that samples taken from the probabilistic failure models will represent a specific reactivity insertion cutset. There, a 30-minute criterion/assumption was used to limit the time needed to simulate an accident scenario based on the assumption that if reactor trip is not needed within 30 minutes, the operator would have recognized the problem and terminated the accident manually. The 30-minutes criterion was used in determining the upper or lower bound of the uniform distributions representing the 13 probabilistic failure models. Before the production runs of the test cases, it was decided that 26 bounding cases corresponding to the upper and lower bounds of the 13 probabilistic failure models should be tested to ensure that the production runs would be executed without problems. These cases also could be used to develop success criteria for evaluating the test results. Accordingly, BNL generated a set of 26 scoping scenarios, that were and sent them to INL to run the tests and acquire output from the CSFT-SS. The success of this scoping test allowed BNL to produce the final set of test cases for use in this project.

Production runs of 10,000 cases

BNL provided INL with the 10,000 test cases stored in 2 solid state Universal Serial Bus (USB) data storage devices. They were organized into 4 groups of approximately 2,500 files each. As described in Section 5, these 4 groups were each generated by running the RELAP5 model on a personal computer. INL simply began running group 1, then 2, 3, and 4. As each group was completed, these grouped output files were zipped and transferred to BNL.

Overall, the INL CSFT-SS system and environment became very efficient and effective for executing test case scenarios that require accuracy in both timeline and signal reproduction.

7.4 Assumptions and Limitations

The test configuration used in the study simulates the conditions experienced by the LOCS being tested in the field. A few deviations from the real conditions are detailed below.

1. In the test configuration, a smaller set of input and output signals were used compared to the hundreds of them in the real situation. The signals associated with the control functions of the LOCS were assumed to have no effect on those used by the protection functions; hence, they were assigned dummy values such that their processing by the LOCS did not significantly affect the timing of the signal processing for the protection functions. This approach reduced the number of I/O modules needed for this study.

2. The input to the LOCS were supplied by a host computer that periodically (with a cycle time of 0.1 second) sends the RELAP5-generated signal values to the LOCS rather than by the real sensor inputs that change constantly. This limitation also reflects the fact that the RELAP5 simulation only generates a set of new values every 0.1 second. The cycle time of the host computer was chosen as 0.1 second. Thus, it can capture the changes in the RELAP5 output.

3. The LOCS has hysteresis reset widows for protection functions. Each protective function has an associated hysteresis window that prevents a trip condition (a measurement exceeding the threshold) from being reset if a trip occurs and the channel value remains near the setpoint. For example, the hysteresis reset window for temperature sensor TT-41 is 2^{o}F (0.04 mA). Thus, if a TT-41 channel indicates a temperature above 510^{o}F at one time step, then that channel will remain in a trip state throughout subsequent time steps as long as the temperature is above 508^{o}F. Section 8 provides more discussions regarding hysteresis reset windows.

   The hysteresis reset windows is set by the LOCS software and was used during the tests to determine when a trip should reset. When evaluating the test outputs, they were taken into consideration when comparing the inputs with the actual time of generation of a trip signal. That is, by examining the inputs and taking into account the effects of the hysteresis reset windows, an expected time was determined when the trip signal should be generated. In fact, to account for the cycle time of the host computer and the LOCS, as is discussed later, a time window in which the trip should take place was determined and used in deciding if an actual trip signal was generated in sufficient time.

4. Since the LOCS and the host computer are not synchronized, and the LOCS has a cycle time of approximately 0.3 second (which is not exact and could vary somewhat) while that of the host computer was 0.1 second, then to capture all the changes the RELAP5 results, some timing considerations in addition to the hysteresis reset windows were used in determining the time window in which an actual trip signal should be generated. The considerations include the following:

   - The LOCS will generate a trip signal whenever, in a time step, the 2-out-of-3 trip logic is satisfied. This signal is expected to last 0.3 seconds, corresponding to 3 time steps in the output.
   - It may take up to 0.3 seconds for the LOCS to read a tripped condition and another 0.3 seconds to generate a tripped output. It may take the host computer 0.1 seconds to read the tripped output from the LOCS.

8. EVALUATION OF TEST RESULTS

This section describes how the test results were analyzed using the inputs to the loop operating control system (LOCS) generated from the RELAP5 model; this determines if each test case represents a success of the LOCS in performing its protection functions. The evaluation of the results was done by (1) estimating, based on input records, a time window in which a trip signal should be generated taking into consideration the cycle times of the LOCS and the test computer as well as the hysteresis windows implemented in the LOCS software (See Section 8.1.1), and (2) determining, based on the output records, the actual time when a trip signals is generated (Section 8.1.2). The timing consideration allows some test results be explained. For example, few test cases show that a trip signal is generated in the first few time steps due to a single input record that exceeded its threshold. Depending on the time when the LOCS reads the input record, it may or may not read the record with the threshold exceeded. Section 8.2 discusses the comparison of the test outputs with the corresponding time windows. Those test cases in which the trip signal was not generated in the time window are called anomalies. The anomalies observed include a failure to trip (however, this was not reproducible) and several early trips and delayed trips. The anomalies were further examined and possible explanations were identified. For some of the anomalous cases, repeated re-runs of the test cases were done to determine if the anomalies could be reproduced. An issue on reproducibility was identified and investigated which is discussed in Section 8.3.

8.1 Determination of a Success Criterion

The input file of a test case consists of records containing the values of the sensors at different time. The results of a test case are saved in a file containing the output of the digital output channels of the LOCS at different time steps. A value of 1 of a digital output channel represents "no trip" and a value of 0 represents a "trip". To determine if the results represent a success, a success criterion had to be established. The criterion used in determining if the LOCS generated a trip signal in time during a test is based on comparing the actual trip time/record determined by output files from the LOCS and the time window in which the trip is expected to occur as determined using the input files to the LOCS. If the actual trip time is outside the expected time window, then it is either an early or late trip. In determining the expected time window, consideration is given to the asynchronous communication between the LOCS (with cycle times of 0.3 second[20]) and the host computer with a cycle time of 0.1 second, and the hysteresis reset windows of the protection functions. Table 8-1 shows the trip setpoints and hysteresis windows for all relevant protective functions. Each function has three channels (sensors); for any time step, a protective function is considered to be in a trip state if 2 out of 3 channels are in a trip state and a trip signal will be sent to the three digital output channels. Each channel of a protective function has an associated hysteresis reset window implemented in LOCS software that prevents the resetting of the trip condition of a channel if a trip occurs in the channel and the channel value remains near the setpoint. For example, the hysteresis window for TT-41 is 2^{o}F (0.04 mA). This means that if a TT-41 channel indicates a temperature above 510 ^{o}F at one LOCS cycle, then that channel will remain in a trip state for subsequent

[20] INL approximated the LOCS cycle time to be 0.3 s based on the observation that when LOCS was challenged with more than 1 trip every 300 ms, it failed to register all the trips. At 1 trip per 300 ms, LOCS successfully registered all the trips. Therefore, the sampling rate for LOCS is at least 300 ms.

LOCS cycles as long as the temperature is above 508 °F. The hysteresis window tends to make it easier (faster) for the LOCS to generate a trip signal. Table 8-1 lists the trip setpoints and hysteresis windows for different trip functions. These windows were accounted for in predicting the time when a trip signal is generated.

Table 8-1 Trip setpoints and hysteresis window for the trip-capable loop protective functions.

Channel Name	Channel Description	Trip Condition	Hysteresis Window
FT-1A, FT-1B, FT-1C	IPT inlet flow	≤ 25 gpm	1 gpm
PT-2A, PT-2B, PT-2C	IPT inlet pressure	≤ 1800 psia	5 psig
TT-41A, TT-41B, TT41C	IPT inlet temperature	≥ 510 °F	2 °F
TT-32A, TT-32B, TT-32C	IPT outlet temperature	≥ 570 °F	2 °F

8.1.1 Estimating a Predicted Trip Time Window

Predicted trip window

The upper boundary of the predicted trip window is the latest time when an actual trip should occur beyond which a delayed trip is considered to have occurred. The LOCS should generate a trip signal and send it to the 3 output channels when any 2 of the 3 input sensor channels exceed the threshold. Since the LOCS and the host computer are not synchronized, there are three possible alignments of the LOCS cycle relative to the host computer cycle to consider, as shown in Figure 8-1.

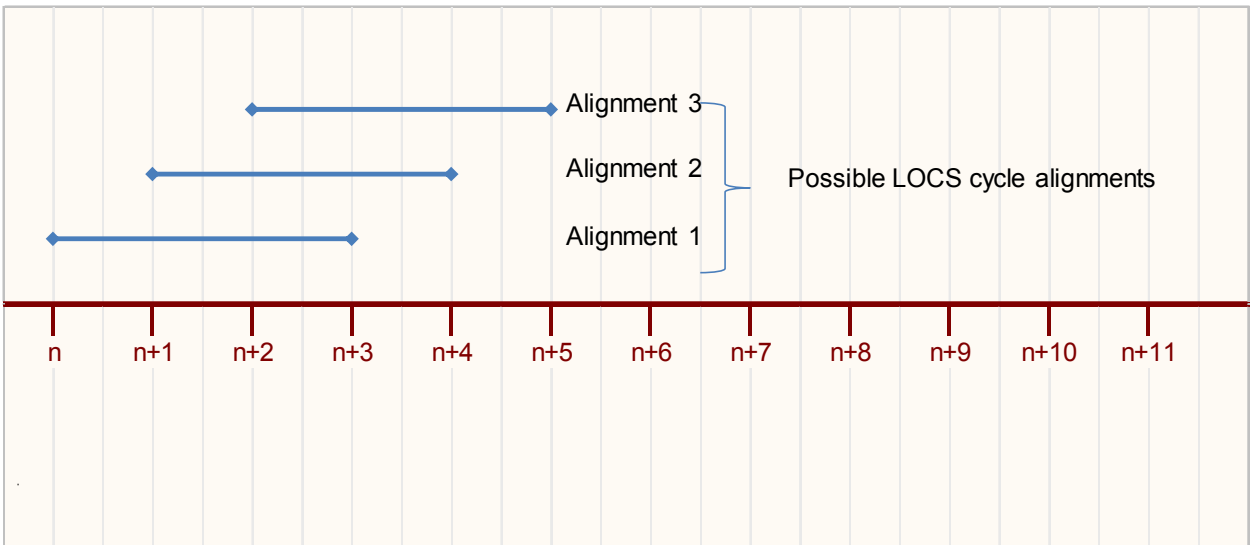


Figure 8-1 Relationship between LOCS cycle and host computer cycle

In alignment 1, the LOCS cycle starts somewhere in the interval [*n*, *n+1*) of the host computer cycle. Assuming that LOCS samples the channel values near the beginning of its cycle, the sampled values will be those at records *n*, *n*+3, *n*+6, etc. (Recall that the output file contains one record per host computer cycle). Similarly, for alignment 2, the values that LOCS samples are those at records *n*+1, *n*+4, *n*+7, etc. If a trip condition exists for only one host computer cycle (i.e., at only one output record), then depending on the alignment, LOCS may completely miss that record. For each alignment, let A_i be the first record that is read by LOCS (assuming its cycle has alignment *i*) that is in a trip condition. The latest time at which LOCS should read the trip condition is $\max_i A_i, i \in \{1,2,3\}$. Similarly, the earliest time at which LOCS can read the trip condition is $\min_i A_i$.

After LOCS reads the trip record, it is expected that a trip status will be output at the end of that cycle (i.e., in 0.3 s). In addition, it may take the host computer up to one cycle (i.e., 0.1 s) to read and write the trip status to the output file. Therefore, a total of 0.4 s (corresponding to 4 host computer cycles) may elapse from the time that a trip condition is seen by LOCS to the time that the trip status is recorded.

From the above discussions, the overall predicted trip window for a parameter (temperature, flow rate, pressure) is $[\min_i A_i, 4 + \max_i A_i]$, where A_i is the first trip record read by LOCS assuming that it as alignment *i*. In total, there are four physical parameters that are monitored by LOCS: IPT inlet flow, IPT inlet pressure, and IPT inlet and outlet temperatures. Each of these parameters will have an associated predicted trip window. The predicted trip window that is used for the analyses described in this section is the minimum of these windows: $[\min_j \min_i A_i^j, 4 + \min_j \max_i A_i^j]$, where A_i^j is the first trip record assuming alignment *i* for physical parameter *j*.

8.1.2 Determination of Actual Trip Time

The output file for each case from INL contains the time, record number, and the trip status of each of the three scram channels. This information is read and the time that 2 out of 3 channels indicate a trip is recorded.

8.2 ATR LOCS Testing Results

In this section, the output files of the tests were evaluated based on the criterion described in Section 8.1, and the anomalies are discussed.

Figure 8-2[21] shows the distribution of the difference between the actual trip record number and the predicted trip window (each record corresponds to 0.1 s). Suppose r_{actual} is the actual trip record number and $[r_{min}, r_{max}]$ is the predicted trip window, then the deviation of the actual trip record from the predicted trip window is

[21] The histogram has the following properties: (1) The bins for the histogram include points in the [lower limit, upper limit) interval (i.e., the lower limit cases are included in the bin, but the upper limit cases are not); (2) The edge bins contain cases with values exceeding the scale. For example, the 43 cases in the [-10,-9) bin contain some with values less than -10.

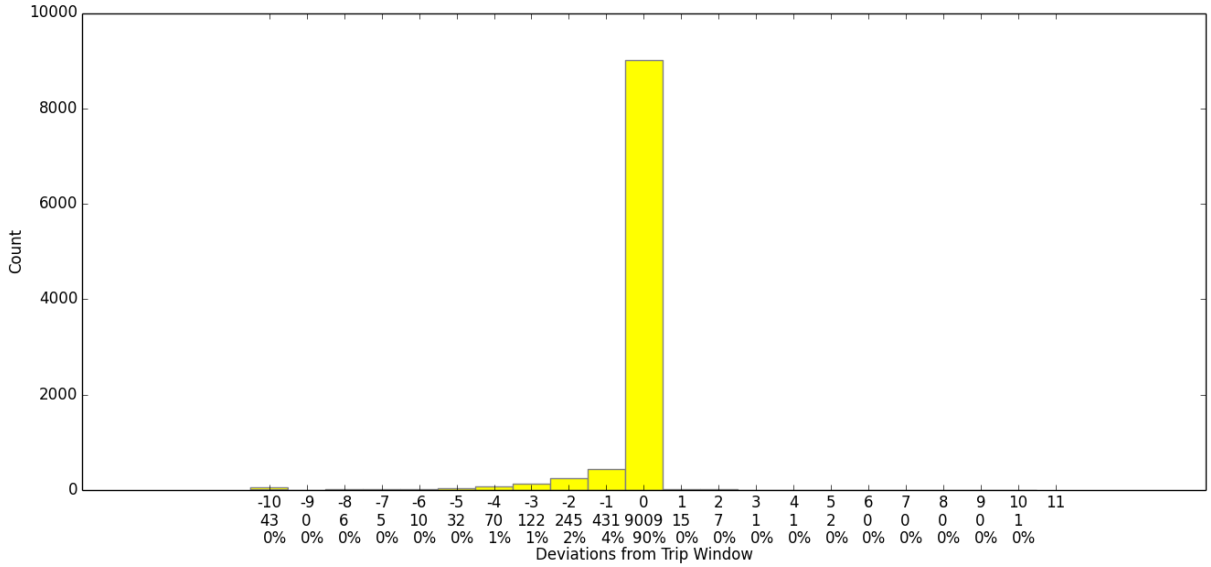


Figure 8-2 Distribution of the deviation of the actual trip record from the predicted trip window

Figure 8-2 shows that about 90% of the cases tripped within the expected trip window while about 10% tripped before the expected window (i.e., early trip). There are 27 cases that tripped after the expected window with the largest delay being 12 records (1.2 s). Tables 8-2 and 8-3 show the delayed and early trip counts breakdown in more detail.

Table 8-2 Delayed Trips.

Delay (s)	Count
(0,0.5]	26
(0.5,1.0]	0
(1.0,1.5]	1
(1.5,∞)	0
Total	27

Table 8-3 Early Trips.

Delay (s)	Count
(-∞,-5)	0
[-5,-4)	3
[-4,-3)	4
[-3,-2)	16
[-2,-1)	19
[-1,0)	922
Total	964

Table 8-4 summarizes the above observations and several anomalies that were observed

during the analysis. During the initial run of the 10,000 samples, one case (RF_316, representing failure of the secondary loop pump) failed to trip even though the sensor readings clearly exceeded the trip setpoint. To investigate this case further, it was rerun an additional 100 times; however, none of the reruns resulted in a trip failure. From the discussion with INL, it is believed that there could have been a problem with the initial test setup that led to the trip failure. Nevertheless, the one trip failure is included in Table 8-4 for completeness but for subsequent analyses, this case will not be considered as a failure.

From inspecting the early trip cases, it appears that all trips initiated by the TT-32 channels (IPT outlet temperature) are early trip. Although the nominal trip setpoint for TT-32 is 570 ^{o}F, the trip actually occurred around 569.5 ^{o}F, based on examination of the output files. Therefore, scenarios where there is large delay from the time the temperature first reached 569.5 ^{o}F to the time it crossed 570 ^{o}F will be counted as early trip.

There are 44 cases where the outputs from LOCS indicate a trip condition for only one record. Since the LOCS cycle is 0.3 s, the expectation is that a minimum of two records should indicate a trip condition. On inspecting the input file for some of these cases, it was found that the mass flow rate dropped to below the trip setpoint rapidly (in 0.1 s) and recovered the next record. To gain better understanding of these cases, LI_496, LI_5472, and LO_FO_HO_TV_2994 have been examined in detail. It was found out that the sudden reduction of the flow rate is caused by a sudden valve opening (simulation a small pipe break) or a sudden reduction of flow area of the flow control valve (simulating flow blockage). RELAP5 has been rerun for the three cases with very small time step size of 0.001 s (original cases were run with $\Delta T = 0.01$ s) to see if the predictions are reasonable. The new results show the same behavior as the originals. This indicates that the sudden reduction of the flow rate a result of the sudden change of flow condition and it is physically reasonable flow behavior.

It was also observed that there are 398 cases where the three DCS outputs do not agree. (Recall that there are outputs from the DCS and they should agree in the ideal case. A 2-of-3 trip status on the outputs causes system to trip). However, they are not considered to be a failure and are included in the table for completeness.

Table 8-4 Summary of cases with anomalies.

Category	Number of Cases	Notes
1. Delayed trips	27	In these events, the LOCS generated a trip signal later than expected. For these cases, the sensor readings oscillated near the setpoint for a prolonged period. Either noise or a LOCS cycle that isn't exactly 0.3 s may contribute to the delay. The delayed trips did not exceed the channel response time requirement.
2. Early trips	964	These trips occurred when the input signals were close to the threshold without meeting the 2-out-of-3 logic. A possible explanation is that, either the testing hardware or LOCS itself may have introduced noise that satisfied the 2-out-of-3 logic earlier than expected.
3. Failures to Trip	0	Case "RF_316" (failure of secondary pump) was originally a failure case in which no trip signal was generated while the input signals exceeded the threshold for a long time. However, this failure cannot be reproduced.
4. Trip lasting only one record	44	These are cases where the output file shows a trip lasting for only one record. Although it is expected that a trip should last for at least two records (since LOCS cycle is 0.3 s), the one-record trip is counted as a valid trip.
5. Three output channels do not change to a trip state at the same time step.	398	These are not failure events. However, they are unexpected, because once the LOCS decides that a trip signal should be generated, it sends the same signal to the 3 channels.

To explore possible reasons for the delayed an early trip, one case from each category is analyzed in detailed below. Generally, these observations also hold true for other cases that are either early or delayed trip.

A. Delayed Trip

The case LO_FO_HO_TV_2994 (loss of the remote processing units) results in a trip delay of 12 records (1.2 s). Note that this case has the largest delay among the 10,000 cases. The graph of the inlet flow rate channels is shown in Figure 8-3. The actual trip record is 733 but the predicted trip window is [2, 721]. Note that from the graph, the flow rate channels B and C dropped below the setpoint briefly (for 1 record) around record 710. Ideally, a trip should occur near that time. However, since the condition only lasted 1 record, it may not be read by the LOCS. In this particular case, there are multiple single records that exceeded the setpoint and through manual examination of the results each of the 3 possible alignments should have read at least one such record. Therefore, a low flow trip is expected but did not occur. One possible explanation of the failure to trip is that noise was present so that the flow value slightly lower

than 25 gpm did not register as a trip-level reading.

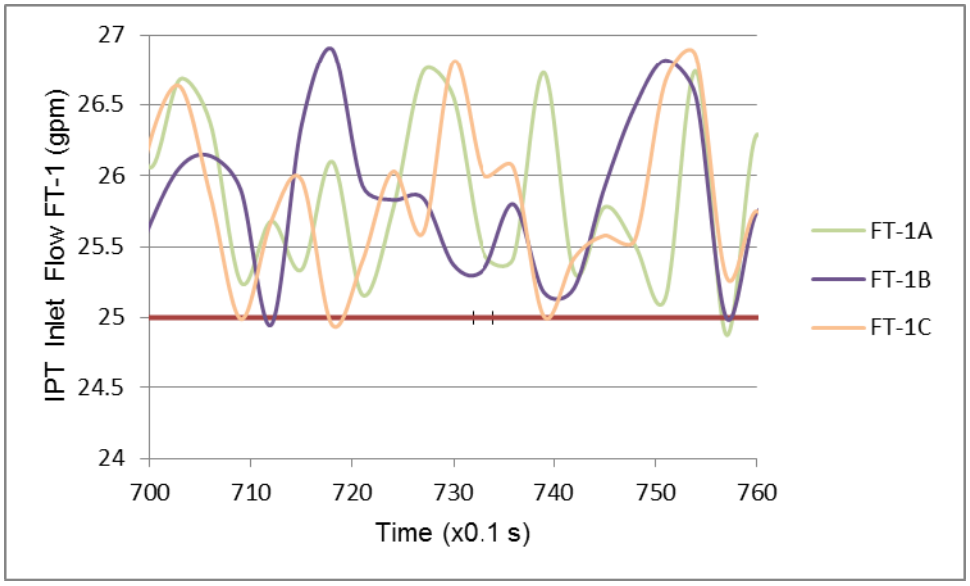


Figure 8-3 LO_FO_HO_TV_2994 is an example of a delayed trip case.

The actual trip occurred at record 733 due to low pressure, but the predicted trip window for low inlet flow is [2, 721]. In this case, the low *pressure* trip signal was generated in a time frame consistent with the expected trip window for this parameter. Therefore, LOCS did not generate a trip on low inlet flow (as initially expected), but instead generated a trip signal on low pressure. Therefore, this is not considered to be a delayed trip on low flow, and highlights the importance of defining the trip window.

Note that using the channel response time criterion (described earlier in Section 2.8), and assuming that the criterion is only applicable for cases when the threshold is exceeded for at least one LOCS cycle (3 records), then this case is not considered a delayed trip. (A low flow trip condition did not least 3 consecutive records.) As indicated, the actual low pressure trip occurred at record 733. At record 731, 2 out of 3 pressure channels exceeded the threshold. This continued to records 732 and 733. Therefore, if we used the channel response time, we expect a trip to occur before record 731+7 (the 7 is from 0.78 s stated in the required response time) = 738. Similarly, for other delayed trip cases in Table 8-2, the channel response time was not exceeded.

B. Early trip

Case HI_217 (line heater control failure) is an example of a case where the actual trip occurred before the predicted trip. Figure 8-4 shows an IPT outlet temperature channel near the time of the trip. It is noted that at the time of the actual trip, the temperature came to within 0.1^{o}F of the setpoint. Although, from the trip window criterion defined earlier is not satisfied, it is possible that noise may be high enough in the system to push the input values to above the setpoint.

This would cause a discrepancy between the predicted and actual trip records, especially in cases where the parameters oscillate rapidly during the time of the trip.

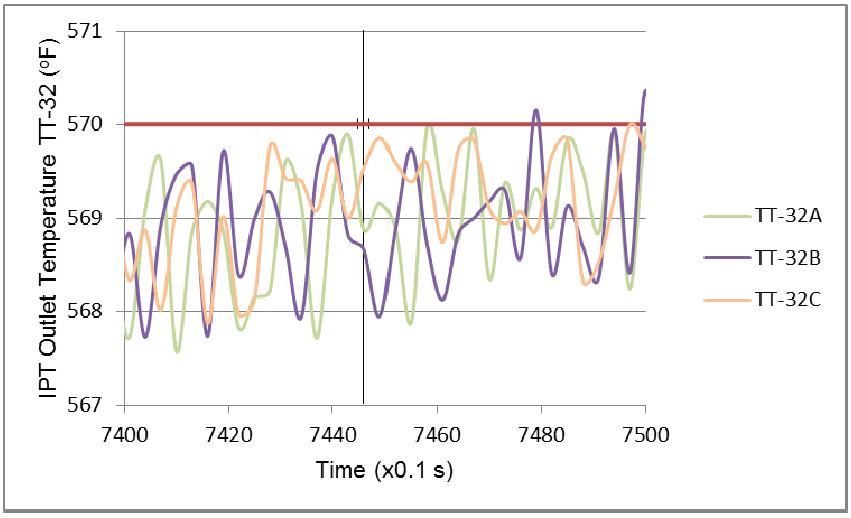


Figure 8-4 HI_217 is an example of an early trip case.

The actual trip occurred at record 7446 but the predicted trip window is [7492, 7510], resulting in a 46 records early trip.

8.3 Reproducibility of the Test Cases

Due to observation of one failed test and many other anomalies, after discussion with INL, it was agreed that some of the test cases be rerun to test the reproducibility of the anomalies. These additional runs are discussed in this section. One reason that the cases are not exactly reproducible is that the LOCS and the test computer are not synchronized and thus each rerun of a case may start with a different input record being read by the LOCS.

The failure of LOCS to trip in RF_316 was unexpected. One possible explanation was that RF_316 was simulated differently than other cases. It belongs to a subset of the group 1 test runs that was done differently from other test runs. In this case the output files contain the identity of the channel. Writing the channel identity to the output file added 1 ms delay for every record. Although this delay, which is cumulative, was corrected during the analysis of the outputs, there was a concern that there may be other anomalies associated with this group that remained. It is also possible to be caused by transient hardware failures. Therefore, all cases in this group were rerun using the procedure that is the same as other cases (i.e., without the trip channel written). The results discussed in Section 8.2 reflect the reruns. The rerun also presented an opportunity to test the reproducibility of the actual trip time/record. In addition, the RF_316 case (trip failure case) was rerun 100 times.

Table 8-5 summarizes the cases that were rerun and presents the results. For case RF_316, no trip was generated in the original run even though the expected trip window was [17735, 17741]. This case was run 100 times in the follow-up but in all these runs, the trip occurred at

either record 17737 or 17738. As seen in Table 8-5, there was no case where a trip failed to be generated in the rerun.

Table 8-5 shows the variability of the actual trip record for the rerun cases. In most scenarios, the trip occurs relatively consistently at the same record number. However, there was some observed variability. For example, in RF_PT_LO_FO_HO_TV_9696, the trip record varied by as much as 19 records (1.9 seconds). This amount of variability can be explained in terms of the difference in alignment. If a trip condition exists for only one record (i.e., if the sensor values recover quickly) as in a case when there is large oscillations in sensor readings, then only one alignment of the LOCS cycle may capture that trip. Electronic noise associated with the same may also cause an early trip if the sensor readings are very close to (but not yet reach) the trip setpoint. In these cases, although the predicted trip will occur later, noise may add a positive (for temperature channels) number to the sensor reading which cause LOCS to see the input as a trip state. Since in most cases, noise can be considered random, the actual trip record will be different from run to run, especially for cases where the sensor readings hover near the trip setpoint for a long time.

In general, the criterion used in this section to specify the predicted trip window assumes that (1) the LOCS cycle is exactly 0.3 s, and (2) the LOCS cycle is constant. When these criteria are not satisfied, it is conceivable that the actual trip record may occur outside the window. Together with system noise, these issues are believed to be responsible for the observed cases of trips not occurring inside the window. In any case, the largest observed delayed trip is within INL's stated margin of 5 s[22].

Table 8-5 Distribution of the actual trip record for the cases that were rerun.

Case	Actual Trip Record	Number of Run with Indicated Actual Trip Record	Expected Trip Window
LI_5472 (pipe break)	4	7	[2, 417]
	5	1	
	409	2	
LO_9360 (failure of analog input module 1A3)	3348	13	[3354, 3381]
	3349	3	
	3360	1	
	3363	3	
RF_316 (failure of secondary loop pump)	17737	1	[11735, 11741]
	17738	99	
RF_9075 (plugging of flow element FE-4-2)	7679	15	[7664, 7679]
	7680	5	
RF_PT_LO_FO_HO_TV_9696 (loss of power to 4.16 kV commercial bus A)	54	15	[39, 71]
	69	1	
	70	3	

[22] INL personnel stated during a telephone conference with BNL that their criterion for a successful trip is for a trip to occur within 5 s after 2-of-3 channels reached the trip setpoint.

9. ESTIMATION OF SOFTWARE PROBABILITY OF FAILURE ON DEMAND

A Bayesian approach was used in this study to estimate the probability of software failure on demand using the test results of zero failure in 10,000 tests. The following provides the mathematics of the Bayesian approach that is a straightforward application of Bayes' theorem. The likelihood function is a binomial distribution, and a conjugate beta prior distribution is used to obtain a beta posterior distribution.

Let Θ be the random variable representing an analyst's knowledge of the unknown probability θ before testing. The prior distribution of Θ is assumed to follow a *Beta*(*a*,*b*) distribution. Thus, the probability density function (pdf) of Θ is

$$f(\theta) = \frac{\theta^{a-1}(1-\theta)^{b-1}}{B(a,b)} \tag{9-1}$$

where $0 \le \theta \le 1$, $a > 0$, $b > 0$, and the normalizing constant $B(a,b)$ is the complete beta function. The expected value of Θ is $a/(a+b)$.

In Bayesian terminology, $f(\theta)$ is the prior pdf of Θ, and $g(x|\theta)$ is the likelihood function of X, conditioned on the value of Θ (i.e. a Binomial distribution). The posterior pdf of Θ, conditioned on the observed (after n tests) value of X, is denoted by $f(\theta|x)$. According to Bayes' theorem, the posterior pdf of Θ, given the observed value x, is

$$f(\theta \mid x) = \frac{g(x \mid \theta) f(\theta)}{\int_0^1 g(x \mid \theta) f(\theta) d\theta} \tag{9-2}$$

Accordingly,

$$f(\theta \mid x) = \frac{\theta^{x+a-1}(1-\theta)^{n-x+b-1}}{B(x+a, n-x+b)} \tag{9-3}$$

Where $x = 0, 1, \ldots, n$, and $0 \le \theta \le 1$.

In other words, the posterior (after testing) distribution of Θ is Beta($x+a$, $n-x+b$), where x is the number of failures observed in n tests, and a and b are the parameters of the prior Θ distribution. The posterior distribution has a mean of

$$\frac{(a+x)}{(a+b+n)} \tag{9-4}$$

The Bayesian approach also can generate an upper bound of the software failure probability θ, θ_u. To do so, a confidence level γ is specified that implicitly defines the upper bound of θ_u such that

$$Pr\{\Theta \le \theta_u \mid x\} = \gamma \tag{9-5}$$

Solving this equation for θ_u determines an interval $0 \le \Theta \le \theta_u$, in which Θ lies with confidence γ. For example, if $\gamma = 0.95$, an analyst is 95% confident that the value of Θ lies in the interval $0 \le \Theta \le \theta_u$.

An interesting application of this upper bound approach is setting the parameters $a = b = 1$ for the prior probability density function because this function becomes the uniform distribution (i.e., $f(\theta)$ is a constant) that can be interpreted as a non-informative prior distribution [Martz 1982]. (Another choice of prior distribution is possible; for example, the handbook on parameter estimation [Atwood 2002] recommended employing a Jeffreys prior distribution.) In addition, by making $x = 0$ (i.e., assuming there is no observed failure), as often is the case in testing safety-critical software, the posterior cumulative distribution function is expressed as

$$F(\theta_u \mid x) = \Pr\{\Theta \le \theta_u \mid x\} = \int_0^{\theta_u} f(\theta \mid x) d\theta \tag{9-6}$$

which reduces to

$$F(\theta_u \mid 0) = 1 - (1 - \theta_u)^{n+1} = \gamma \tag{9-7}$$

Solving this equation for θ_u:

$$\theta_u = 1 - (1 - \gamma)^{1/(n+1)} \tag{9-8}$$

The number of successful tests required to show that the failure probability bounded by θ_u at confidence level γ is obtained from Equation (9-8):

$$n = \frac{\ln(1-\gamma)}{\ln(1-\theta_u)} - 1 \tag{9-9}$$

Using the Bayesian approach above with the parameters $a = b = 1$ for the prior probability density function (a uniform distribution), the posterior distribution for the software failure on demand is *Beta*(1,10001), with a mean failure probability of 1/10002~$1*10^{-4}$ (Equation 9-4). The 5th and 95th percentiles of the *Beta* distribution are, respectively, $5*10^{-6}$and $3*10^{-4}$.

Similarly, considering the 27 delayed trips[23] with the largest delay less than 2 seconds, the probability of a delayed trip is given by *Beta*(28,9974) with its mean value equal to ~ $3*10^{-3}$ and the 5th and 95th percentiles equal to $2*10^{-3}$and $3.7*10^{-3}$, respectively. The probability of a delay trip is still lower than the probability of LOCS hardware failure of $7.2*10^{-3}$ (See Table 4-3).

[23] As discussed previously, the delay trips may not exceed the channel response time requirement. Assuming they are failures is conservative.

10. CONCLUSIONS AND INSIGHTS

Accomplishments and Conclusions

In this study, a statistical software testing approach was developed and applied to the loop operating control system (LOCS) of the Advanced Test Reactor (ATR) at Idaho National Laboratory (INL). Since the tests were performed with the actual LOCS, they also serve as tests of the hardware and the interactions between hardware and software. The application used the reactor's probabilistic risk assessment (PRA) to define the testing environment, and the thermal-hydraulic model to simulate the experiment loop conditions which are inputs to the LOCS. A test configuration was established to execute test cases generated from the thermal-hydraulic simulation. 13 probabilistic failure models were developed to capture the variability of the failure effects and specify the exact scenarios to be simulated using the RELAP5 model. The test output from the LOCS were evaluated to determine if a trip signal was generated in time, considering the cycle times of the LOCS and the test's host computer. One failure was initially observed among a total of 10,000 test cases representing different reactivity insertion accidents that were performed. The failure was not reproducible in subsequent 100 reruns of the same case and thus no longer considered a failure. The test results were used in estimating the probability of failure of the software on demand. Additional anomalies of the tests were identified and possibly explanations were provided. For example, in 27 cases, the trip signal was generated with a delay of up to 1.2 seconds. They can possibly be explained by noises. In addition, for the longest delay case, the trip timing was not inconsistent with the expected channel response time.

In addition, the PRA was used to determine the importance of the LOCS in terms of the total core damage frequency. The PRA results shows that the LOCS system reliability based on statistical testing results is consistent with its stated reliability goal of 1E-04 [INL 2008]. However, for the purpose of demonstrating that the LOCS system is a minor contributor to core damage frequency, the system could be tested to a lower reliability target based on the context in which it is used. The main reason of the low contribution is the plant protection system always serves as backup to the LOCS.

Theoretically, the suggestion by earlier researchers that quantification of system level failure probability may optimistic is considered resolved based on (1) the quantification is effectively using data collected from operating experience and (2) earlier researchers were not able to properly account for the overlap in software execution paths during testing.

There are many issues associated with simplifying assumptions and realism of the study that, in principle, can be resolved; they are discussed below. The lessons learned associated with the issues also are briefly described.

Simplifications, assumptions, and lessons learned

Statistical testing attempts to simulate the actual demand on the system and use the results in estimating the software failure probability. It is very important that the simulation is realistic. However, there are practical limitations on the PRA model, the RELAP5 model, and the test configurations. These limitations and the lessons learned from them are discussed below with more detailed discussions provided in earlier sections. The limitations are common to

engineering analyses but impose practical difficulties in the study. They can be overcome with better engineering work.

1. Fault tree modeling is not commonly accepted for modeling digital systems.

Modeling digital systems for PRA purposes has been a subject of research sponsored by the NRC. However, due to the many unique attributes of digital systems, several challenges to modeling and data collection exist, and there is no consensus on how the reliability models should be developed [NRC 2008]. For example, it remains unclear whether or not a fault tree model adequately captures all dependencies. How software failures should be included in a reliability model also remains to be investigated. Under the NRC's sponsorship, BNL developed a simulation based a modeling method [Chu 2009] that is better in representing the detailed design of digital systems. However, it has not yet been commonly accepted.

In this study, the fault tree model of the ATR PRA was modified and used in defining the cases used in testing.

2. Fault tree modeling of both the control and protection functions of the LOCS highlights the importance of accounting for the dependency and consistency of the two models.

Because the LOCS performs control functions and protection functions, failures associated with control functions may lead to reactivity insertion accidents that may be mitigated by the protection functions of the same system. Two fault trees had to be modeled in the ATR PRA, one modeling the reactivity insertion events caused by equipment failures of the experiment loop including the LOCS, the other models the LOCS's protection functions that would generate a reactor trip signal in different scenarios. BNL made changes to the original ATR PRA model to better account for this dependency and the consistency of the two models. For example, failures of distributed processing units (DPUs) were added to the fault tree that models reactivity insertion events.

3. Probabilistic failure models that capture the variability of failure effects of PRA-defined scenarios had to be developed, subject to the simplifications of the RELAP5 model.

The need to develop the 13 reliability failure models arose because the PRA model only specifies the failure events at a higher level without the specifics needed in a RELAP5 simulation of the failure events. The RELAP5 simulation done in this study uses the probabilistic failure models to generate test cases and has to consider the variability represented by the probabilistic failure models (similar to what a dynamic PRA has to do). In general, a way of modeling the failure effects of each PRA modeled failure event must be developed. For example, for a LOCA, its size and location certainly can be varied.

Some of the probabilistic failure models used in this study have generic applicability. For example, for a pump trip, randomness was introduced to simulate the variation in the trip coastdown curve by multiplying it by a random number. In general, more engineering analyses of pump coastdown and additional collections of failure experience may improve the model. In addition, some probabilistic failure models were developed to accommodate the simplified RELAP5 model. For example, due to lack of modeling of the secondary side of the experiment loop, a probabilistic failure model was developed to represent all those failure events associated with the secondary side by varying the heat-transfer coefficient at the interface with the

secondary side. Using such a probabilistic failure model can be avoided if the secondary side is added to the RELAP5 model.

4. The RELAP5 simulation was done with a simplified, incomplete control model of the LOCS.

This issue again is related to the fact that the LOCS performs both control and protection functions. The RELAP5 model of the experiment loop only models some of the control functions of the LOCS in a simplified way (i.e., without using the real LOCS), while the PRA model has scenarios involving failures of some of the LOCS components. It was decided that changing the RELAP5 model of the control functions to simulate the failure events was not possible. Instead, the failure effects were simulated by simplified means. For example, for those failures associated with flow control, the flow through a flow control valve was varied by changing its flow area. For failures of pressure sensors, a break in the loop was used to simulate the effects because pressure control is not modeled in the RELAP5 model.

5. The RELAP5 model could be further enhanced to refine statistical testing results.

The preceding discussions already cover some of the limitations imposed by the simplified RELAP5 model used in this study. They are related to the scope and level of detail of the modeling, and in general, can be improved within the state-of-the-art. In addition, a thermal-hydraulic model typically does not model redundant sensors. In this study, a single sensor value at a node was modified by adding noise to the value such that redundant sensors would produce somewhat different values. A more general question centers on how far to go in modeling to make it more realistic. For example, the experiment loop has a secondary and a tertiary system that is further cooled by water from a lake or river that is cooled by the atmosphere. It may not be necessary to consider the effects of the weather which is changing all the time. A basic requirement is probably being able to model the specific effects of what is modeled in the PRA.

6. The test configuration used some simplifying approaches for several control functions of the LOCS.

The test configuration used in the study was intended to simulate the condition that the LOCS being tested experiences in the field. A few deviations from the real condition are described below:

- In the test configuration, a smaller set of input and output signals were used compared to the hundreds of signals in the real situation. Those signals associated with the control functions of the LOCS were assumed to have no effect on the signals used by the protection functions and were assigned dummy values such that their processing by the LOCS does not significantly affect the timing of the processing of the signals for protection functions. This was done to reduce the number of I/O modules needed for this study.

- The inputs to the LOCS were supplied by a host computer which periodically (with a cycle time of 0.1 second) sends the RELAP5-generated signal values to the LOCS, as opposed to the real sensor inputs that constantly change. The cycle time of the host computer was selected such that it can supply input records at a rate significantly faster than the rate that the LOCS is reading its inputs with a cycle time of 0.3 second. This cycle time in turn determines the time step of 0.1 second used in the RELAP5 simulation...

7. Test outputs were evaluated using an estimated time window in which a trip signal is expected.

The time window in which a trip signal should be generated was estimated based on the timing of the input records and the estimated cycle times of the test computer and the LOCS. That is, a test is considered a success if the trip signal is generated in the time window. This represents a realistic way of evaluating the test results. One reason for using the time window approach is it allows us to consider the detailed timing associated with the cycle times and better explains the test results. In this approach, we did not consider the 5 second delay that may be introduced by the watchdog timer upon failure of the DPUs. Allowing the delay would make the time window approximately 5 second longer.

8. Observation of a failed test was a surprise that we still do not have a good explanation. An attempt to reproduce the failure by re-running the case 100 time was not successful. Reruns of the cases in general produced results that are similar to those of the original runs. Inability to reproduce the test results exactly can be partially explained by the fact that the LOCS and the test computer are not synchronized and each has one's cycle time. Other possible explanations such as noises were postulated. In general, the irreproducibility is related to software hardware interaction and may need to be further explored.

Follow on research

- This study was limited by its RELAP5 and PRA models' capability in supporting the statistical testing method (STM). A more realistic application would be that of a RPS or ESFAS of a nuclear power plant with good models. Use of the NRC's TELEPERM platform, with Software from Oconee is one possibility. Other plants with FPGA systems also are possible.

- Lessons learned from this study can be used to enhance the approach on statistical testing, such that some of the issues that were not addressed in this study can be in the future. Guidance on how to perform statistical testing for quantifying the failure probabilities of software can be developed.

- In this study, we resolved the issue that the quantification of the black-box testing results may be overly optimistic. How to use white-box testing results in quantifying software reliability is an issue that deserves additional research to explore its potential benefits (i.e., use of structure information) over the black-box method.[24]

- Development of risk-informed guidance for determining required testing requirements NUREG/CR-7044 developed an approach for determining the number of tests needed to demonstrate that a software program does not contribute significantly to the risks of a nuclear power plant. This study demonstrated its usefulness by showing that, for a non-risk-significant digital system, the needed tests may not be extensive. The same approach can be used to determine or allocate the required licensing requirements of digital protection systems/functions based on risk considerations.

[24] Zhang [2004] developed an approach that accounts for the paths in a software and concluded that it is not possible to exhaustively consider all possible paths.

11. REFERENCES

[Aldemir 2006] Aldemir, T., et al., "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," NUREG/CR-6901, February 2006.

[Aldemir 2007] Aldemir, T., et al., "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, October 2007.

[Aldemir 2009] Aldemir, T., et al., "A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems," NUREG/CR-6985, February 2009.

[Atwood 2002] Atwood, C.L., et al., "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, November 2002.

[Chu 2008] Chu, T.L., et al., "Traditional Probabilistic Risk Assessment Methods for Digital Systems," NUREG/CR-6962, October 2008.

[Chu 2009a] Chu, T.L., et al., "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods," NUREG/CR-6997, September 2009.

[Chu 2009b] Chu, T.L., et al., "Workshop on Philosophical Basis for Incorporating Software Failures into a Probabilistic Risk Assessment," Brookhaven National Laboratory, Technical Report, BNL-90571-2009-IR, November 2009.

[Chu 2010] Chu, T.L., et al., "Review Of Quantitative Software Reliability Methods," Brookhaven National Laboratory, BNL-94047-2010, September 2010.

[Chu 2013] Chu, T. L., Yue, M., Martinez-Guridi, G., and Lehner, J., "Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants," NUREG/CR-7044, October 2013.

[IEC 61508] International Electrotechnical Commission, "Function Safety of Electrical/Electronic/Programmable Safety-Related Systems," Parts 1-7, IEC 61508, various dates.

[IEEE 610] Institute of Electrical and Electronics Engineers (IEEE), "Systems and software engineering Vocabulary," IEEE Standard 610-2010, December 15, 2010.

[IEEE 1633] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Recommended Practice on Software Reliability," IEEE Standard 1633-2008, March 27, 2008.

[Jones 2001] Jones, E., Oliphant, T., et. al., "SciPy: Open Source Scientific Tools for Python," http://www.scipy.org/ (2001).

[INL 2008] Idaho National Laboratory (INL), “ATR Loop Operating Control System,” System Design Description, SDD-7.9.20, Rev., 8, April 22, 2008.

[INL 2009] Idaho National Laboratory, “FY 2009 Advanced Test Reactor National Scientific User Facility Users’ Guide,” INL/EXT-08-14709, 2009.

[INL 2010] Idaho, National Laboratory, “Technical and Functional Requirements, 2A Loop Instrumentation and Operating Control System”, TFR-499, Rev. 3, March 2, 2010.

[Kaser 2012] Kaser, T.G., and Marts, G.A., “ATR Pressurized Water Loop 2A RELAP Inputs and Control System Simulation Information,” INL/MIS 12-27669, November 2012.

[Korsah 2010] Korsah, K., et al., “An Investigation of Digital Instrumentation and Control System Failure Modes,” Oak Ridge National Laboratory, ORNL/TM-2010/32, March 2010.

[Kuball 2004] Kuball, S., and May, J., “Test-Adequacy and Statistical Testing: Combining Different Properties of a Test-Set,” Proceedings of the 15th International Symposium on Software Reliability Engineering (ISSRE’04).

[Labview] National Instruments, “LabVIEW System Design Software.”

[Lyu 1996] Lyu, M.R., Editor in Chief, Handbook of Software Reliability Engineering, McGraw-Hill, 1996.

[Marts 2012] Marts, G.A., “ATR Pressurized Water Loop 2A Operating Control System Information,” Idaho National Laboratory, INL/MIS-12-27637, October 2012.

[Martz 1982] Martz, H. F., and Waller, R.A., *Bayesian Reliability Analysis*, John Wiley & Sons, Inc., 1982.

[May 1995] May, J., Hughes, G., and Lunn, A.D., “Reliability Estimation from Appropriate Testing of Plant Protection Software,” *Software Engineering Journal*, November 1995.

[Miller 1992] Miller, K.W., et al., “Estimating the Probability of Failure When Testing Reveals No Failures,” *IEEE Transactions on Software Engineering*, Vol. 18, No. 1, January 1992.

[NEA 2009] Nuclear Energy Agency, “Recommendations On Assessing Digital System Reliability In Probabilistic Risk Assessments Of Nuclear Power Plants,” NEA/CSNI/R(2009)18, December 17, 2009.

[NRC 1995a] USNRC, “Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities,” Final Policy Statement, August 16, 1995.

[NRC 1995] U.S. Nuclear Regulatory Commission,” RELAP5/MOD3 Code Manual,” NUREG/CR-5535, August 1995.

[NRC 2008] USNRC, “Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessment,” Interim Staff Guidance, DI&C-ISG-03, August 11, 2008.

[NRC 2010a] USNRC, “NRC Digital System Research Plan FY2010-FY2014,” February 2010.

[NRC 2011] U.S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 2, May 2011.

[Rossum] Rossum, Guido van, et al, “The Python Language Reference”, Python Software Foundation, https://docs.python.org/3/reference/index.html.

[Smith 2000] Smith, C.L., et al., “Testing, Verifying, and Validating SAPHIRE Versions 6.0 and 7.0,” NUREG/CR-668, October 2000.

[Wood 2012] Wood, R. T., et al., “Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants,” Oak Ridge National Laboratory, Letter Report LTR/NRC/RES/2012-001, February 2012.

[Zhang 2004] Zhang, Y., “Reliability Quantification of Nuclear Safety-Related Software,” Ph. D. Thesis, Department of Nuclear Engineering, Massachusetts Institute of Technology, February 2004.

Appendix A
TOP 200 CUTSETS OF RLHIE FAULT TREE

This appendix lists the 200 cutsets from which the test cases were sampled. They comprise about 99% of the total RLHIE frequency of 0.97 per year (i.e., they are responsible for 99% of the loop 2A-initiated reactivity insertion events). The first column contains the cutset number, while the second is the frequency of that particular cutset relative to the RLHIE total frequency. For instance, the first cutset is responsible for about 54% of the total RLHIE frequency. The third column lists the groups (Table 6-1) to which the cutset belongs. The cutset code used in the SAPHIRE7 model is shown in the fourth column. The last column describes the basic events. In these cutsets, the 365 day-to-year conversion factor and the plant availability factor are not shown since they were not used in generating the test cases.

#	Fraction	Group	Cut Set	Description
1	5.39E-01	gRFW130	RFW-MDP-FR-00MRBM35-0000	Motor-driven RFW pump MRB-M-35 fails to run
2	1.85E-01	gRFW130	ASW-AOV-FF-000FCV45-0000	Flow control valve FCV-4-5 fails to function
3	1.36E-01	gRFW130	ASW-STF-FF-0000FE42-0000	Flow element FE-4-2 fails (plugs)
4	2.95E-02	gFlow	EXT-SNR-PG-02ACT145-0000	Train 2A-C strainer 145 plugs
5	1.14E-02	gRFW130	DCS-DOM-FF-2NE2F1_A-0000	Digital output module 2NE-2F1 fails to function/operate
6	4.26E-03	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
7	4.00E-03	gPipe	EXT-HTR-FF-000002AC-0000	Pressurizer heaters fail to function
8	4.00E-03	gRFW130	RFW-ORF-PG-0000FE72-0000	Flow element FE-7-2 is plugged
9	3.62E-03	gPipe gPump gRFW130	CDP-TFM-FF-000MRBE4-0000	Service transformer MRB-A-4 (4160/480 V) fails to remain energized
10	3.62E-03	gPump	DGP-TFM-FF-000MRBE8-0000	Service transformer MRB-A-8 (4160/480 V) fails to remain energized
11	3.36E-03	gTctrlHI	EXT-STT-FF-02ACT402-0000	Train 2A-C temperature sensor (TE-40-2 Line heater outlet B) fails to indicate temperature
12	3.36E-03	gTctrlV	EXT-STT-FF-02ACT311-0000	Train 2A-C temperature sensor (TE-31-1 Mixing tee outlet A) fails to indicate temperature
13	3.29E-03	gPipe	EXT-STP-FF-02ACPT4A-0000	Train 2A-C pressure sensor (PT-4A) fails to indicate pressure

#	Fraction	Group	Cut Set	Description
14	2.91E-03	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
15	2.59E-03	gRFW130	RFW-HTX-PG-00MRBM33-0000	RFW heat exchanger MRB-M-33 plugged
16	2.26E-03	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
17	1.80E-03	gFctrlI	EXT-AIM-FF-002AC1A2-0000	Analog input module 1A2 (channel A - flow pressure temperature) fails to function
18	1.80E-03	gPipe	EXT-AIM-FF-002AC1A3-0000	Analog input module 1A3 (channel B - flow pressure temperature) fails to function
19	1.80E-03	gTctrlHI	EXT-AIM-FF-002AC1B3-0000	Analog control module 1B3 channel A fails to control line heaters
20	1.80E-03	gTctrlV	EXT-AIM-FF-002AC1E3-0000	Anal control module 1E3 fails to control temperature
21	1.80E-03	gRFW130	DCS-AIM-FF-001NE1A2-0000	High level analog input module 1NE-1A2 fails to function/operate
22	1.80E-03	gFctrlO gPipe gTctrlHO gTctrlV	DCS-AOM-FF-02AC1A7-0000	Analog output module 1A7 fails
23	1.78E-03	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
24	1.74E-03	gPump	DGP-BAC-FF-00MRBE20-0000	Failure of 480V diesel power panel MRB-A-20 to remain energized
25	1.74E-03	gPipe gPump	CDP-BAC-FF-002AE101-0000	Failure of 480 V MCC 2A-A-101 to remain energized
26	1.74E-03	gPump	DGP-BAC-FF-000MRBE3-0000	Diesel bus MRB-A-3 fails to remain energized
27	1.74E-03	gPump	DGP-BAC-FF-000MRBE9-0000	Failure of 480 V diesel bus MRB-A-9 to remain energized

#	Fraction	Group	Cut Set	Description
28	1.74E-03	gPump	DGP-BAC-FF-002AE102-0000	Failure of 480V MCC 2A-A-102 to remain energized
29	1.74E-03	gPipe gPump gRFW130	CDP-BAC-FF-000MRBE1-0000	Failure of 4160 V commercial bus A (MRB-A-1)
30	1.74E-03	gPipe gPump gRFW130	CDP-BAC-FF-000MRBE5-0000	Failure of 480 V commercial bus A (MRB-A-5)
31	1.37E-03	gFctrlO gPipe gTctrlHO gTctrlV	EXT-DPU-CF-000002AC-0000	Train 2A-C common cause DPU failure event
32	1.37E-03	gRFW130	DCS-DPU-CF-0001NE00-0000	Common cause failure of RPU 1NE DPUs
33	1.37E-03	gRFW130	DCS-DPU-CF-0002NE00-0000	Common cause failure of RPU 2NE DPUs
34	1.35E-03	gRFW130	IAS-PIP-AL-00IARUPT-0000	IAS piping rupture
35	1.21E-03	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
36	1.14E-03	gRFW130	DCS-DPU-FF-00013200-0000	RPU 1NE DPU-1-32 fails to function/operate
			DCS-DPU-FF-00013300-0000	RPU 1NE DPU-1-33 fails to function/operate
37	1.14E-03	gRFW130	DCS-DPU-FF-00013400-0000	RPU 2NE DPU-1-34 fails to function/operate
			DCS-DPU-FF-00013500-0000	RPU 2NE DPU-1-35 fails to function/operate
38	1.14E-03	gFctrlO gPipe gTctrlHO gTctrlV	EXT-DPU-FF-00002ACA-0000	Train 2A-C RPU DPU A fails to function
			EXT-DPU-FF-00002ACB-0000	Train 2A-C RPU DPU B fails to function
39	1.08E-03	gPipe	EXT-PIP-RU-02ACPIPE-0000	Train 2A-C pipe break
40	9.41E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
41	7.29E-04	gFCV1	EXT-AOV-SO-02ACFCV1-0000	Train 2A-C flow control valve FCV1 spuriously closes
42	7.29E-04	gTCV31	EXT-AOV-SO-2ACTCV31-0000	Train 2A-C temperature control valve TCV31 spuriously closes
43	7.29E-04	gRFW130	RFW-AOV-SC-00LCV72B-0000	LCV-7-2B spuriously closes
44	7.29E-04	gRFW130	RFW-AOV-SO-000PCV71-0000	PCV-7-1 spuriously opens
45	7.29E-04	gRFW130	RFW-AOV-SO-00LCV72B-0000	LCV-7-2B spuriously opens

#	Fraction	Group	Cut Set	Description
46	6.84E-04	gPump	DGP-CBK-SO-SBMRBE20-0000	Supply breaker to 480V power panel MRB-A-20 fails to remain closed
47	6.84E-04	gPipe gPump	CDP-CBK-SO-2AE1011A-0000	Breaker 2A-A-101-1A fails to remain closed
48	6.84E-04	gPipe gPump	CDP-CBK-SO-0MRBE5E3-0000	Breaker E3 from 480V commercial bus MRB-A-5 fails to remain closed
49	6.84E-04	gPump	DGP-CBK-SO-AE10210A-0000	Breaker 10A to 480V MCC 2A-A-102 fails to remain closed
50	6.84E-04	gPump	DGP-CBK-SO-0MRBE202-0000	Breaker E2 from 480V diesel power panel MRB-A-20 fails to remain closed
51	6.84E-04	gRFW130	CDP-CBK-SO-0000E5C4-0000	Breaker C4 from 480V commercial bus A MRB-A-5 fails to remain closed
52	6.84E-04	gPump	DGP-CBK-SO-0MRBE324-0000	Circuit breaker MRB-A-3-24 from 4160 V diesel bus MRB-A-3 fails open
53	6.84E-04	gPump	DGP-CBK-SO-0MRBE9B2-0000	Circ breaker B2 from 480V diesel bus MRB-A-9 fails to remain closed
54	6.84E-04	gPipe gPump gRFW130	CDP-CBK-SO-MRBE1007-0000	Circuit breaker 7 from 4.16 kV commercial bus A (MRB-A-1) fails open
55	6.84E-04	gRFW130	DCP-CBK-SO-MRBE4455-0000	Breaker 5 from panel MRB-A-445 fails open (no transfer attempt)
56	5.49E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
57	4.26E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
58	4.09E-04	gFlow	EXT-STF-FF-002ACFE1-0000	Train 2A-C FE1 flow element fails (plugs)
59	4.09E-04	gFlow	EXT-STF-FF-002ACFE2-0000	Train 2A-C FE2 flow element fails (plugs)
60	4.09E-04	gFctrlI	EXT-STF-FF-02ACFI1A-0000	Train 2A-C flow sensor (FI-1A) fails to indicate flow
61	4.09E-04	gRFW130	DCS-STL-FF-00LT0702-0000	LT-07-2 fails to function
62	4.05E-04	gRFW130	DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX

#	Fraction	Group	Cut Set	Description
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
63	3.88E-04	gTctrlV	EXT-STT-XM-02ACTALL-B000	Train 2A-C temperature sensor (TE-31-1) miscalibration
64	3.88E-04	gPipe	EXT-STT-XM-02ACPALL-0000	Train 2A-C pressure sensor (PI-2B) miscalibration
65	3.88E-04	gTctrlHI	EXT-STT-XM-02ACTALL-A000	Train 2A-C temperature sensor (TI-41) miscalibration
66	3.88E-04	gFctrlI	EXT-STT-XM-02ACFALL-0000	Train 2A-C flow sensor miscalibration
67	3.75E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
68	3.69E-04	gRFW130	DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
69	3.65E-04	gFctrlO gPipe gTctrlHO gTctrlV	EXT-DPU-FF-00002ACA-0000	Train 2A-C RPU DPU A fails to function
			EXT-DPU-FF-002ACDPU-0000	Train 2A-C RPU DPU fails to backover
			EXT-TMR-FF-02ACWTCD-OG00	Train 2A-C RPU watchdog timer fails to function
70	3.65E-04	gFctrlO gPipe gTctrlHO gTctrlV	EXT-DPU-FF-00002ACB-0000	Train 2A-C RPU DPU B fails to function
			EXT-DPU-FF-002ACDPU-0000	Train 2A-C RPU DPU fails to backover
			EXT-TMR-FF-02ACWTCD-OG00	Train 2A-C RPU watchdog timer fails to function
71	3.49E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
72	3.44E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate

#	Fraction	Group	Cut Set	Description
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
73	3.11E-04	gRFW130	DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
74	2.92E-04	gTctrlHI gTctrlV	EXT-STT-CF-02ACTI41-0000	Train 2A-C temperature sensor (TI-41) common cause event
75	2.91E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
76	2.85E-04	gPipe	EXT-STP-CF-002ACPI2-0000	Train 2A-C pressure sensor common cause event
77	2.56E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
78	2.42E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
79	2.40E-04	gRFW130	DCS-PSP-CF-0001NEC1-0000	Common cause failure of RPU 1NE Cabinet 1 power supplies (24 VDC)
80	2.40E-04	gRFW130	DCS-PSP-CF-0002NEC1-0000	Common cause failure of RPU 2NE Cabinet 1 power supplies (24 VDC)
81	2.35E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13

#	Fraction	Group	Cut Set	Description
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
82	1.92E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-TM-00MRBM43-POWR	Diesel MRB-M43 unavailable due to maintenance (power op)
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
83	1.85E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAC-FF-0MRBE117-0000	Failure of instrument UPS panel MRB-A-117 to remain energized
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
84	1.85E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
85	1.82E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
86	1.78E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
87	1.56E-04	gFctrlI gPipe gTctrlHI gTctrlV	EXT-AIM-CF-02AC1A23-4000	Train 2A-C analog input module common cause event
88	1.46E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running

#	Fraction	Group	Cut Set	Description
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
89	1.38E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-CBK-SO-0E116CB4-0000	Utility UPS MRB-A-116 output breaker CB4 fails open
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
90	1.31E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
91	1.31E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-TM-00MRBM43-POWR	Diesel MRB-M43 unavailable due to maintenance (power op)
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
92	1.28E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
93	1.07E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104

#	Fraction	Group	Cut Set	Description
94	1.02E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-TM-00MRBM43-POWR	Diesel MRB-M43 unavailable due to maintenance (power op)
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
95	1.01E-04	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
96	8.99E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
97	7.71E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAC-FF-0MRBE117-0000	Failure of instrument UPS panel MRB-A-117 to remain energized
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
98	7.71E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
99	7.28E-05	gPump	CDP-CBK-SO-0MRBE5D4-0000	Breaker D4 from 480V bus MRB-A-5 to instrument UPS MRB-A-104 fails open
			DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6

#	Fraction	Group	Cut Set	Description
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
100	7.28E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-CBK-SO-A117CB11-0000	Breaker CB11 from instr UPS panel MRB-A-117 fails to remain closed
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
101	7.28E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-CBK-SO-0E104CB1-0000	Breaker CB1 in instrument UPS MRB-A-104 fails open
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
102	7.28E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-CBK-SO-MRBE117M-0000	Main breaker to instrument UPS panel MRB-A-117 fails open
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
103	7.28E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-CBK-SO-0E116CB4-0000	Utility UPS MRB-A-116 output breaker CB4 fails open
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
104	6.94E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116

#	Fraction	Group	Cut Set	Description
105	5.76E-05	gRFW130	CDP-TFM-FF-000AEBT1-0000	Failure of transformer AEB-T-1 to remain energized
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
106	5.74E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-CBK-SO-0E116CB4-0000	Utility UPS MRB-A-116 output breaker CB4 fails open
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
107	5.69E-05	gRFW130	DCS-PSP-CF-0001NEAL-0000	Common cause failure of all RPU 1NE power supplies (24 VDC)
108	5.69E-05	gRFW130	DCS-PSP-CF-0002NEAL-0000	Common cause failure of all RPU 2NE power supplies (24 VDC)
109	5.49E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
110	5.47E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
111	5.33E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
112	4.67E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate

#	Fraction	Group	Cut Set	Description
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-TSW-SO-0000MTS1-0000	Manual transfer switch MTS-1 fails to remain closed
113	4.59E-05	gRFW130	DCS-OEI-FF-002NE100-0000	RPU 2NE OEI-1 fails to function/operate
			DCS-OEI-FF-002NE200-0000	RPU 2NE OEI-2 fails to function/operate
			DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
114	4.50E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
115	4.18E-05	gRFW130	DCS-OEI-FF-002NE100-0000	RPU 2NE OEI-1 fails to function/operate
			DCS-OEI-FF-002NE200-0000	RPU 2NE OEI-2 fails to function/operate
			DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
116	4.09E-05	gRFW130	DCS-OEI-CF-0002NE00-0000	Common cause failure of RPU 2NE OEIs
			DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
117	4.01E-05	gRFW130	DCS-AIM-FF-002NE1A2-0000	Analog input module 2NE-1A2 fails to function/operate
			DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
118	3.86E-05	gRFW130	DGP-BAC-FF-0MCCE107-0000	Failure of 480V MCC A-107 diesel to remain energized
			DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
119	3.75E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
120	3.72E-05	gRFW130	DCS-OEI-CF-0002NE00-0000	Common cause failure of RPU 2NE OEIs
			DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run

#	Fraction	Group	Cut Set	Description
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
121	3.66E-05	gRFW130	DCS-AIM-FF-002NE1A2-0000	Analog input module 2NE-1A2 fails to function/operate
			DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
122	3.62E-05	gPipe gPump gRFW130	CDP-BAC-FF-000MRBE1-030M	Failure of 4160 V commercial bus A (MRB-A-1) [30 min]
123	3.54E-05	gFctrlI	EXT-STF-CF-002ACFI1-0000	Train 2A-C flow sensor common cause event
124	3.52E-05	gRFW130	DCS-OEI-FF-002NE100-0000	RPU 2NE OEI-1 fails to function/operate
			DCS-OEI-FF-002NE200-0000	RPU 2NE OEI-2 fails to function/operate
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
125	3.52E-05	gRFW130	DGP-BAC-FF-0MCCE107-0000	Failure of 480V MCC A-107 diesel to remain energized
			DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
126	3.51E-05	gRFW130	DCS-PSP-FF-0002NE1L-0000	Power supply 2NE-PWR-1L fails to function (operate)
			DCS-PSP-FF-0002NE1R-0000	Power supply 2NE-PWR-1R fails to function (operate)
127	3.51E-05	gRFW130	DCS-PSP-FF-0001NE1L-0000	Power supply 1NE-PWR-1L fails to function (operate)
			DCS-PSP-FF-0001NE1R-0000	1NE-PWR-1R power supply fails to function (operate)
128	3.51E-05	gRFW130	DCS-PSP-FF-0001NE1L-0000	Power supply 1NE-PWR-1L fails to function (operate)
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
129	3.51E-05	gRFW130	DCS-PSP-FF-0002NE1L-0000	Power supply 2NE-PWR-1L fails to function (operate)
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
130	3.49E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6

#	Fraction	Group	Cut Set	Description
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
131	3.49E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAC-FF-0MRBE115-0000	Failure of utility UPS panel MRB-A-115 to remain energized
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
132	3.44E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
133	3.29E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
134	3.29E-05	gRFW130	RFW-AOV-FC-000PCV71-0000	PCV-7-1 fails to close
135	3.28E-05	gRFW130	DCP-TFM-FF-0MRBE444-0000	Failure of 480/208/120 V transformer MRB-A-444 to DCS panel MRB-A-445
			UDC-RLY-FF-0MRBE447-0000	Relay MRB-A-447 (ATS) fails to transfer supply to panel MRB-A-446
136	3.19E-05	gPump gRFW130	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			UDC-INV-CF-UP116104-0000	CCF of inverters for UPS MRB-A-116 & -104
			UDC-TSW-SO-0000MTS1-0000	Manual transfer switch MTS-1 fails to remain closed
137	3.17E-05	gRFW130	DCP-TFM-FF-0MRBE444-0000	Failure of 480/208/120 V transformer MRB-A-444 to DCS panel MRB-A-445
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
138	3.17E-05	gRFW130	DCP-TFM-FF-0MRBE444-0000	Failure of 480/208/120 V transformer MRB-A-444 to DCS panel MRB-A-445

#	Fraction	Group	Cut Set	Description
			DCS-PSP-FF-0002NE1R-0000	Power supply 2NE-PWR-1R fails to function (operate)
139	3.17E-05	gRFW130	DCP-TFM-FF-0MRBE444-0000	Failure of 480/208/120 V transformer MRB-A-444 to DCS panel MRB-A-445
			DCS-PSP-FF-0001NE1R-0000	1NE-PWR-1R power supply fails to function (operate)
140	3.13E-05	gRFW130	DCS-OEI-CF-0002NE00-0000	Common cause failure of RPU 2NE OEIs
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
141	3.11E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
142	3.08E-05	gRFW130	DCS-AIM-FF-002NE1A2-0000	Analog input module 2NE-1A2 fails to function/operate
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
143	3.06E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BDC-FF-00MRBE23-0000	Failure of 250 Vdc utility bus MRB-A-23 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
144	3.04E-05	gPump	CDP-CBK-SO-0MRBE5D4-0000	Breaker D4 from 480V bus MRB-A-5 to instrument UPS MRB-A-104 fails open
			DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
145	3.04E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running

#	Fraction	Group	Cut Set	Description
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-CBK-SO-MRBE117M-0000	Main breaker to instrument UPS panel MRB-A-117 fails open
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
146	3.04E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-CBK-SO-0E104CB1-0000	Breaker CB1 in instrument UPS MRB-A-104 fails open
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
147	3.04E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-CBK-SO-A117CB11-0000	Breaker CB11 from instr UPS panel MRB-A-117 fails to remain closed
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
148	3.04E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-CBK-SO-0E116CB4-0000	Utility UPS MRB-A-116 output breaker CB4 fails open
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
149	2.96E-05	gRFW130	DGP-BAC-FF-0MCCE107-0000	Failure of 480V MCC A-107 diesel to remain energized
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
150	2.89E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FR-00MRBM43-0000	Diesel MRB-M43 fails to continue running
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
151	2.82E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running

#	Fraction	Group	Cut Set	Description
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
152	2.76E-05	gRFW130	CDP-BAC-FF-000DWBE1-0000	Failure of 480 V comm/diesel MCC DWB-A-1 to remain energized
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
153	2.76E-05	gRFW130	CDP-BAC-FF-0AEBMCC1-0000	Failure of bus AEB-MCC-1 to remain energized
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
154	2.60E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			DGP-RLY-FF-67E327GB-0000	Relay 27GB fails to actuate given undervoltage on diesel bus MRB-A-3
155	2.55E-05	gRFW130	IAS-XVM-PG-000GT610-0000	IAS manual isolation valve GT-6-10 fails to remain open (plugs)
156	2.55E-05	gRFW130	RFW-XVM-PG-0000GT79-0000	Manual valve GT-7-9 plugged
157	2.55E-05	gRFW130	RFW-XVM-PG-000GT722-0000	Manual valve GT-7-122 plugged
158	2.55E-05	gRFW130	RFW-XVM-PG-000GT794-0000	Manual valve GT-7-94 plugged
159	2.55E-05	gRFW130	RFW-XVM-PG-000GT796-0000	Manual valve GT-7-96 plugged
160	2.55E-05	gRFW130	RFW-XVM-PG-000GT797-0000	Manual valve GT-7-97 plugged
161	2.55E-05	gRFW130	RFW-XVM-PG-00GT6699-0000	Manual valve GT-6-699 plugged
162	2.55E-05	gRFW130	RFW-XVM-PG-00GT7083-0000	Manual valve GT-7-83 plugged
163	2.55E-05	gRFW130	RFW-XVM-PG-00GT7123-0000	Manual valve GT-7-123 plugged
164	2.55E-05	gRFW130	RFW-XVM-PG-00GT7146-0000	Manual valve GT-7-146 plugged
165	2.55E-05	gRFW130	RFW-XVM-PG-00GTT721-0000	Manual valve GT-T-7-21 plugged
166	2.55E-05	gRFW130	RFW-XVM-PG-00GTT722-0000	Manual valve GT-T-7-22 plugged
167	2.55E-05	gRFW130	IAS-XVM-PG-00GT6552-0000	IAS manual isolation valve GT-6-552 fails to remain open (plugs)
			IAS-XVM-XM-PAIAXTIE-0000	Operator fails to open PLA-IAS crosstie valve
168	2.47E-05	gPump gRFW130	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running

#	Fraction	Group	Cut Set	Description
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-TSW-SO-0000MTS1-0000	Manual transfer switch MTS-1 fails to remain closed
169	2.42E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
170	2.38E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-BAC-FF-0MRBE117-0000	Failure of instrument UPS panel MRB-A-117 to remain energized
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
171	2.38E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
172	2.27E-05	gRFW130	DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
			RFW-MDP-FS-0000M221-0000	Booster pump M-221 fails to start
173	2.10E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
174	2.10E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6

#	Fraction	Group	Cut Set	Description
			UDC-BDC-FF-00MRBE23-0000	Failure of 250 Vdc utility bus MRB-A-23 to remain energized
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
175	2.07E-05	gRFW130	DIW-MDP-FR-000DWB21-0000	Demin pump DWB-21 fails to continue to run
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FS-0000M221-0000	Booster pump M-221 fails to start
176	2.07E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-CF-A116E104-0000	Common-cause failure of rectifiers for UPS units MRB-A-116 & -104
177	2.02E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			UDC-BDC-FF-0MRBE459-0000	Failure of 250 Vdc control power bus MRB-A-459 to remain energized
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
178	1.95E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DSA-SNR-PG-00000J13-0000	Diesel generator M43 starting air strainer ST-J-13
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
179	1.92E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-TM-00MRBM43-POWR	Diesel MRB-M43 unavailable due to maintenance (power op)
			UDC-INV-FF-0MRBE116-0000	Inverter for instrument UPS MRB-A-116 fails to operate
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
180	1.77E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand

#	Fraction	Group	Cut Set	Description
			UDC-CBK-SO-0E116CB4-0000	Utility UPS MRB-A-116 output breaker CB4 fails open
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
181	1.74E-05	gRFW130	DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			DIW-STP-FF-00PS823A-0000	PS-8-23A fails to function (DIW transfer pump DWB-21 autostart)
			RFW-MDP-FS-0000M221-0000	Booster pump M-221 fails to start
182	1.69E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-BAT-FF-00MRBE58-0000	Battery bank MRB-A-58 fails to operate
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
183	1.65E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-FS-00MRBM43-0000	Diesel MRB-M43 fails to start on demand
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-SSW-FF-MRBE116S-0000	Utility UPS MRB-A-116 static switch fails to transfer
184	1.62E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-XF-67M42M43-0000	Failure to start standby diesel as backup to MRB-M-6
			UDC-BDC-FF-00MRBE23-0000	Failure of 250 Vdc utility bus MRB-A-23 to remain energized
			UDC-INV-FF-0MRBE104-0000	Inverter for instrument UPS MRB-A-104 fails to operate
			UDC-REC-FF-0MRBE116-0000	Failure of rectifier for utility UPS MRB-A-116
185	1.57E-05	gRFW130	DIW-MDP-CR-TRNPUMPS-0000	DIW transfer pumps fail to run due to CCF
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
186	1.57E-05	gPump	DGP-DGN-FR-00MRBM42-0000	Diesel MRB-M42 fails to continue running
			DGP-DGN-TM-00MRBM43-POWR	Diesel MRB-M43 unavailable due to maintenance (power op)

#	Fraction	Group	Cut Set	Description
			UDC-BAC-FF-0MRBE116-0000	Failure of utility UPS panel MRB-A-116 to remain energized
			UDC-REC-FF-0MRBE104-0000	Rectifier for instrument UPS MRB-A-104 fails to operate
187	1.57E-05	gRFW130	DCP-BAC-FF-00MRBE15-0000	Diesel-comm MCC MRB-A-15 fails to remain energized
			UDC-RLY-FF-0MRBE447-0000	Relay MRB-A-447 (ATS) fails to transfer supply to panel MRB-A-446
188	1.57E-05	gRFW130	DCP-BAC-FF-0MRBE445-0000	DCS power panel MRB-A-445 fails to remain energized
			UDC-RLY-FF-0MRBE447-0000	Relay MRB-A-447 (ATS) fails to transfer supply to panel MRB-A-446
189	1.56E-05	gRFW130	DIW-MDP-TM-000DWB21-0000	Demin pump DWB-21 unavailable due to testing or maintenance
			DIW-MDP-XM-STARTDIW-0000	Operator fails to manually start an DIW transfer or flush pump
			RFW-MDP-FR-0000M221-0000	Booster pump M-221 fails to run
190	1.52E-05	gRFW130	DGP-CBK-SO-0MRBE9E1-0000	Breaker E1 from 480 V diesel bus MRB-A-9 fails to remain closed
			DIW-SYS-FH-FLWDVDRX-0000	Flow diversion in RTC DIW system resulting in insufficient flow to DRX
191	1.52E-05	gRFW130	DCP-BAC-FF-00MRBE15-0000	Diesel-comm MCC MRB-A-15 fails to remain energized
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
192	1.52E-05	gRFW130	DCP-BAC-FF-0MRBE445-0000	DCS power panel MRB-A-445 fails to remain energized
			UDC-SSW-SO-0MRBE104-0000	Static transfer switch MRB-A-104 fails open
193	1.52E-05	gRFW130	DCS-PSP-FF-0001NE1L-0000	Power supply 1NE-PWR-1L fails to function (operate)
			UDC-BAC-FF-0MRBE117-0000	Failure of instrument UPS panel MRB-A-117 to remain energized
194	1.52E-05	gRFW130	DCS-PSP-FF-0001NE1L-0000	Power supply 1NE-PWR-1L fails to function (operate)
			UDC-BAC-FF-0MRBE446-0000	DCS power panel MRB-A-446 fails to remain energized
195	1.52E-05	gRFW130	DCS-PSP-FF-0002NE1L-0000	Power supply 2NE-PWR-1L fails to function (operate)
			UDC-BAC-FF-0MRBE117-0000	Failure of instrument UPS panel MRB-A-117 to remain energized

#	Fraction	Group	Cut Set	Description
196	1.52E-05	gRFW130	DCS-PSP-FF-0002NE1L-0000	Power supply 2NE-PWR-1L fails to function (operate)
			UDC-BAC-FF-0MRBE446-0000	DCS power panel MRB-A-446 fails to remain energized
197	1.52E-05	gRFW130	DCP-BAC-FF-00MRBE15-0000	Diesel-comm MCC MRB-A-15 fails to remain energized
			DCS-PSP-FF-0002NE1R-0000	Power supply 2NE-PWR-1R fails to function (operate)
198	1.52E-05	gRFW130	DCP-BAC-FF-0MRBE445-0000	DCS power panel MRB-A-445 fails to remain energized
			DCS-PSP-FF-0002NE1R-0000	Power supply 2NE-PWR-1R fails to function (operate)
199	1.52E-05	gRFW130	DCP-BAC-FF-00MRBE15-0000	Diesel-comm MCC MRB-A-15 fails to remain energized
			DCS-PSP-FF-0001NE1R-0000	1NE-PWR-1R power supply fails to function (operate)
200	1.52E-05	gRFW130	DCP-BAC-FF-0MRBE445-0000	DCS power panel MRB-A-445 fails to remain energized
			DCS-PSP-FF-0001NE1R-0000	1NE-PWR-1R power supply fails to function (operate)