U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7234

Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop SSOP
   Washington, DC 20402-0001
   Internet: http://bookstore.gpo.gov
   Telephone: 1-866-512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22161-0002
   http://www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
http://www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG-0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-7234

Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability

Manuscript Completed: December 2015
Date Published: May 2017

Prepared by:
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]
Nancy Johnson[2], and Ming Li[3]

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

Ming Li, NRC Project Manager

NRC Job Code V6196

Office of Nuclear Regulatory Research

ABSTRACT

A statistical testing approach for quantifying on-demand failure probabilities for safety-related digital systems has been developed and applied to the loop-operating control system (LOCS) of an Advanced Test Reactor (ATR) experimental loop at Idaho National Laboratory (INL). This work is the result of a collaboration between Brookhaven National Laboratory (BNL), INL, and the Korea Atomic Energy Research Institute (KAERI).

The objectives of the study include:

1. development of a statistical testing approach for estimating digital system failure probability, the results of which are suitable for including in a probabilistic risk assessment (PRA); and

2. application of this approach to the LOCS, and insights into the feasibility, practicality, and usefulness of the estimation in models of digital systems for inclusion in nuclear power plants' PRAs.

The study used the ATR's PRA to define the testing environment, that is, the conditions under which the safety system would be called upon to initiate a safety function. Based on the PRA accident sequence information, a thermal-hydraulic model (RELAP5) was used to simulate the experimental loop conditions (e.g., pressure, temperature, and flow) during the selected accident sequences in order to provide realistic input signals to the LOCS test platform. To ensure that the test cases provided adequate coverage of operational conditions, thirteen probabilistic failure process models (PFPMs) were developed to represent the varieties associated with timing, component failure modes, and process variable control. An automated test platform was developed to supply input signals for each test case to the LOCS digital system and monitor when a trip signal was generated. The testing results were then used to quantify the on-demand failure probability of the digital LOCS system.

FOREWORD

Nuclear power plants (NPPs) have traditionally relied upon analog instrumentation and control (I&C) systems for monitoring, control, and protection functions. As current analog systems approach obsolescence, there is increasing interest in replacing these systems with digital equipment. Additionally, new reactor designs fully incorporate digital systems into critical safety systems. However, digital systems have some unique characteristics (e.g., software), and may have different failure causes and/or modes than analog systems. Therefore, modeling these digital systems in NPP PRAs presents special challenges for the U.S. Nuclear Regulatory Commission (NRC).

The current NRC licensing process for digital systems relies on deterministic engineering criteria. In its 1995 PRA Policy Statement, the NRC 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. Though many activities are carried out in the life cycle of digital systems to ensure a high-quality product, there is presently no universally agreed upon state-of-the-art method available to quantify the reliability of digital systems in a manner suitable to support risk-informed regulatory decision-making. To address this limitation, the NRC is currently performing research on the development of probabilistic models for digital I&C systems.

Brookhaven National Laboratory (BNL) has been supporting the NRC in this research program through a series of projects on digital I&C system reliability modeling and quantification. They developed a PRA-based statistical testing method to quantify the on-demand failure probability for a safety system deployed in a test reactor. The existing test reactor PRA information was used to identify demand scenarios that were then simulated using RELAP5 to generate realistic digital system inputs. The testing was automated by feeding test cases into the test reactor digital system and recording its output (i.e., the generation of a trip signal) as testing results.

This study successfully developed a PRA based statistical testing method, applied this method to a deployed digital system, and demonstrated its feasibility for digital I&C safety systems in NPPs.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

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, risk assessment for digital systems has not been fully developed. The NRC established a plan for research on digital systems to identify and develop methods, analytical tools, and regulatory guidance for (1) including models of digital systems in the PRAs of nuclear power plants (NPPs), and (2) incorporating digital systems in the NRC's risk-informed licensing and oversight activities.

Previous NRC research explored approaches for addressing digital instrumentation and control (DI&C) system failures in the current NPP PRA framework. Specific areas investigated included PRA modeling digital hardware, identification of desirable attributes of quantitative digital system reliability methods, and assessments of software quality attributes to support development of a Bayesian Belief Network model of software reliability. These elements were identified as necessary to integrate DI&C into PRAs. The statistical testing research described in this report was jointly conducted by Brookhaven National Laboratory (BNL) and Idaho National Laboratory (INL) in order to advance the state of the practice of quantifying safety-related digital system reliability.

A digital system consists of hardware and processing logic (software). Failures of a digital system arise from hardware failures, software failures (unexpected behaviors), and erroneous interactions between different hardware and software components. Hardware failures are caused by wear-out and are called "random failures" because they follow a stochastic process. Software failures are due to the triggering of pre-existing defects in the processing logic (software defects) under the system operational environment. On the other hand, software failures are often referred to as "design errors" and their failure mechanisms are deemed deterministic. In other words, if the triggering condition repeats, then the corresponding software failure repeats. Software defects can arise from errors made during different phases of the system development process such as the requirements, design, or coding phases. The system operational environment includes factors such as the time history of digital system inputs, communication interfaces, the state of the internal digital system, and external conditions. Such environmental factors are assumed to follow a random process. Thus software failures are "modulated" to follow random processes. The software failure probability is then a function of both the number of pre-existing defects and the presence of a triggering condition caused by the manner in which the software is used. Therefore, testing a digital system under different operational conditions could yield completely different test results.

In order to quantify digital system failure probability in an NPP PRA, the digital system should be tested under the operational conditions specified by the NPP PRA. This study utilizes the statistical testing method (STM) to produce the operational environment and test the system to determine whether the environment is capable of triggering pre-existing defects. The test results (number of failures) thus represent operational failures. The operational conditions are determined by each PRA sequence in which the digital system appears. For example, if one postulated that the digital reactor protection system (RPS) appears in both the loss of coolant accident (LOCA) and the steam generator tube rupture (SGTR) sequences, the inputs to this digital RPS (such as the reactor's temperature, pressure, steam-generator level, steam pressure) would follow different patterns, and different parts of the RPS logic would be challenged. Consequently, the probability of RPS failure might differ for each sequence. The STM method developed in this research produces test scenarios specific to each sequence and tests the RPS system against these scenarios to generate sequence-specific failure probabilities for this RPS system.

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

1. Select a system under test (SUT);
2. Identify SUT-related PRA sequences (represented by the cutsets);
3. Determine the thermal-hydraulic simulation boundary conditions corresponding to the selected cutsets;
4. Run the thermal-hydraulic model to calculate a time history of the reactor and the plant physical conditions. Such outputs are test scenarios to the SUT;
5. Execute test scenarios and collect test results; and
6. Analyze the test results to quantify the SUT on-demand 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 with the ATR PRA and RELAP5 models relevant to the LOCS system. BNL revised these models to make them STM-friendly, identified the LOCS-relevant cutsets, configured the RELAP5 model according to plant conditions defined by the cutsets, executed the RELAP5 model, and produced test scenarios. These scenarios were delivered to INL to test the LOCS. INL developed a LOCS test configuration that automated the testing. This test configuration automatically fed BNL's test scenarios to the LOCS, and collected the results. They were then statistically analyzed to generate the probability of LOCS failure.

For this study, 10,000 different test cases were used to demonstrate a reliability level consistent with PRA and design requirement assumptions. The test cases did not trigger any pre-existing digital logic defects, or hardware random failures. The testing did identify one potential failure that was not reproducible and was determined to be caused by the test equipment setup. However, a few early trips and delayed trips were observed and were further analyzed. The analysis demonstrated that these anomalies were likely caused by the inaccuracy of the analog input/output modules.

This method tests the SUT as a black box; therefore the testing result includes any possible type of failure within the SUT: hardware, software, internal communication (if it exists), and common cause failures (CCFs). Since the test cases were selected to represent a realistic operational profile based on PRA insights, this method of black box testing represents how the SUT would perform in service.

ACKNOWLEDGMENTS

The authors would like to express deepest appreciation to all those who made it possible to complete this report. A special gratitude goes to the United States Nuclear Regulatory Commission project manager Mr. Alan Kuritzky and his Branch Chief Dr. Kevin Coyne, whose contribution in making suggestions and providing encouragement, coordinating this project especially in writing this report. The authors are grateful to Dr. Joy Leggett of the NRC for her technical review and editing of this report, and to the other NRC reviewers who reviewed this report.

The authors also thank Jim Higgins and Avril Woodhead of the Brookhaven National Laboratory for their editorial review of the report, and to Linda Fitz and Maria Anzaldi of the Brookhaven National Laboratory who put several versions of the report together and helped with the logistics of the project.

The authors would also like to show gratitude to Dr. Hyun Gook Kang of Rensselaer Polytechnic Institute (previously of Korea Atomic Energy Research Institute and then Korea Advanced Institute of Science and Technology) and his research staff for sharing their pearls of wisdom with us during the course of this research.

ABBREVIATIONS

AIM	analog 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
DI&C	digital instrumentation and control
DOM	digital output module
DPU	distributed processing unit
EPRI	Electric Power Research Institute
ESFAS	engineered safety features actuation system
FCV	flow control valve
PFPM	probabilistic failure process model
FPGA	field programmable gate array
HDW	high pressure demineralized water
HTC	heat transfer coefficient
KAERI	Korea Atomic Energy Research Institute
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	Organization 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
RCCS	rod clutch control system
RELAP	Reactor Excursion and Leak Analysis Program
RG	regulatory guide
RPS	reactor protection system
RPU	remote processing unit
RTD	resistance thermal detector
SLOCA	small loss of coolant accident
SCR	silicon-controlled rectifier
STM	statistical testing method
SUT	system under test
TCV	temperature control valve
TH	thermal-hydraulic
V&V	verification and validation
WGRisk	Working Group on Risk Assessment

1 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 (DI&C) systems are expected to play an increasingly important safety role at nuclear power plants (NPPs), the NRC established a plan for research on digital systems [NRC 2010a] defining a coherent set of projects to support regulatory needs. Some of the projects included in this research plan address risk assessment methodologies and data for digital systems. The objective of the NRC's research on risk in digital systems 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 into the NRC's risk-informed licensing and oversight activities.

Figure 1-1 graphically depicts the interrelationships between the various activities associated with the NRC's research on digital systems. The effort to develop an approach to modeling digital system reliability is being coordinated with several related research activities that the NRC is undertaking. As depicted in Figure 1-1, these other areas include the identification and analyses of failure modes [Chu 2008 and 2009a], investigating methods and tools for the probabilistic modeling of digital systems [Chu 2008 and 2009a], investigating the modeling of digital systems using dynamic PRA methods [Aldemir 2006, 2007, 2009], the operating experience [Korsah 2010], and the digital system's 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 research on digital system reliability is the need to establish a commonly accepted basis for incorporating the failure behavior of software into reliability models of the digital I&C system that are compatible with existing NPP's PRAs[1]. For several years, the NRC sponsored Brookhaven National Laboratory (BNL), 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 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 have been developed using traditional (static) event-tree and fault-tree methods. To address software failures in the current PRA framework, software failures need to be captured in the PRA sequences or basic events. In other words, software functions or components need to be modeled as the event tree's top events or the fault tree's basic events, and quantified using one or more of the quantitative software reliability methods that are the primary interest of this study.

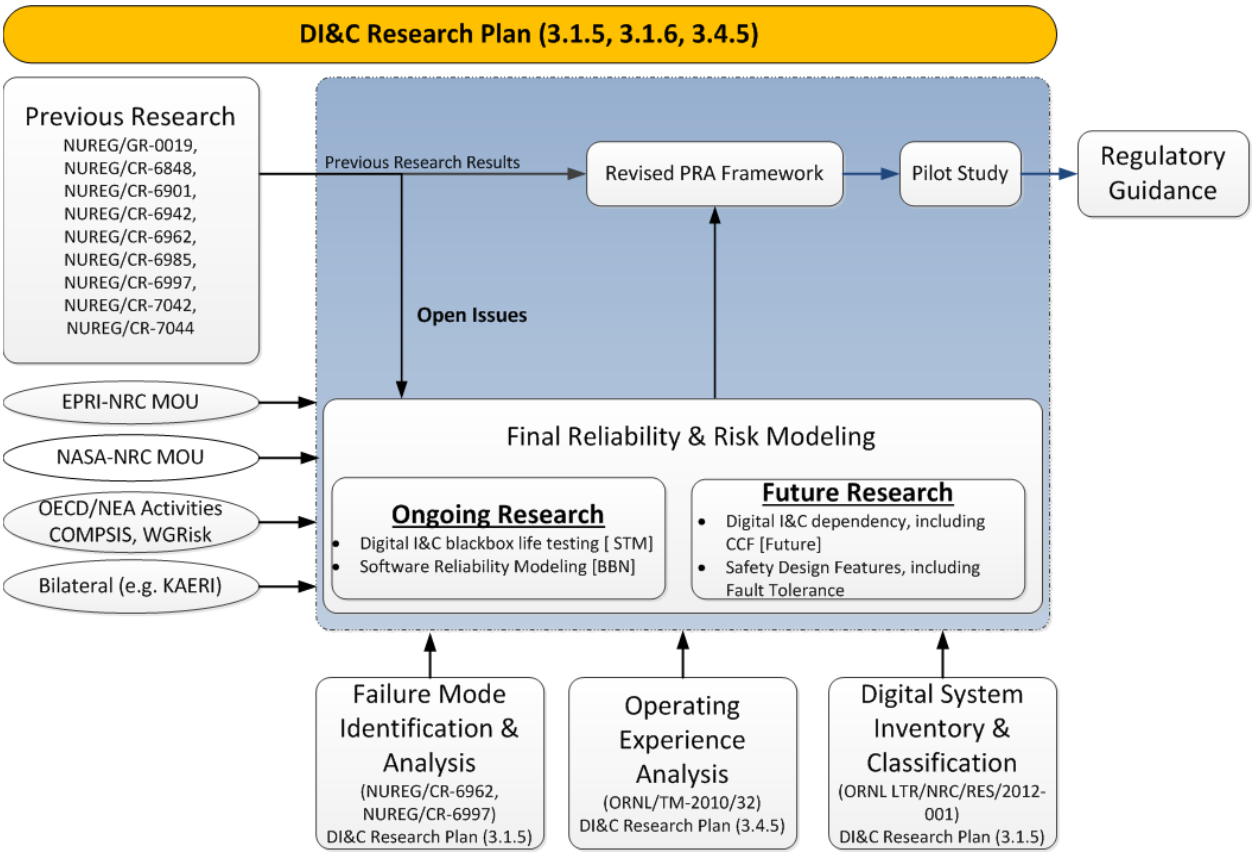


Figure 1-1 NRC Research Activities on Digital System Reliability

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, that results in, or contributes to, the host (digital) system's failing to accomplish its intended function, or initiating an undesired action. 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.

The NRC's Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital I&C Systems recommended the NRC staff to investigate the philosophical basis of software failures. The NRC tasked BNL accordingly in 2008 to organize an expert panel (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."*

The panel also agreed 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.

The BNL research team reviewed a spectrum of methods to quantify frequencies of digital systems failures and software failures that can be integrated into a PRA [Chu 2010]. The methods were identified by reviewing the research sponsored by the NRC or NASA, performed by international organizations, and/or published in journals and conference proceedings. A set of ranking criteria with respect to their capabilities of quantifying digital system on-demand failure probabilities was established and these methods were evaluated against this set of criteria in a later study [Chu 2013]. Two methods (i.e. the statistical testing method and the Bayesian Belief Network) were selected based on this evaluation as preferred approaches and were further developed to meet the NPP PRA needs. This study demonstrates how to apply the STM to one trial system.

A DI&C system might fail due to hardware failures, software failures (called software failures in the literature), and interaction issues among hardware/software components. Hardware failures are material wear-out and follow random processes. These types of failures, such as power unit failures, normally immediately stop the DI&C functions when they occur.

A software failure is caused by the triggering of a defect residing in the software, introduced during its development life-cycle that results in, or contributes to, the host (digital) system either failing to accomplish its intended function or initiating an undesired action. Triggering includes the generation of particular inputs to the digital system due to the state of the operating environment (i.e., of the NPP), in combination with the internal state of the digital system. By this definition the software failures are input-dependent. The probability of software failures is a function of residual defects and the input distributions (operational profile).

Interaction issues include internal state inconsistencies that might be led by hardware failures such as single event upset, software interface mismatches, software internal data inconsistencies, and other failures. These issues are latent in nature and make them very difficult to capture and model using traditional reliability analysis methods. Therefore, due to these unique DI&C system failure mechanisms, the traditional reliability life testing method becomes inappropriate to evaluate DI&C failure probability. Since the probability of the software failures relates to the operational profile under which the DI&C runs, the DI&C system modeled in a PRA sequence should be tested under the conditions defined by this PRA sequence in order to evaluate its PRA-specific failure probability. The test cases are sampled from the operational profile and statistically represent the operation conditions; for this reason, this method is referred to as the statistical testing method.

In this study, the STM was developed and applied 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 was a collaboration between BNL's and INL's staff following the overall approach developed by BNL. In addition to supplying the ATR's PRA and the RELAP5 model of the experiment loop, INL established the needed test configuration and carried out the tests. Chapter 2 details the approach of this study, including the step-by-step procedure followed. In this study, a non-informative prior distribution was used to Bayesian estimate the test results.

1.2 Objective and Scope

The following are the objectives of the statistical testing method:

1. Develop a statistical testing approach for estimating the on-demand failure probability[2] of safety-related digital systems, the results of which are suitable for inclusion in a PRA; and

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 models of digital systems 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 the failure mode in which the system fails to perform its protection functions (represented by the probability of failure on demand) at an NPP, in other words, the system fails to produce safety actuation signals (trip signals) when safety (trip) conditions are present.

    - This method tests the SUT as a black box, therefore the testing result includes any types of possible failures within the SUT: hardware, digital logic, internal communication (if it exists), and common cause failures (CCFs). CCFs and other types of dependency failures among SUT and other components in NPPs were not evaluated by this study but should be captured in NPP PRAs. These are still open research topics.

[2] A "demand" refers to a plant condition that requires the actuation of safety systems such as the reactor-trip system.

2 GENERAL APPROACH

The PRA-based STM designed for estimating NPP safety-related DI&C failure probabilities is described in this chapter. Figure 2-1 provides an overview of the STM process. Sections 2.1-2.7 of this chapter provide summary descriptions of each of the steps shown in Figure 2-1. These sections begin by describing the general approach of a given step followed by the specifics associated with this study. The chapter concludes by summarizing the assumptions and limitations of the STM approach.

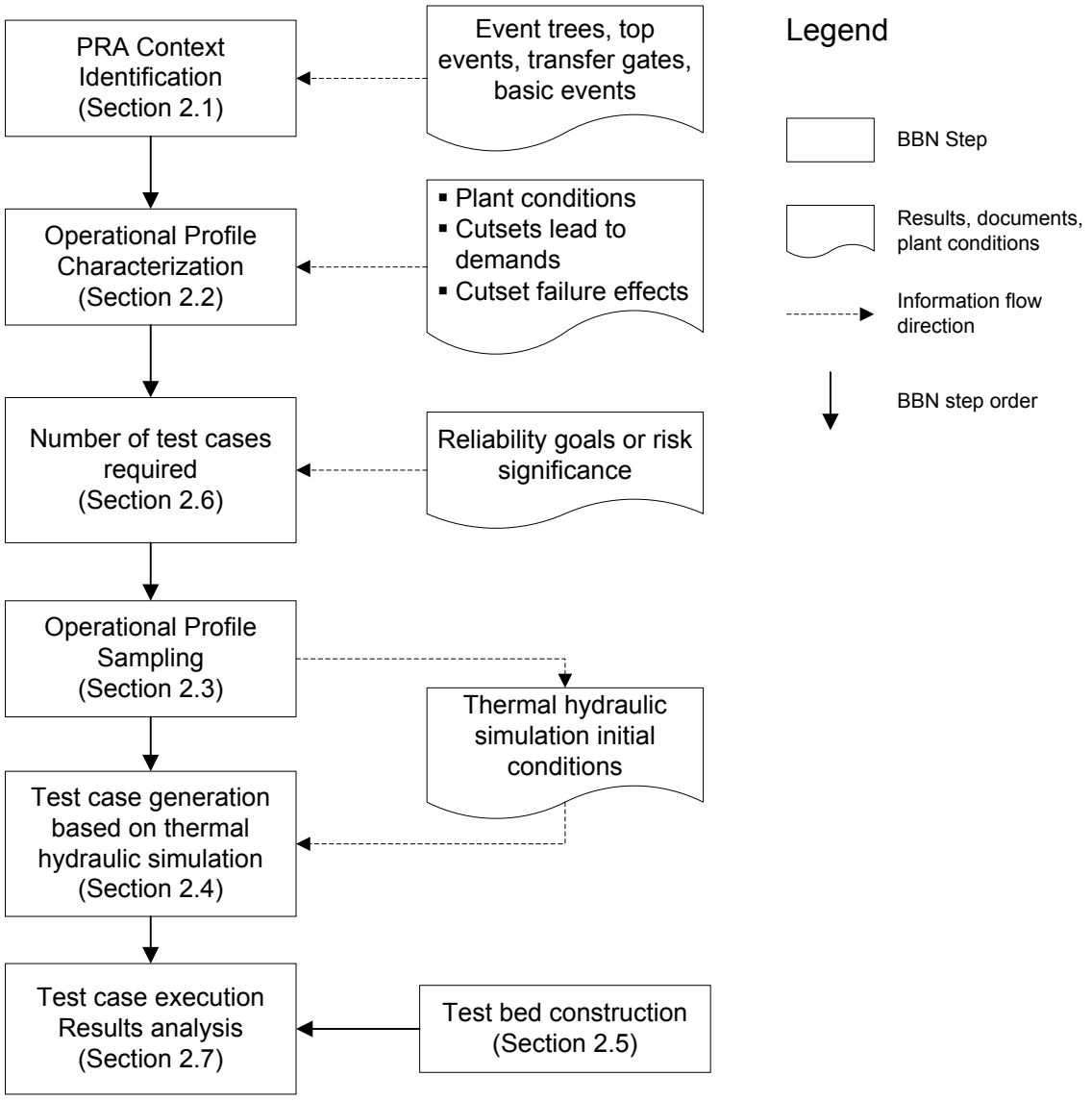


Figure 2-1 STM Procedure

The terms “context” and “operational profile” are defined as below for this study:

- Operational profile: The set of distributions of occurrence likelihood (or frequency) for the inputs over values. For example, given a binary input that has two possible values, 0 and 1, if its operational profile were defined as Pr(0) = 0.3 and Pr(1) = 0.7, then the value of 1 would appear 70% of the time while a value of 0 would appear 30% of the time.

- Context: Context is also referred to as “PRA context” in this report, and is defined as plant conditions under which the software operates as determined by PRA scenarios. For instance, if an RPS appears as a top event after a small loss of coolant accident (LOCA) as an initiating event (IE), the condition (represented as input values for the software) associated with this IE is identified as the “PRA context” for this RPS software. For each context, an operational profile can be defined.

2.1 Use of PRA-Defined Contexts

In a PRA, the digital protection systems can be modeled either as 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 that typically are used as transfer gates in the fault trees of emergency safety features (e.g., a safety injection system). PRA scenarios leading to a 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 to estimate 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 (SUT). For example, the cutset of a sequence that leads to a demand for safety injection is a more detailed context for the ESFAS. In addition, events used in PRA are simplified representations of an NPP’s physical operational conditions 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’s physical conditions constitute the operational profiles upon which test scenarios were generated. A thermal-hydraulic model was used to simulate the NPP physical conditions and generate scenarios.

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. Chapter 4 gives the details of the PRA model. A RELAP5 [NRC 1995] model of the loop was used to generate the test-scenario inputs to the LOCS. Chapter 5 details the RELAP5 model.

2.2 Operational Profile Characterization

The operational profile for a DI&C system defines its possible inputs and associated likelihood. The PRA contexts described in Section 2.1 might be at high abstraction level and need further “instantiation” to create real inputs for the DI&C system. For instance, a PRA cutset defines a small LOCA accident; however, conditions such as the location of the breach and size of the

rupture are normally not included in the PRA cutset. Such information needs to be defined in order to enable the thermal hydraulic simulation to produce signals as inputs to the DI&C system (RPS in this case). In this study, characteristics such as the size and location of the ruptures are assumed to follow some distributions and are randomly sampled from these distributions to represent their varieties in real NPP operations. Such varieties are classified into the three groups listed below.

1. *Initial condition of the plant.* The plant's condition before 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 this list 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.* PRA contexts are defined in terms of failure events whose 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 that have different effects on the plant's condition, that is, a pump trip leading to its coast down can lead to a different condition than a seizure of the pump would. To capture this type of variability, more detailed models of the failure events must be developed than those in the PRA. They need to encompass 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 scenarios simulated via a thermal-hydraulic model.

For demonstration purposes, 100% power was used in this study to derive the operational profile. Other power levels can be used for real NPP applications. Cutsets representing different reactivity insertion scenarios were sampled according to their frequencies. Thirteen probabilistic failure process models[3] (PFPMs) were developed for 13 types of failure events represented in the cutsets. For example, the closure of a flow-control valve was modeled in terms of its closure time, which is assumed to be uniformly distributed between 15- and 45-seconds. Section 5.2.2 gives detailed descriptions of the probabilistic failure process models.

2.3 Operational Profiles Sampling

A test scenario can be identified by sampling from the operational profile. The test scenario 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 process model of each failure event in the cutset.

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

Each sample from the operational profile is then used to define a thermal-hydraulic simulation of the plant's condition experienced by the digital protection system. Simulation results 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 their frequencies, generating 10,000 cutset samples. For each sampled cutset, its associated probabilistic failure process model parameters were sampled to completely define the scenario. Such scenario was then simulated using the RELAP5 model. That is, each test scenario represents a reactivity insertion event caused by component failures in a sampled cutset with associated probabilistic failure process model(s). The 200 cutsets were considered adequate for this demonstration study because they cover all the primary system failures that are modeled in the RELAP5 model. It should be noted that failures in the secondary- and tertiary-sides may be dominant contributors to reactivity insertion. These failures were modeled approximately in RELAP5 due to the limitations that will be described in Section 2.4. Chapter 6 details the generation of test scenarios.

2.4 Using a Thermal-hydraulic Simulation

A thermal-hydraulic model is needed 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. Since a PRA scenario starts with the plant initially in a normal steady-state condition, the thermal hydraulic model should first establish a steady state condition of the plant before component failures that lead to trip conditions are introduced. It should realistically model the failure effects defined by the process modes.

In this study, an INL RELAP5 model[4] of Loop 2A, which is one of the six experimental loops of the ATR, was modified to include additional features necessary to support the full characterization of the operational profile of the statistical testing method. The INL version does not model the ATR itself and the Loop 2A model is simplified, that is, it does not model all of the primary system components that are included in the PRA (e.g., the makeup to the loop), does not include the secondary- and tertiary-sides of the loop, nor does it model all the control functions of the loop, including those performed by the LOCS. Modifications made to the RELAP5 model in this study were intended only to represent the failures of components that are not included in the initial model. For example, in the INL model, the secondary side is modeled as a boundary condition of the heat exchanger. Therefore, all secondary-side failures need to be modeled in terms of the heat-transfer coefficient in this study. Chapter 5 documents the model that was used to simulate the scenarios.

2.5 Test Configuration

A test configuration was built that feeds test inputs such as the simulation results of a thermal-hydraulic code to the system under test and records the outputs from the system under test. This test configuration consists of the digital protection system, a host computer, and the interfaces between them (i.e., I/O modules). The SUT should be used in its original configuration, including the I/O modules. The host computer converts thermal-hydraulic simulation outputs to values with

[4] In this study the RELAP5 code was used to demonstrate the thermal hydraulic simulation mainly because the ATR thermal hydraulic model is in RELAP5. The STM method does not exclude the use of other thermal hydraulic codes.

the same input formats as the SUT and feeds them into the SUT. It also captures the outputs from the system under test.

In this study, the host computer is a personal computer running the LabVIEW software [Labview] developed by National Instruments; it supplies the inputs to, and records the outputs from, the LOCS. An approximation of the actual configuration of the LOCS at the plant was used. In addition, the LOCS also undertakes control functions that require processing a large number of signals and thus, a large number of I/O modules. Since the scope of this study is the protection functions, inputs to LOCS control functions were set to dummy values and a smaller number of I/O modules were used. It is assumed for this study that this configuration does not intervene with the LOCS protection functions. Chapter 7 describes the test configuration and its usage in detail.

2.6 Determination of the Number of Tests Needed

In order to ensure that the DI&C's contribution to overall risk is considered acceptable, the number of scenarios that are needed is determined using (1) a reliability goal specified for the DI&C and (2) the frequency of the digital system failures derived from risk considerations [Chu 2013]. The number of tests without failure that are 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 would require 10,000 tests without failure to demonstrate a mean failure-probability of 10^{-4} [Chu 2013].

2.7 Testing 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 the sensor's signals. The records are converted by the host computer into a format that the digital protection system can read and are then sent to that 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 are then examined to determine whether the trip signal is generated at the right time in order to verify the correctness of the test results. An important part of the examination is to determine the criterion for success in terms of the time when an actual trip signal is generated based on the system's design requirements. For example, given a small LOCA, a high-pressure safety-injection system has to be actuated before degraded cooling results in core damage. Since the digital protection system will generate a trip signal only when a threshold is exceeded, a requirement may be stated as follows: "…a trip signal should be generated within 0.1 second after the threshold is exceeded." The length of that time should be determined in the design requirements that, in turn, are set by the physical conditions in which the system is designed to function. 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 DI&C failure. Since the tests are performed on the digital system consisting of both hardware and software, the results can be used to quantify the failure probability of the system. If failures are observed, the causes of the failures can be identified (i.e., either software or hardware) and used to quantify software and hardware failure probabilities separately.

In this study, two sets of 10,000 test scenarios were executed. During the initial set of tests, a significant number of early- and delayed-trips occurred which made interpretation of the test results difficult. A second set of test scenarios were then run after improvements were made in the

testing method in order to reduce the occurrence of early- and delayed-trips. The two runs are summarized below and described in detail in Appendix B and Chapter 8, respectively.

In the initial run, the evaluation of the test results was based on the understanding of how the test configuration works, and was not related to the design requirements. The evaluation approach was not successful in explaining the test results, especially anomalies associated with early- and delayed-trip results. The main consideration of the evaluation was related to the fact that the host computer and the LOCS were not synchronized. The LOCS has a cycle time of between 100 and 300 milliseconds, while the host computer has one of approximately 100 milliseconds. Accordingly, the RELAP5 model generates inputs to the LOCS at a rate of every 100 milliseconds (RELAP5 can simulate a higher speed than the LOCS digital system). Whether or not a test resulted in a success or failure was based on an estimated time window in which the trip signal was expected to be generated, considering the possible delay caused by the cycle times of the host computer and the LOCS. An important assumption in determining this time window is that the LOCS has a constant cycle time of 0.3 seconds and that of the test computer is 0.1 second. Appendix B details the evaluation of the test outputs. Twenty seven delayed trips and 964 early trips were observed. A few of them were analyzed in more detail. It was found that some delayed trips do not exceed the corresponding times of the channel's response specified in LOCS' design requirements [INL 2010], and do not have to be considered failures-on-demand. The early trips tended to occur when the parameters were close to the thresholds, and may be caused by hardware inaccuracies or noise from the LOCS or test equipment.

A few changes were made in the rerun of the scenarios to address the difficulties and issues identified in the initial run. They include the removal of the artificial noise added to the RELAP5 output, more accurate calibration of test equipment and the LOCS hardware, and more precise measurement of the test computer and LOCS cycle times. The criterion for determining if a test is successful is based on the following:

1. The earliest time when a trip signal can be generated is the time when the first input record exceeding a threshold occurs in a test scenario.

2. To ensure that the LOCS reads a record exceeding the threshold, three consecutive exceeding-threshold input records are required. Therefore, the latest time when a trip signal should be generated in a test scenario is the time when the third such record occurs, plus a delay time of 0.5 second estimated by INL[5].

The above criterion is more conservative than the channel-response times specified for the channels [INL 2010]. Using this criterion, 45 delayed trips and 16 early trips were observed. To explain the anomalies, INL evaluated the inaccuracy of the analog I/O modules, and demonstrated that if the inputs were corrected accordingly, then all the anomalies would be avoided. Therefore, the anomalies were caused by hardware inaccuracies, not system failures. For a total of 10,000 tests and no failures, a mean failure probability was obtained by assuming a uniform prior distribution. Chapter 8 gives more details of the rerun. Chapter 9 documents the quantification of system reliability using the results of the test.

[5] The 0.5 seconds is based upon the testing that was done to support this project, considering the cycle times of the LOCS, and of the host computer.

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. How the limitations can be overcome is either described or self-explanatory.

1. *Whether or not the PRA accurately models the demands on the protection system.* In this study, the different ways reactivity accidents can occur were explicitly modeled in the ATR PRA. BNL made some modifications to the model to meet the needs of the study. For example, additional branches were introduced in an event tree to better account for the accidents' severity in mitigating the accidents. In addition, both the control and protection functions of the LOCS are modeled in the PRA, and the dependency between the two must be correctly modeled.

   The top 200 cutsets were used to generate test scenarios for demonstration purposes. However, this is not a limitation of this method as more cutsets could be used to increase the testing fidelity. It is worth noting that the total testing effort increases proportionally.

   The cutsets produced from PRA are minimal cutsets. They represent the possible sets of the minimum number of failure components that lead to an end state. One may argue that the non-minimal cutsets contain component failures that might lead to different failure scenarios. This potential omission can be covered by a full-spectrum sampling strategy from component failure events not included in the minimal cut set. For instance, assume that one NPP has *n* components modeled in a PRA. One cutset has *m* components, where *m* is less than or equal to *n* components. This implies failures of these *m* components would certainly lead the NPP to an undesired end state (normally core damage), regardless of the success or failure states for the rest of (*n*-*m*) components. However successes or failures of these (*n*-*m*) components might cause the DI&C system to execute different processing logic. Therefore, the thermal hydraulic simulation should include possible statuses for the (*n*-*m*) components. This could be done by random sampling from the (n-m) components joint status distribution. The use of the design of experiment principles to reduce the number of combination is recommended. A detailed discussion of this topic is outside the scope of this study and is therefore not included in this report. This topic should be covered in future studies.

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

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 variables 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 considerations of the potential accidents.

In this study, the engineering (design basis) analysis was not available. The maximum allowed channel-response times of different types of trips (e.g., low flow, high temperature, and low pressure) were specified [INL 2010] with the shortest maximum response time being 0.78 second for low pressure[6]. Instead of using the channels' response times, this study's success criterion was a 0.5 second delay, as described in Section 2.7. 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 signal is generated within that window.

All of 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 encountered in 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 DI&C failure.

The assumptions and limitations of this study are discussed in more detail in later sections.

[6] 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.

3 SYSTEM DESCRIPTION

Chapter 3 provides a brief description of the Advanced Test Reactor (ATR) at Idaho National Laboratory (INL) with a focus on the loop operating control system (LOCS) of an experimental loop, which is the system used for this study. The descriptions in this chapter 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 researching 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 on nuclear fuels and materials.

The ATR core (Figure 3-1) has a serpentine arrangement that permits positioning 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 °C (125 °F), and flows upward through the annulus outside the cylindrical tank containing the core. The coolant then flows down through the core and, at full power, leaves the core with an average temperature of 71 °C (160 °F).

The core is composed of fuel plates arranged in 40 assemblies, each with 19 plates. These curved-plate fuel elements are arranged in a serpentine shape around a 3x3 array of primary testing locations. The ATR contains 68 experimental positions, and nine high-intensity neutron-flux traps, six of which are equipped with pressurized water loops. Each loop 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 experimental loop consists of three concentric loops (Figure 3-3). The assembly penetrates the vessel's bottom closure-plate; its inlet and outlet are 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 a needed insulating jacket because the inside of the pressure tube is in contact with the high-temperature loop coolant.

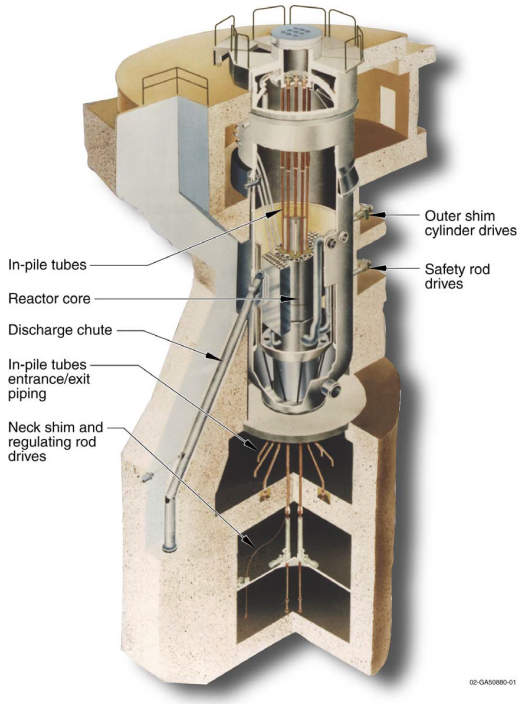


Figure 3-1 Location of the in-pile tubes in the ATR, and a cut-away view of the core

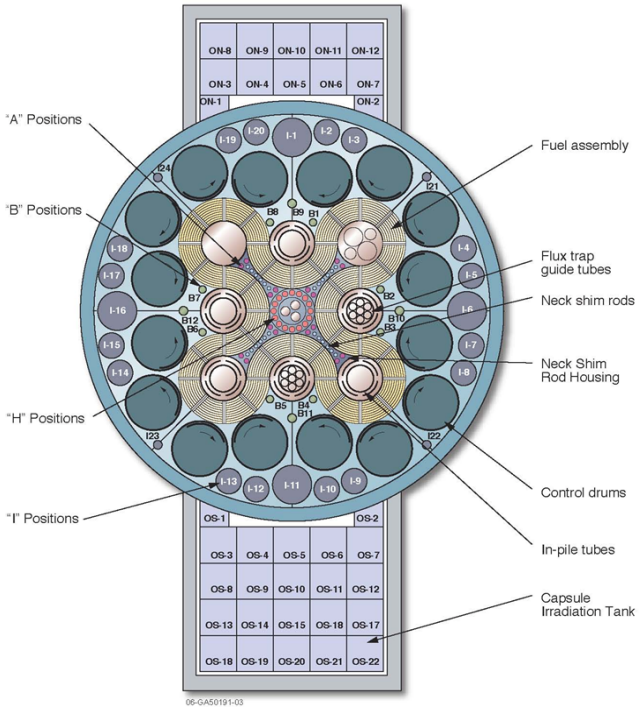


Figure 3-2 ATR's flux trap and irradiation test positions

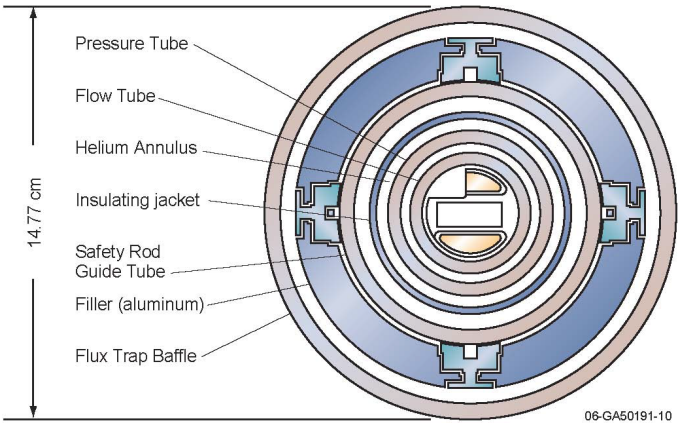


Figure 3-3 Cross-section of the in-core portion of a typical pressurized-water loop

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

3.2 Overview of the Loop Operating Control System

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

The major component of LOCS is the Metso Automation maxDNA distributed control system (DCS) that 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 the field signals into digital signals. The output modules convert the digital signals to interface with the loop equipment to, for example, start or stop a piece of equipment. The two pairs of DPUs (the A/B and C/D pairs) interface with the I/O modules to operate the loop equipment because 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.

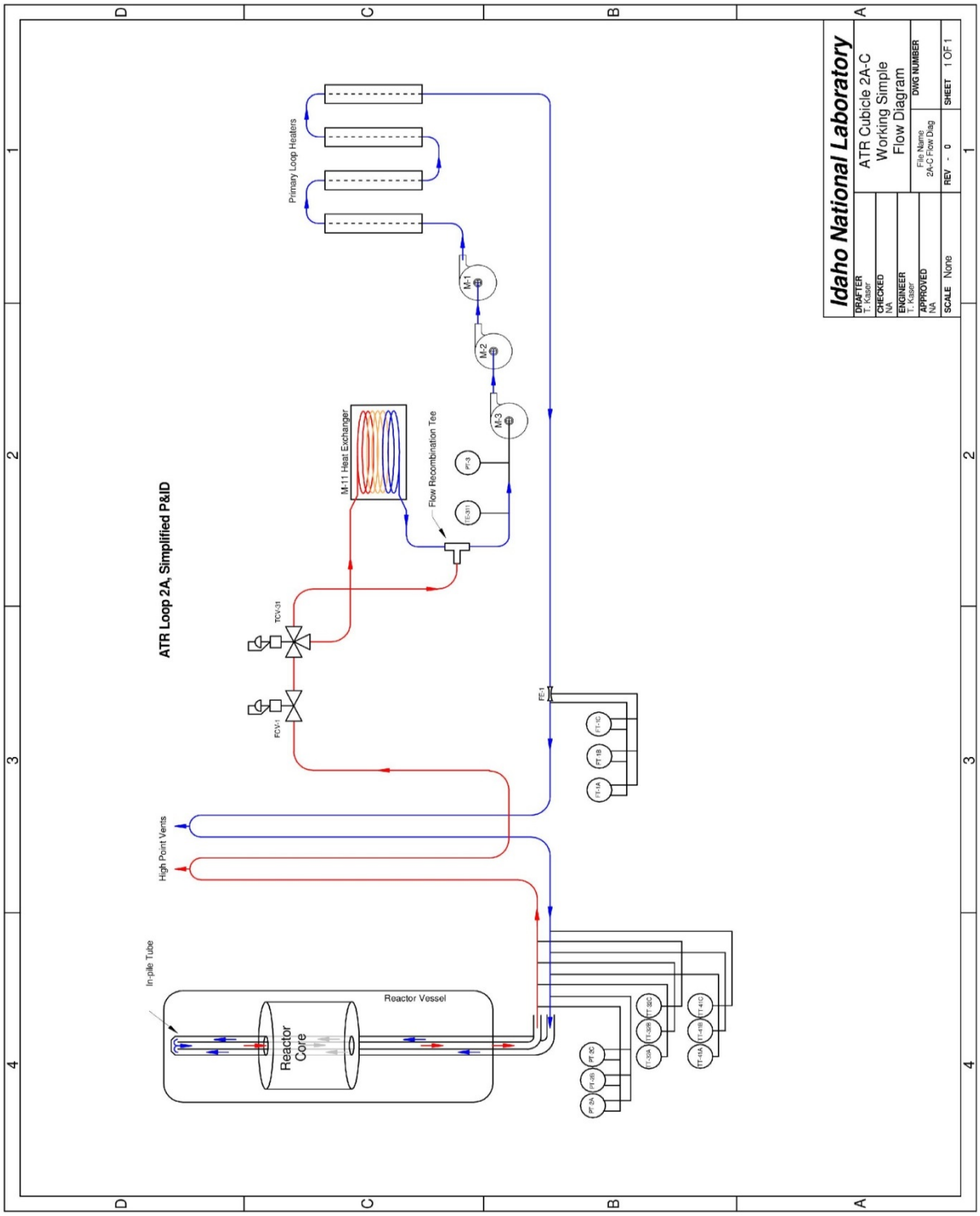


Figure 3-4 Simplified flow diagram of Loop 2A

3.3 LOCS Control Functions

The control functions of the 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 the LOCS include the primary coolant pumps, loop-line heaters, loop- pressurizer heaters, makeup pumps, purification-flow control valve, makeup system pump, and conductivity flow control. The process variables controlled by the LOCS are the primary coolant's flow rate, temperature, and pressure; the degassing flow rate; and the flow rate at the exchanger column.

The control of the primary coolant's flow rate consists of a PID (proportional, integral, and derivative) controller that 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 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 opens them on an input of 100%. Increasing the controller's output (opening the FCV) increases the loop flow. Figure 3-4 shows the location of the FCV in loop 2A.

The primary-coolant's 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's 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's 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 either on a loss of air, or an electrical signal. Decreasing the controller's output (0% output corresponds to a closed valve) lowers 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 determines 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. These valves close on the loss of either air or an electrical signal. Decreasing the controller's output, which closes the valve, reduces the flow. The valve automatically closes in the event of a high temperature in the ion-exchanger inlet. In addition to the processes detailed above, the LOCS similarly controls the pressurizer's level and the makeup system's 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 that, in turn, is connected to the DCS. Only one sensor is used for control at any time; the operator manually can select the one 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 a diesel at any given time. The pumps can be shut off (unless set in a bypass, or in the 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 up 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 makeup system's recirculation flow and level control are controlled by 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 sounds 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 loops' makeup pumps. The control valve for the storage tank level opens when it is low.

3.4 LOCS Protective Functions

The protective functions of the LOCS are designed to initiate mitigating actions to prevent damage to the loop's hardware and the installed experiments. The LOCS monitors seven process variables: (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 allowed only during a 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.

A low IPT inlet flow is detected via delta pressure. Rosemount 1151 Smart transmitters convert the signal into 4 to 20 mA 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 also are required for protecting the IPT. Their temperatures are sensed via 4-wire, platinum-type resistance-thermal-detectors (RTDs). Rosemount 3044 smart temperature transmitters convert the RTD signal to a linear 4 to 20 mA 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; however, this function can also be disabled if not required. Sensing is accomplished by registering the difference between the temperatures of the IPT outlet and inlet, which is calculated in the DCS. A low loop coolant-pump's power (low voltage) can trip the reactor

but it can also be disabled. Two under-voltage relays monitor the differential phase-voltages to each loop's 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 (AIM) B. The three scram channels are driven by three separate relay-output modules that are normally energized. With a trip from any of the 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 AIMs must be in a trip condition in order to trip the reactor.

To ensure the integrity of the DPU, a watchdog timer continuously checks the status of the DPUs. This 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. The LOCS connects to the reactor's PPS channels A, B, and C through the CLLC that provides the 12 VDC that the trip interrupts.

Figure 3-5 illustrates the connections involved in the protective function of the three TT-41 sensors (i.e., TT-41A, TT-41B, and TT-41C). The sensors monitor the temperature of the IPT inlet. 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 a 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's 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 normally should 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 a sensor/AIM, and a second is at the level of the digital-output modules.

RTD – Resistance Thermal Detector
PPS – Plant Protection System

Figure 3-5 IPT high inlet-temperature protection channel

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 Advanced Test Reactor's (ATR) probabilistic risk assessment (PRA) that was originally developed by Idaho National Laboratory (INL) defines the PRA context that was used to generate test scenarios for the Loop 2A Loop Operating Control System (LOCS). The reactivity insertion accidents in the PRA serve as the demands to the LOCS to generate a trip signal, and are used to generate test scenarios for statistical testing. This section describes the PRA model that was used to define and generate the test scenarios simulated using a RELAP5 [NRC 1995] model of Loop 2A (see Chapters 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 to the ATR's PRA to meet the study's specific needs[7]. Sensitivity and importance calculations were performed to gain insights from the model. Section 4.4 uses the PRA model for some risk-informed considerations regarding the necessary reliability level for the LOCS software and the number of tests without failure required to demonstrate this 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 Chapter 3, Loop 2A is controlled by its LOCS to maintain this 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 exceed 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 them. 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 the loop, which is a fast and large reactivity insertion. On the other hand, a trip of the loop's primary cooling pump may lead to a slower reactivity insertion. Loop 2A is modeled using two fault trees: (1) one that models potential reactivity insertion accidents due to failures of the components associated with the loop, including those of the LOCS (e.g., failure of the LOCS's pressure-control function), and (2) a fault tree that models the failure of the LOCS's protection functions (e.g., high inlet and outlet temperature, low flow, and low pressure) due to failures of LOCS components during reactivity insertion accidents[8]. The first fault tree is used to calculate the frequencies of

[7] It should be pointed out that BNL does not have detailed design information of the ATR, especially for the LOCS. The ATR's PRA was provided to BNL under export control limitations without any documentation except for those from a few conferences between BNL and INL to resolve questions directly related to modeling the LOCS. 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.

[8] The protection functions of the LOCS are designed for protecting the IPT, rather than the ATR core. Therefore, the use of some of the LOCS protection functions in the PRA to mitigate reactivity insertion accidents for the ATR core may not be appropriate unless the specific circumstances associated with the generation of a LOCS protective action during reactivity insertion accidents are considered.

different reactivity insertion scenarios (cutsets) that define the PRA context for the statistical testing of this study. The LOCS is modeled in two fault trees that are effectively intersected (ANDed) in the event trees' 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 subsumed within the same cutset 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 a conservative one 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 accident 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 (i.e., the inpile tube's low inlet flow, low inlet pressure, high inlet temperature, or high outlet temperature setpoints) are exceeded with a delay of 0.3 s of the system's maximum cycle time. (3) The LOCS generates a setback signal to insert the shim rods due to excessively high temperature of the specimens or high coolant differential temperature of the IPT. The trip signals generated by PPS and LOCS activate the insertion of the same control rods while a setback signal would activate the insertion of a different set of rods that may require a 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. Failure of the LOCS to generate a reactor trip signal is modeled in terms of failures of its components. For example, the 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 these accidents and the associated core-damage frequency. Section 4.3 details the modeling of the PRA used to calculate the 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 Loop 2A equipment. A separate fault tree is used to model the protection functions of the LOCS. Section 4.3.1 describes the event tree for reactivity insertion accidents associated with experimental loops and the fault trees associated with different ways a reactor trip signal can be generated. Section 4.3.2 describes the fault tree that models reactivity insertion accidents, while Section 4.3.3 describes the changes that were made to the PRA model to fit the needs of this study, including the event tree that models the LOCS. Section 4.3.4 discusses some results of the analysis, including risk contributions from LOCS failures.

4.3.1 Description of Reactivity Insertion Event Tree

Figure 4-1 shows the original RLH[9] 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

[9] RLH and the later RLHIE are names used in INL PRA. They are not acronyms.

RLHIE that includes events related to all six experiment loops but, unless otherwise stated, only those events related to loop 2A are considered in this report. The RLH event tree is set up such that should there be a reactivity insertion, the LOCS protection is first queried to determine whether it can trip the reactor. Failure of the LOCS protection function is modeled using the LOCS fault tree and considers failures of the LOCS hardware (e.g., the data-processing units (DPUs)), sensors, and AIMs; other failures including mechanical failures and those of the rod clutch control system (RCCS); and the common cause failure (CCF) of divisional logic. The mechanical failures include individually stuck control 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 rods 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, manual shutdown and slow insertion (MRSR) can trip the reactor. If an event fails the LOCS, SLH, and MRSR, then ultimately it leads to core damage (P4 state in RLH). Even with a successful trip, the loss of long-term cooling might also lead to core damage. These events are developed further via the transient event tree that transfers off some branches in the RLH.

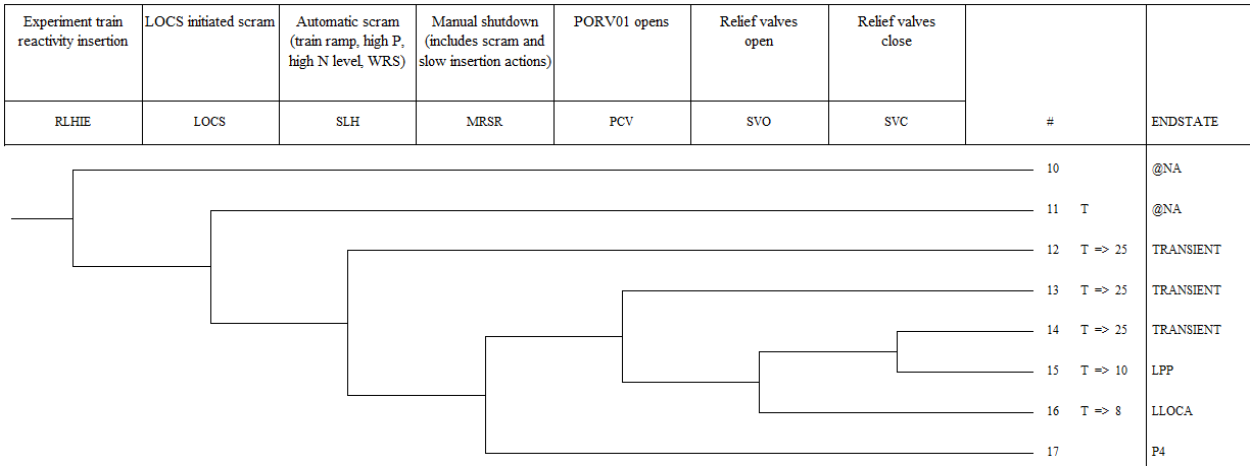


Figure 4-1 The RLH event tree in the original PRA model

In the PRA model, the LOCS and SLH use the same fault tree, while flag sets[10] are used to select the appropriate branch when solving the event tree sequences. LOCS and SLH share some events, such as a stuck rod, whereas LOCS-specific subtrees simply are de-selected when solving the SLH. The MRSR tree also partially shares subtrees with the 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 is essentially a mechanism to reduce the power of the reactor after an event. This is achieved via a rotating drum with neutron absorbers covering half of it. Normally, the absorber face points away from the core but, on demand, the drums rotate the absorber's face towards the core, thereby reducing neutron flux. A typical demand for the slow-insertion system occurs when the

[10] A flag set is a feature of the SAPHIRE code. It is a set of user-defined changes 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.

temperature of an experiment specimen is too high. In this situation, a reactor trip may not be immediately needed, and slow insertion can be used to reduce the reactor's power to lower the specimen's temperature to an acceptable value. The time needed for reducing power is typically several minutes. Accordingly, for events that need a faster reactor trip, the MRSR tree cannot be credited.

Section 4.3.3 describes modifications that were made to alter some of the above logic to account for accidents in which some of the trip system features were not credited for the purposes of conducting statistical testing of the LOCS system.

4.3.2 Description of the Reactivity Accident Fault Tree

This section discusses in detail 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 with different basic events. Failure in the top event of any of these subtrees results in an RLHIE failure (i.e., the subtrees are joined via an OR gate). This sub-tree includes all events in loop 2A that will lead to reactivity insertions. Figure 4-2 shows the top portion of EXT-2AC-AQU which has three subtrees: failures of the flow equipment (EXT-2AC-FEQ), failures of the temperature equipment (EXT-2AC-TEQ), and failures of the pressure equipment (EXT-2AC-LPEQ).

The EXT-2AC-FEQ subtree models events that can cause low flow in loop 2A. This condition increases the loop temperature that ultimately can lead to reactivity insertion via voiding (the 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 locations are modeled as three separate events. Similarly, EXT-2AC-TEQ addresses events that directly increase the temperature. It includes failures of the line-heater control and the temperature-control valve. Subtree EXT-2AC-LPEQ includes events that cause the loop pressure to drop, including pipe breaks and failure of the pressurizer heater. Table 4-1 shows all events in these three subtrees; some events therein may be caused by several different failures. For example, event "temperature control component failure" can be caused by a failure of the DPU pair, the AIMs, the analog output modules (AOMs), or other components of the temperature-control system.

Some component failures can cause multiple failures of both the control functions and the protection functions. For example, failure of the DPU pair leads to a simultaneous loss of the control of temperature, flow, and pressure. One extreme example is failure of the DPU power-supply elements such as transformers, buses, or batteries that can lead to loss of power to the DPU and cause the entire LOCS to fail.

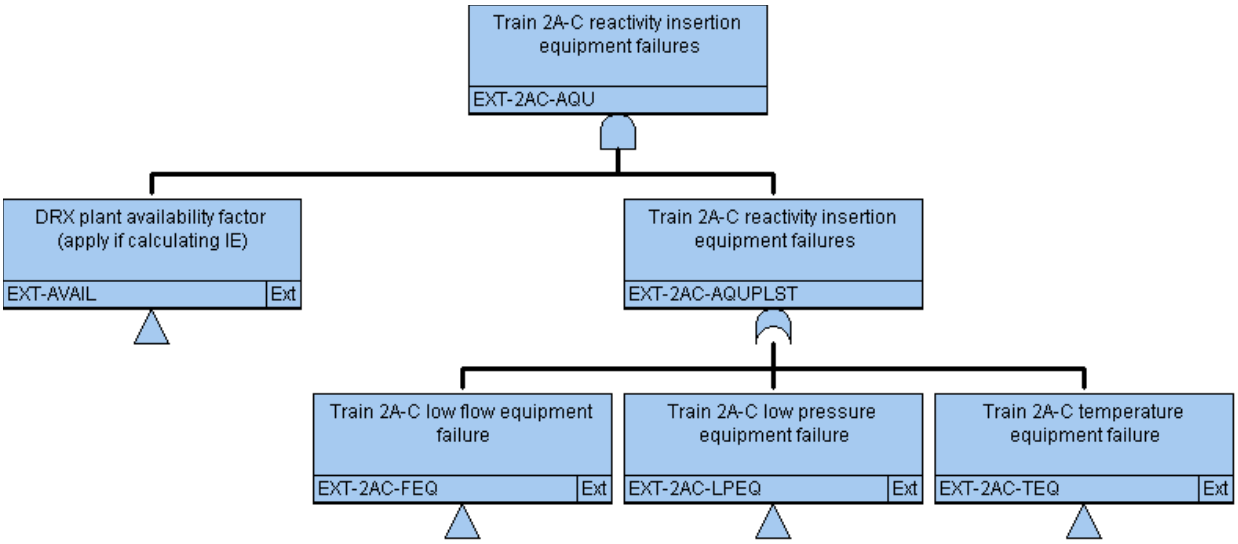


Figure 4-2 Loop 2A reactivity insertion fault tree

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

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

4.3.3 Modifications to the ATR PRA

Several modifications were made to the initial PRA model for the purposes of this study. The following lists the changes that were made.

Changes to the RLH event tree (reactivity insertion originating from experiment loops)

A large LOCA (LLOCA) in the loop 2A piping can lead to a very fast reactivity insertion. The insertion can occur fast enough that there is insufficient time for the LOCS to trip the reactor. Similarly, the results of the RELAP5 simulations were reviewed to identify cutsets that would lead to fast reactivity insertion rates (i.e., a trip would be required within 3 minutes). For simplicity, it was assumed in this study that since a trip must occur within 3 minutes, slow insertion would not be a valid means of reducing the reactor power because slow insertion requires more than 3 minutes and therefore cannot be credited in the PRA in this situation.

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 situations in which the reactor has three mechanisms that cause it 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 at least 3 minutes after the accident is initiated. Branch 2 (sequences 18 and 19) represents the LLOCA case. Here, neither the LOCS, which requires at least 0.3 s to generate a trip signal, nor slow insertion is fast enough to trip the reactor in time to prevent damage to the core. 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 0.3 s. 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 wherein 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 between 0.3 s and 3 minutes. In generating test scenarios, only branches 1 and 3 were considered because the LOCS cannot mitigate branch 2.

Table 4-2 shows the assignment of 13 failure effect categories to branches 1 and 3 of the event tree (Figure 4-3) [11]. The categories were used to group the effects of failures and developing probabilistic failure process models as described in Section 5.2.2. Table 5-1 of Section 5.2.2 gives more information about each category.

Because some of the reactivity insertion cutsets involve multiple failures, those that do so were assigned to the branches based on the failure effect with the earliest trip time. For all cases, a SAPHIRE linkage rule was used to assign different cutsets to one of the branches.

Table 4-2 Assignment of failure effect categories to branches 1 and 3 of the event tree

Branch 1 (>180 s)	Branch 3 (<180 s)
• Loss of heat exchanger cooling (gRFW130) • Temperature control components failure – Input (gTctrlHI) • Temperature control components failure – Output (gTcrlHO)	• Flow control components failure – Input (gFctrlI) • Flow control components failure – Output (gFctrlO) • 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 failure effect categories in Table 5-1. From these results, the earliest trip time was recorded for each category. If this time was less than 180s, then the category was assigned to Branch 3. Categories whose earliest trip time exceeded 180s were assigned to Branch 1.

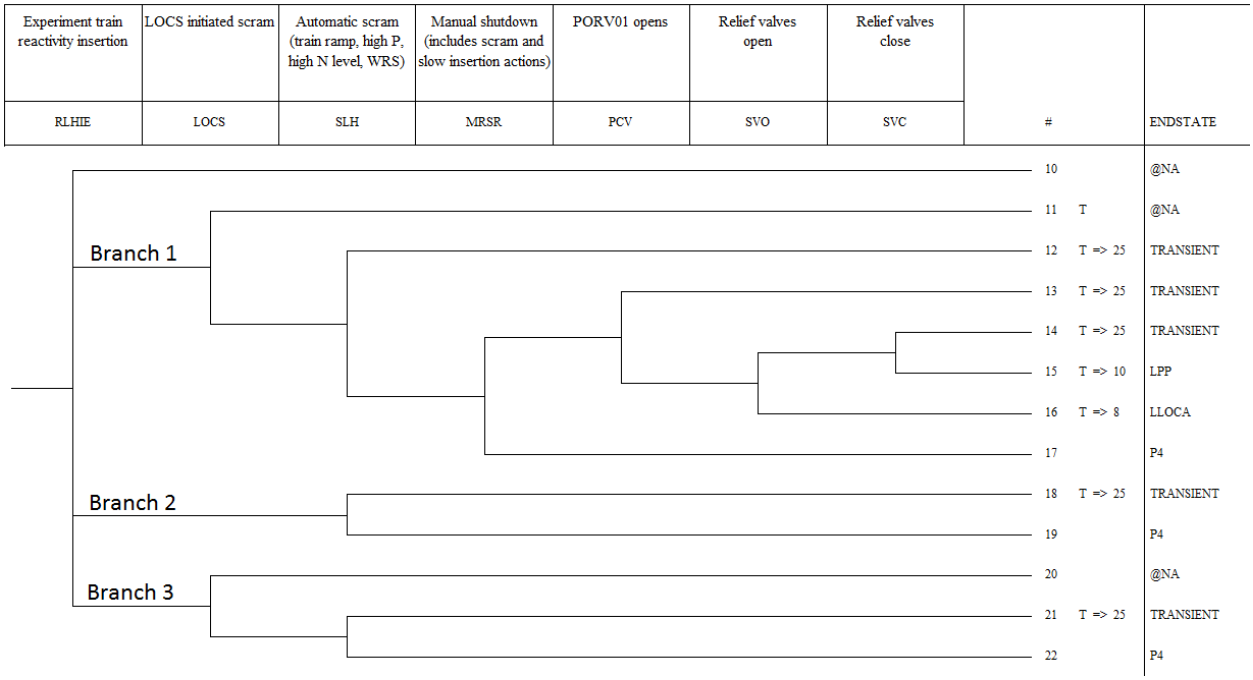


Figure 4-3 Revised reactivity insertion event tree

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

1. In the original PRA model, each cutset of EXT-2AC-AQU has a basic event that effectively multiplies the cutset frequency by 365 to convert it from the per-day frequency to the per-year frequency. However, for cutsets containing multiple failure-to-run events, multiplying by 365 implies that only one component needs to run for 1 year, while the remaining components need to run for only 24 hours (i.e., the PRA mission time). This approach assumes that the first component failure is immediately detected and the reactor is shut down (and all component failures cease 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, an additional multiplicative factor of 365 was included to account for exposure times beyond 24 hours.[12] This is a conservative assumption for the purposes of this study. Events of the on-demand failure type (e.g., failure to start a pump) do not have the corresponding multiplicative factor of 365.

2. Common-cause basic events, for the AIM and sensor failure, and for the sensor's mis-calibration events are included in the fault tree modeling of the protection function of LOCS, but not in the tree for the control function (EXT-2AC-AQU). To maintain consistency, these events were also added to the control function tree.

3. AIMs 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

[12] It was conservatively assumed that a component failure will not be detected (automatically or by periodic tests) such that it can be repaired or replaced. Otherwise, the mission time for the failure-to-run events could be shorter.

system is set to use the last-known value of component failure, and this should not lead to reactivity insertion. However, if a perturbation occurs while the control signal is 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, AIMs 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. They were not included in the original fault tree as they are analog-output modules. However, in this study, they were added to the fault tree.

5. Distributed processing units are needed for the LOCS control function. Like the AIMs and sensors, they were not included in the original fault tree. The DPUs were added to the fault tree to appropriately model the control functions for the purposes of this study.

6. Even though two of the analog-input modules can be selected to process the sensor signals to be used for the LOCS control function, only one input module is employed at any given time [Marts 2012]. Also, there is no automatic switching upon failure of the module in use. Therefore, only one module was credited in the revised PRA.

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 the failure of LOCS to trip the reactor. Therefore, the modules were added to the fault tree representing the protection function of the 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 request for a response. If the DPU fails to respond in five seconds, the watchdog will initiate a trip signal. Since the LOCS has two DPUs for each experiment loop (an active and a backup DPU), a failure to trip from a watchdog will occur only 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 the 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 to generate 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. The rest of this subsection further discusses the results.

Table 4-3 Summary of PRA calculations

	Frequency of reactivity accidents from experiment loops per year	CDF/yr
Total of ATR	1.75 (1.9)	2.4×10^{-6} (3.0×10^{-6})
Loop 2A's contribution	0.97	6.46×10^{-7}
Loop 2A LOCS control function's contribution	3.4×10^{-2}	9.3×10^{-8}
Loop 2A LOCS protection function's contribution	NA	4.0×10^{-8}

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 0.97 per year. It includes the failures of both LOCS components and those of the non-LOCS loop hardware (e.g., pipe clogging and failures of components originating from the secondary side). The frequency is dominated by the non-LOCS loop hardware failures. The total reactivity insertion frequency caused by all 6 experiment loops is approximately 1.9 per year[13].

As described in Section 4.3.3, the Loop 2A reactivity insertion events are divided into three groups, each corresponding to a branch in the event tree in Figure 4-3. Group 1 contains events wherein the trip setpoint is reached after 3 minutes. Here, LOCS, PPS, and power setback can be credited for preventing damage to the core. Group 3 contains events in which 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 was 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[14], 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 the failure of the temperature sensor (26%), AIM failure (28%), and AIM failure (14%). By contrast, the failure of the secondary loop's 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 Loop 2A total frequency.

In this study, the first 200 dominant cutsets of the Loop 2A-related reactivity accidents were used to generate the test scenarios. 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 the basic events.

[13] Approximately 80% of the frequency is from cutsets involving the 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. 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.

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

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 to analyze 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 (e.g., station blackout). 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 that caused reactivity insertion accidents. It includes the contributions from failures of LOCS components (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 a strainer plugging up, leading to a reactivity insertion, together with a common-cause failure of the safety rod, which leads to a failure to trip. The latter 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 that eventually results in core damage. The second most dominant cutset (6%) is a strainer plugging with a trip failure caused by a common-cause failure of the trip's division logic. (The division logic is used to transmit a trip signal to the rod's clutch-control system.) Note that the contribution of Loop 2A to total CDF is dominated by cutsets that are not a part of the LOCS. The contribution of LOCS components are discussed as follows.

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 significant changes were made to the event tree associated with loop 2A. 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 the total CDF. As described previously, 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 ATR CDF around 3×10^{-6} 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 (e.g., pipe clogs in Loop 2A) were removed from the calculation of the loop 2A contribution described above by setting their probability to zero and re-quantifying the CDF cutsets. The change in total CDF, 9.3×10^{-8} per year, is the contribution to total CDF from loop 2A's control functions, 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. In this cutset, the sensor is used only by the control functions of the LOCS, not the protection functions, making the former more important. The next three dominant cutsets (11% each) involve the failures of the various analog input and output modules, together with the common-cause failure of the safety-rod group. The modules also are mostly associated with the control function only.

Similarly, the contribution to total CDF of non-LOCS loop 2A hardware failures (e.g., pipe breaks, plugging) and LOCS failure due to failure of the supporting system, which is calculated by assuming that the LOCS hardware failure probability is zero, is 5.53 x 10-7 per year. The top two

dominant cutsets here are the same as those in the second case described above (i.e., the loop 2A's 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 the total CDF

The LOCS protection functions are always backed up by the PPS; therefore, its contribution to the total CDF is very small (4.0×10^{-8} per year). The main difference between the contribution of LOCS control function and the protection function is due to those LOCS components that are only used by the control functions, as described in the preceding paragraph.

4.4 Assumptions and Limitations of the Application

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

1. BNL has neither complete documentation for the ATR PRA nor the design information needed to undertake a detailed review of it. Therefore, BNL worked with the SAPHIRE7 model and concentrated on the part of the SAPHIRE model related to the LOCS. A few conference calls were held with INL's staff who are familiar with the PRA and the RELAP5 model to resolve some questions BNL had. Thereafter, BNL made some changes based on their understanding of the system and the reactor for the purposes of this study. The most significant one is the success criteria associated with those systems that can be used to generate a reactor-trip signal. As a result, the strainer-plugging model became an important contributor to the CDF.

2. BNL did not change the modeling of other experiment loops that were modeled in the same way as was Loop 2A in the PRA. Approximations were used as described in Section 4.3.4 in estimating the effects on total CDF if the loops had been modified.

3. The PRA assumes that the LOCS designed to protect the experiment can also mitigate reactivity insertion accidents. That is, the LOCS' trip setpoints 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 scenarios 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 process models (PFPMs) was necessary to capture the variability of the failure effects (e.g., reduction of coolant flow due to a pump

trip) by characterizing them in terms of parameters with uncertainties. The choice of parameters and their probabilistic distributions can be improved by conducting engineering analyses and possibly collecting data on the effects of failure. For example, in case of a pump trip, research can be done on the possible variation in the pump's coastdown curve. In addition, past experience of pump trips may provide useful information on how the flow changes with time.

7. BNL used the first 200 cutsets of the fault tree for reactivity insertion accidents involving Loop 2A. The cutsets contributed 99% to the frequency of the top event and covered all the primary components modeled in the RELAP5 model. In general, the approach can be extended to a larger number of cutsets that contain additional conditions for the LOCS. The effort required would increase proportionally. The tradeoff between the testing fidelity and required effort would vary case by case and is recommended as a future study.

5 GENERATING TEST SCENARIOS USING THE RELAP5 MODEL

This Chapter describes how the Loop 2A RELAP5 [NRC 1995] model was used to generate the test scenarios for the loop operating control system (LOCS). The RELAP5 model provided by Idaho National Laboratory (INL) was revised for this study to simulate the PRA scenarios and their associated variations (e.g., LOCA sizes and locations). The INL RELAP5 model does not contain details of the loop components that are necessary to fully analyze the operational contexts defined by the probabilistic risk assessment (PRA) used in this study. For example, the secondary side that supplies cooling to the loop through a heat exchanger was not modeled. Because the secondary-side failures are the dominant contributors to the reactivity insertion scenarios, the PRA model was revised by including the secondary heat exchange in the PRA. In addition, the cutsets from the Advanced Test Reactor's (ATR's) PRA do not specify exactly how the failures would affect the physical condition of Loop 2A. BNL developed probabilistic failure process models (PFPMs) that are used to specify the failure effects and their possible variations. These limitations and associated assumptions do not impact the usefulness of this study in demonstrating the statistical testing method for the LOCS system.

Section 5.1 describes the RELAP5 model INL provided and the changes that BNL made to facilitate this simulation study. Section 5.2 describes how the failure events defined in the PRA are simulated and how they can be grouped based on their failure effects. It also describes how the PFPMs are used to model variations of the scenarios. Section 5.3 summarizes the key assumptions and limitations of the RELAP5 simulation.

Chapter 6 describes how the test scenarios were sampled from reactivity insertion cutsets generated in Section 4.3, and how the RELAP5 input decks[15] were automatically prepared for each of the test scenarios. The outputs of the RELAP5 runs then were used as input to tests of the LOCS, as described in Chapter 7.

5.1 RELAP5 Model of Experimental Loop 2A

This section describes the original RELAP5 [NRC 1995] model provided by INL, changes made by BNL, and 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 control variables representing safety-related signals used by the LOCS and associated reactor-trip setpoints. The signals include measured loop coolant temperature, pressure, and flow rate. The trip setpoints are specified for low and high temperatures, low pressure, and low flow rate. Additional control variables representing the control functions of the LOCS are included. 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's primary side is not available to BNL, and is therefore 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 reactor's primary side are not modeled, which means that any feedback from the experimental loop to the primary loop cannot be represented.

[15] In early days, computer input data were prepared with a deck of punched cards. The term "deck" has been used to describe a set of computer-input data.

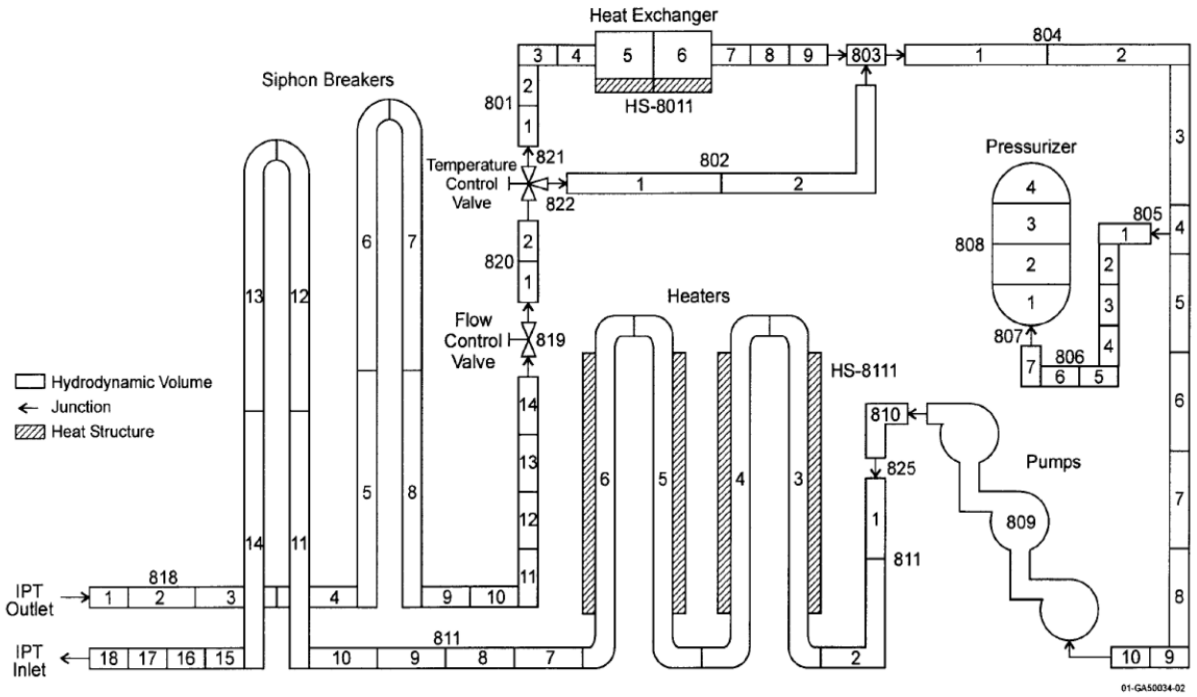


Figure 5-1 RELAP5 nodalization of the original model for the out-of-pile loop piping

The RELAP5 model of Loop 2A was not designed for generating test scenarios 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 insertion 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 from INL was revised to add some control functions to better meet the needs of this study. It should be noted that thermal hydraulic models initially developed to investigate design basis accidents often lack detailed models for some control systems. However, when such models are used to develop a realistic operational context for software testing, it is necessary to include these systems to ensure that temperature, pressure, and flow data represent expected conditions. Consequently, BNL added the following control functions:

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

2. Pressurizer-level control.

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

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) filled with water during the steady state, and has no room for steam. During a transient run, the original model adds an additional node containing steam to the pressurizer. To avoid having to modify the pressurizer for each transient run, the model was changed such that three additional nodes were added to component 808 (pressurizer) in the steady-state input deck. These nodes contain gas (steam) to allow for the expansion of water.

2. The 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 scenarios for the statistical testing method (STM).

4. Control variables were added to output both the engineering unit and the electric current unit of the pump's inlet pressure. These outputs were requested by INL for their test execution.

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 loss-of-coolant accidents (SLOCAs).

7. To simulate pipe plugging, the PIPE components were modified by adding a single junction at three locations (at the IPT inlet and outlet, and at the strainer). The single-junctions were placed between the 17th and 18th nodes of Component 811, the 1st and 2nd nodes of Component 818, and the 1st and 2nd nodes of Component 804. This was done by splitting each of these components into two separate ones. Pipe plugging was simulated by reducing the flow area of a specific single junction during a transient run.

8. To facilitate certain sensitivity calculations, a control logic was developed to terminate transient runs in order to avoid running transient cases for a very long time. This control logic stops RELAP5 running 1800 seconds if no reactor scram signal is generated after a deciding variable has changed by 10% from its initial value.

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

10. A valve (Component 865) and a time-dependent volume (Component 866) were modeled and connected to the top of the pressurizer to adjust the system's pressure to a desired pressure during steady-state runs. For transient calculations, the valve (Component 865) is closed.

Figure 5-2 Shows the nodal diagram of the modified RELAP5 model for Loop 2A.

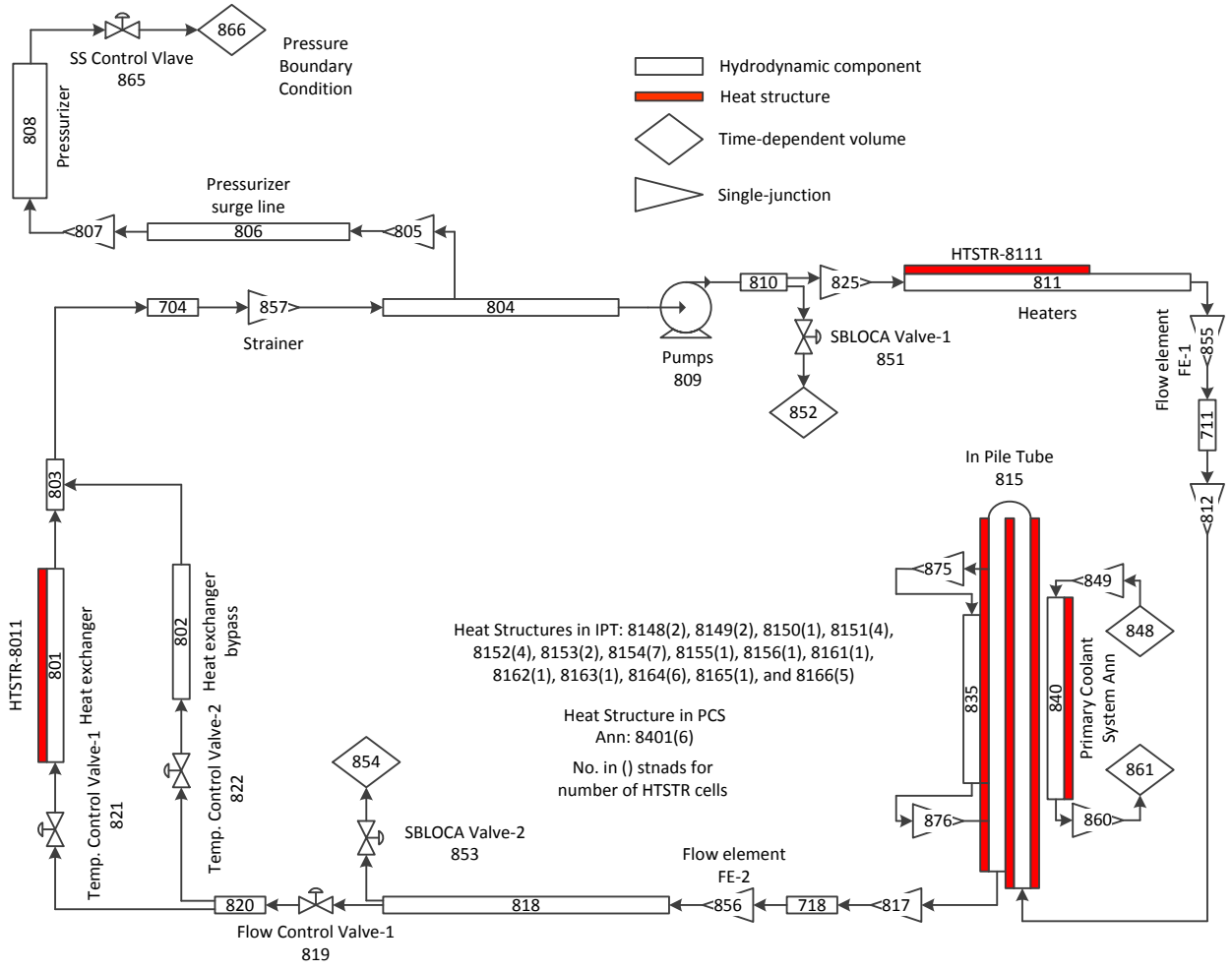


Figure 5-2 RELAP5 nodalization of the modified model for Loop 2A

The modifications above do not add control functions for the loop pressure and the temperature-control valves nor were any components for the secondary loop added. The main reason is that BNL does not have the requisite design information to model these components and control functions; including them in the model would involve assumptions that might 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 realistically predicted. For any one accident scenario,

more than one control function[16] may respond to compensate for the deviation from steady state. For example, an accident leading to low flow will most likely involve the flow control function opening the flow-control valve in an attempt to increase flow. If the low-flow situation also leads to an increase in pressure, then the pressure control function also will respond. The simultaneous responses from these two control functions may take the system in a trajectory that differs 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 the scenarios in which the model will accurately predict the system's behavior.

In addition to the limitation of the control functions, the lack of secondary-side modeling restricts the type of scenario that the model can represent. A majority of the cutsets of events leading to reactivity insertion from loop 2A are events involving the failure of secondary-side components (e.g., failure of secondary-flow control, failure of secondary coolant pump, and loss of secondary inventory). The exact trajectory of the primary loop's state will vary with the type of secondary failure. Specifically, the temperature change rate of the primary coolant differs for different scenarios involving secondary components. However, the use of a bounding temperature to represent the secondary side means that all scenarios must be approximated using this representation. For example, the scenario in which there is a pipe break in the secondary-side loop is expected to evolve differently than the case in which a secondary pump fails. Yet the lack of representation means that these two scenarios are both modeled using the changes in the heat transfer coefficient. 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 the flow will need to be reduced for the reactor to experience a reactivity insertion. For this project, it is assumed for simplicity that any scenario leading to IPT voiding will introduce enough reactivity that the LOCS is not 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 by considering the LOCS's cycle time such that LOCS can generate a trip signal in time.

The assumptions described in the preceding paragraphs were used in the manner listed below. They are used to determine whether the LOCS can be used to mitigate different reactivity insertion scenarios. Only those scenarios that LOCS can mitigate were used in the simulation with the results defining the test scenarios.

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

2. For a SLOCA case, if a scenario occurs in which the setpoint is reached within 0.3 s 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 and that LOCS is allowed to trip at or after 0.3 s. Scenarios in this group were simulated.

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

3. If a SLOCA case occurs in which the setpoint is reached within 0.3 s, and voiding of the IPT also occurs within the same time frame, then the LOCS cannot be credited with preventing core-damage. Scenarios in this group were not simulated.[17]

5.2 Modeling of Reactivity Insertion Cutsets with RELAP5

There are a few issues associated with modeling 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 process models.

5.2.1 Issues Associated with Modeling of PRA-Defined Reactivity Insertions

RELAP5 Model Enhancement

The original Loop 2A RELAP5 model does not model many cutset components. In these cases, 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 the same failure effect categories. Section 5.2.1 discusses in detail how these categories, which were mentioned briefly in Section 4.3.3, were constructed. These categories enabled such component failures to be included in the simulation. 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 failure effects were developed and represented by 13 failure process models. They are described in Section 5.2.2.

The absence of control systems for loop pressure in the RELAP5 model precludes the direct modeling of cutsets associated with failures of pressure control components (e.g., loss of pressure sensor). For pressure sensors, a false high failure when the actual pressure is low will lead to a reactivity insertion. This scenario will leave the initial low pressure uncompensated, and may lead to the pressure control system reducing the pressure 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 the positive void coefficient of the reactor. Therefore, it is important to apply a method to simulate the pressure control system in the RELAP5 model to analyze scenarios involving the failure of pressure control components.

One way to model a pressure sensor failure or the equivalent 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, BNL introduced a randomly sized pipe break (to simulate a random rate of pressure decrease) at a pre-specified location to simulate the equivalent pressure-drop. Notably, this approximation means that modeling the pressure-sensor failure is identical to modeling a small-pipe break. Accordingly, the pressure sensor failures and the pipe break are grouped together.

[17] In the PRA model, it is assumed that the LOCS can mitigate a SLOCA.

Mapping PRA-Failure Events to the RELAP5 Model

A PRA model typically models the failure modes of generic components, such as "pump fails to continue running." In some cases, a failure mode may be as simple as "the component failed." In this STM study, once a component failure event is selected, it is necessary to specify how the component fails in the RELAP5 model. For example, if a valve closes spuriously, the position of the valve, which determines the flow area through it, as a function of time must be specified since the different flow area represents a different scenario. For example, a fully opened valve may spuriously close to a half-open position in one scenario and to a fully closed position in a different scenario. Therefore, a random variable representing the flow area is used to model the valve-closure event. Each time this event is simulated, a value from this random variable is sampled. In this study, thirteen failure effect categories were developed and uniform distributions were assumed for the random variables. Engineering considerations and judgment were used to assess the parameters. Each category is characterized by a probabilistic failure process model. Examples of the random parameters include valve-flow area, break area, pump-stop time, and flow-plugging fraction. Section 5.2.2 discusses the assessments of the random parameters for each category.

PRA Cutsets May Include Failures with Multiple Failure Effects

In the PRA model of the reactivity insertion events, some of the cutsets may contain failures of support system components that may cause failures of multiple control functions, each with a different effect on the thermal hydraulic condition of the loop. Therefore, one component failure event may have failure effects that are applicable to more than one failure effect category.

5.2.2 Categories of Failure Effects and Their Associated Probabilistic Failure Process Models

In this section, thirteen categories of failure effects and their associated probabilistic failure process models are detailed. Table 5-1 shows these thirteen categories. It also shows the upper- and lower-bounds of the uniform distributions used to model the variability of the failure effects. This section provides details of how the probabilistic failure effect models were developed. Appendix A provides a mapping of the 200 reactivity insertion cutsets to these categories.

Note that some of the following categories contain subcategories specifying how a component fails. Each individual failure mode should be associated with a unique subcategory. If a subcategory was not specified, then a sub-category was selected randomly under that category when sampling from its associated group, and a sample is taken from the selected subcategory.

(1) Loss of Heat Exchanger Cooling

A majority of the reactivity insertion cutsets include failures that cause a loss of heat exchanger cooling (i.e., loss of heat transfer to secondary loop) for the loop 2A. These cutsets account for approximately 80% of the total frequency of loop 2A's annual reactivity insertion frequency. The heat exchanger is the primary means by which loop 2A is cooled, and its loss eventually leads to an increase in the coolant's temperature. A variety of failures can cause a loss of cooling, such as loss of makeup water to the secondary loop, failure of the secondary pump, failure to close the secondary side flow control valve, or failure of the secondary flow-control system.

Table 5-1 Probabilistic modeling of failure effect categories

No.	Failure Effect Category	Subcategory [Frequency of Subcategory]	Parameter	Lower Bound	Upper Bound
1	Loss of HX cooling	-	Time at which the heat transfer coefficient reaches zero. [s]	0	1670
2	Pump Failure	Trip [49%]	Multiplication constant to the time variable for the pump's coastdown curve	0.5	1.5
3		Seizure [51%]	Time for pump to reach complete stop [s]	0.001	2.04
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) [flow area ratio]	0	0.382423
11	Loss of line heater control – input	-	CV-1 (490°F - Temperature sensor input) [°F]	45	490
12	Loss of line heater control – output	-	CV-4 (Line heater controller output) [W]	1.799637E+05	2.16E+05
13	Loss of TCV control	-	Time for valve TCV-3-1 to be fully closed. [s]	15	45

Since the INL RELAP5 model does not model the secondary side of the test loop, BNL modified the existing parameters to approximate the failure effects of components there. That is, BNL decreased the heat transfer coefficient (HTC) between the primary and secondary sides to zero to approximate the failures of the secondary components. This decrease is not a jump drop; rather, it is a linear decrease from the initial steady-state value to zero over a period of time. The zero-HTC implies the same coolant temperature in the secondary system as that in the primary system, no flow in the secondary side, or that the secondary system is filled with gas. The period of time of decrease is a random number within a certain interval (Tables 5-1 and 5-2). This randomness is intended to simulate the different effects that the different secondary side components failures have. The lower bound of the random number indicates a simultaneous termination of heat transfer to the secondary side and represents events such as a large pipe break in the secondary loop. The upper bound was chosen using a RELAP5 sensitivity calculation wherein the time at which HTC becomes zero was varied, and the upper bound was determined so that the trip setpoint would be reached within 30 minutes from the start of the transient. It is assumed that if a trip is not needed 30 minutes into the accident, the operator would have recognized it and manually terminated it. Based on this assumption, for all failure effect categories, 30 minutes was

[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, it was assumed that there is an equal probability of plugging at all three locations.

the maximum time for which the scenarios were simulated; events leading to a trip setpoint after 30 minutes were not considered. Table 5-2 summarizes how the upper- and lower-bounds were selected for the 13 failure effect categories.

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

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 a 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

(2) and (3) Pump Failures

Cutsets that lead to the stoppage of the loop 2A pumps were assigned to the pump failure category. These cutsets are further categorized into two subcategories (i.e., the Trip and Seizure subcategories), depending on how they affect the pumps. A loss of power to a pump will lead to a pump trip, while a stuck pump shaft will result in a pump seizure. The Trip subcategory 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 coastdown curve. To simulate the variation in the coastdown curve, randomness was introduced by multiplying the independent variable (time) by a random number sampled between 0.5 and 1.5. That is, it was assumed that the coastdown time can be higher or lower by up to 50%.

The Seizure subcategory represents events that cause the pump to come to a sudden stop. It was modeled by assigning a linear coastdown curve/line to the pump. In a normal coastdown curve, the pump's speed initially decreases very quickly before decreasing slowly. It was assumed that the fastest seizure occurs in 0.001 second. That is, the pump speed decreases from the normal speed of 3600 rpm to zero in 0.001 seconds. The 0.001 second is the lower bound of time to zero speed. An upper bound of time to zero speed was selected by assuming the pump's speed decreases linearly at a rate equal to that occurring in the first second of a normal coastdown. That is, in the first second of a normal coastdown, the pump speed's decreases from 3600 rpm to 1832 rpm in one second. Assuming the rate of decrease in speed remains constant, the pump would reach zero speed at 2.04 seconds. The time to zero speed represents the probabilistic failure process model of a pump seizure

The probabilities of the trip and of the seizure subcategories are 49% and 51%, respectively. The PRA model does not specify the failure modes of these subcategories, so it was assumed that their frequencies are 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's location and reducing the flow area of this single-junction. The final area of the junctions (i.e., the flow area after plugging) is a random number between zero (complete plug) and an upper limit that was chosen so that the flow rate remains below the trip setpoint for longer than 1 second. For flow areas 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 would not cause a trip. In some cases, the flow rate is calculated from RELAP5 oscillations near the trip's setpoint and it does not stay below it 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

There is only one pipe-break event in the PRA model. However, based on physical considerations, its impact is expected to differ depending on its break location. Two locations were considered: the IPT's inlet and its outlet. For simplicity, an equal probability that the break occurs at either location was assumed. The break was modeled in RELAP5 by adding a normally-closed valve at the location. The valve is opened to initiate the break. The random parameter is the valve's 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 size such that voiding in the IPT occurs at least 0.3 s after the break. Note that for break sizes 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 given no IPT voiding occurs.

(9) Loss of Flow Control-Input

Events that were assigned to this category are those that affect the input to the LOCS flow controller. They include the failures of the flow sensors and the AIMs. The PRA model does not specify the modes of failure of these components. In this study, BNL assumed the failure modes are ones that lead to the most severe consequences. Flow sensors were assumed to fail high, causing the controller to (incorrectly) reduce the flow rate. The lower rate eventually will cause a high temperature in the loop, and if a high-temperature trip does not occur, it will eventually lead to IPT voiding that, in turn, 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" category were modeled in RELAP5 by modifying control variable 240 (CV-240) that receives the mass flow rate as an input and processes it to generate an output variable that determines the position of the flow control valve (i.e., the flow area). To simulate events in this category, the connection from the mass flow rate to CV-240 was replaced by a random number assigned as input to CV-240. This random number lies in a range that ensures that the trip setpoint occurs within 30 minutes given that the RELAP5 case does not fail/crash (the RELAP5 model would fail if the valve flow area is near 0).

(10) Loss of Flow Control-Output

Cutsets assigned to this category are those that affect the output of the LOCS flow controller. They include the LOCS DPUs, and the digital output modules (DOMs). Like the case of the "loss of flow control-input" category, the PRA model does not specify the manner in which the component fails. Therefore, they were assumed to fail in a way that caused the most severe consequences, that is, both the DOM and DPU were assumed to erroneously instruct the flow control valve to close. Events in the category were modeled in RELAP5 by directly modifying control variable CV-24 that represents a flow-area ratio. This control variable is part of the mechanism by which the flow controller determines the flow area of the flow-control valve (FCV). A smaller output of CV-24 causes a smaller flow area resulting in a smaller flow rate. By setting CV-24 to a random number (per test scenario), the position of the flow-control valve no longer responds to the actual flow rate. The random number was selected from a range that ensures the trip setpoint, rather than a new steady state, could be reached. One cutset in the PRA includes the FCV spuriously closing. This cutset was also assigned to Category 10 since its effect is the closing of the FCV, which is the same as the other events in this category.

(11) Loss of Line Heater Control-Input

This category is similar to the "loss of flow control-input" category but involves the line-heater controller instead of the flow controller. Events in this category were modeled in RELAP5 by assigning a random number to CV-1, which represents the temperature difference between the fluid temperature and a reference temperature of 490°F, instead of using inputs from a temperature sensor. Assigning CV-1 a random number simulates the failure of the input portion of the line heater's controller. A sensitivity study showed that the power level of the line heater is increased by assigning a higher value to CV-1 that, in turn, causes an increase of the fluid's temperature and an increase in the reactivity. The lower bound of the random number was determined based on a sensitivity analysis so that the trip setpoint is reached within 30 minutes. The upper bound was chosen as the maximum allowable temperature difference of 490°F.

(12) Loss of Line Heater Control-Output

This category is similar to the “loss of flow control-output” category but involves the line-heater controller instead of the flow controller. Events in this category were modeled in RELAP5 by modifying CV-4 to represent the power level demanded for the line heater. The line heater directly reads the value of CV-4 and adjusts the heater’s power accordingly. As the value assigned to CV-4 increases, the power level of the line heater increases concurrently, resulting in higher reactivity. To simulate the output portion of the line-heater controller, CV-4 was directly modified by setting it to a random number selected from an interval based on sensitivity analysis. The lower bound (179,964 W) of the interval of the CV-4 output was selected because it caused a reactor scram at around 1700 s due to a temperature higher than 570°F at the outlet of the IPT. The upper bound of 216,000 W is the upper limit of CV-4 given in the RELAP5 model.

(13) Loss of TCV control

Two temperature-control mechanisms in LOCS are the mechanism for line heater power adjustment and the temperature-control valve (TCV). The latter controls the ratio of flow that bypasses the heat exchanger. Events in this category are those that lead to loss of temperature control. Examples include the TCV spuriously closing and the loss of DPU. These cutsets were simulated by completely closing the TCV in various periods of time before full closure. The time to closure was a random number sampled from a range determined using engineering judgment.

Several assumptions were used to determine the ranges of the uniform distributions described above. They are summarized below:

1. LOCS has a 0.3 s maximum cycle time. Thus, the LOCS protection system cannot mitigate any accident scenario that needs a trip to occur faster than 0.3 s. Based on this, the range for some of the parameters was determined so that all test scenarios generated do not require a trip before 0.3 s. For example, the upper limit for the size of the pipe break at the IPT outlet was determined to be approximately 0.4” diameter (i.e., break area of 9.43×10^{-4} ft^2 in Table 5-1) such that a trip signal is expected in 0.3 seconds.

2. After the occurrence of an event, it was assumed that the operator would initiate mitigation actions to terminate the reactivity insertion in no later than 30 minutes. This assumption limits the duration of RELAP5 simulation, and thus, the range for some of the parameters. 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 after the break.

In addition, some of the bounds were based on physical considerations. For example, for the size of a plugged flow-area, a natural upper limit is the full flow area, and the worst pump seizure occurs when the pump instantaneously comes to a full stop.

Table 5-1 lists the ranges of the uniform distributions for all failure effect categories as determined from sensitivity calculations using RELAP5. These calculations determined the appropriate parameter limits based on the above assumptions. Table 5-2 briefly describes how each of the limits was estimated. The uniform distributions were then sampled to define the test scenarios to be simulated. For example, for the loss of heat-exchanger cooling cutset (failure effect category 1 of Table 5-1), its RELAP5 simulation was generated by decreasing the heat-transfer coefficient from the steady state value to zero over a period between 0 and 1670 s. When generating a scenario to be simulated using RELAP5, a random number between 0 and 1670 was sampled. This number represented the period over which the heat-transfer coefficient would drop to zero.

As Table 5-2 shows, the upper limit of 1670 s was obtained from 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 this to drop to zero, then a trip signal will not be generated within 30 minutes.

5.3 Assumptions and Limitations of the RELAP5 Simulation

The purpose of the RELAP5 simulation is to realistically simulate the conditions of the reactivity-insertion accident under which LOCS operates. Such accident scenarios were identified by the PRA and further characterized by the probabilistic failure process models that capture their potential variability. RELAP5 runs that simulated the accident scenarios were used to generate the inputs for testing the LOCS. This section summarizes assumptions used in the RELAP5 simulation.

1. RELAP5 Model Enhancement

The INL RELAP5 model was originally used to simulate large loss-of-coolant accidents (LLOCAs). While the failure events identified in the PRA and used to demonstrate the statistical testing approach may progress more slowly than the LLOCAs, some may involve failure of specific components on the secondary side. BNL enhanced this model for the purposes of this study. For example, the secondary side that provides cooling to the loop was modeled by the heat exchanger's heat-transfer coefficient with a constant secondary-side temperature. BNL approximated the secondary-components' failures by varying (reducing) the heat transfer coefficient. In some other cases, BNL had to modify the RELAP5 model with assumed parameters such that some specific failures could be better modeled. For example, BNL added a steam volume to the pressurizer model and added a valve to simulate an SLOCA at a specific location. BNL also added a few such control functions to the RELAP5 model. Including these control functions improve the ability to more realistically characterize the operational context. However, some of these control functions were modeled in a simplified manner. These simplifications can introduce inaccuracy in simulating accident scenarios.

Some of the LOCS's protection functions were included in the original RELAP5 model. 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, the INL RELAP5 model was developed to support specific safety analysis reviews. BNL revised this model to meet the needs of the statistical testing approach. Such modifications include addition of control functions, adjustment of the assumptions of boundary conditions, and disabling of the protective functions. These changes relaxed some of the bounding assumptions used in the deterministic safety analysis and provided a more realistic PRA context for characterizing the digital system operational profile.

2. Modeling of variability in the plant's initial condition

In general, the reactor may operate under different conditions, for example, at a level lower than 100% power. Then, Loop 2A may operate in different conditions in terms of its thermal hydraulic condition, and the LOCS can be challenged in these instances. In this study, the initial condition of Loop 2A was defined in the RELAP5 model. That is, the reactor is assumed to be operating at 100% power and no variability in the condition was considered. This is also the assumption often made in a PRA.

3. Modeling of PRA failure events

The failure events modeled in a PRA are often at a high level of abstraction and thus lack the details needed for RELAP5 simulation. For example, a pump failure event may not specify if it is a pump trip or a pump seizure. Therefore, BNL developed thirteen probabilistic failure process models to detail the effects of failure in the RELAP5 model. Each cutset was assigned to one or more of the 13 categories. The assessment of the probability distributions involved engineering considerations (e.g., deciding the upper and lower bounds of a distribution) and assumptions on the type of distributions (e.g., the choice of uniform distribution). In some cases, the bounds of the distributions were selected without strong bases. Engineering analyses of the failure modes, if available, can offer a better basis for choosing 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 thermal hydraulic condition of the loop, such as the case of a loss of a bus that supplies power to some components of the LOCS. Therefore, the effects of these failures are approximated by one or more of the 13 failure effect categories.

The development of probabilistic failure process models to capture the variability in the thermal hydraulic effects of PRA-postulated failures is an innovative approach that is needed in STM. In general, the probabilistic failure process models could be enhanced by operational data, testing data, and engineering analyses should they become available.

4. Assigning equal probability to subcategories of failure effects

As described in Section 2.3, reactivity insertion cutsets were sampled based on their frequencies. 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, these subcategories are assumed to be equally likely. For most of these categories (e.g., pipe plugging and pipe break), the assumption of equal likelihood may be reasonable because they represent failure occurring at different locations that the PRA model does not specify. However, for pump failures, the two subcategories, pump trip and pump seizure, do not have the same likelihood; the former is expected to happen much more often than the latter. This is an area where improvement can be made by mapping individual cutsets directly to the subcategories provided that the cutsets differentiate between the different failure modes.

6 GENERATING TEST SCENARIOS

6.1 Grouping of Cutsets for Generating Test Scenarios

The probabilistic risk assessment (PRA) model described in Chapter 4 was used to generate cutsets from the fault tree modeling of the Loop 2A reactivity accidents. Each cutset consists of one or more component-failure events and leads to a reactivity insertion accident. The cutsets were sampled based on their frequency. Each sample defines a test scenario to be simulated with the RELAP5 model.

This study demonstrates how to use the RELAP5 model to simulate reactivity insertion events (RIEs). For demonstration purposes, RIE cutsets were grouped by failure effects using the failure effect categories described in Chapter 5. Section 6.1.1 details the general paradigm used for grouping cutsets, and briefly describes the types of effects that each failure-effect category represents. Section 6.1.2 discusses a semi-automated method of classifying a cutset into one or more categories of failure effects. Finally, Section 6.1.3 describes how the probabilistic failure process models (PFPMs) associated with the failure-effect categories were used to capture the variability in these effects within the individual categories, and then used to generate test scenarios that would be simulated with RELAP5. Appendix A shows the top 200 cutsets that were employed in this study to generate test scenarios and their associated failure-effect categories.

6.1.1 Cutset Grouping by Failure Effects

Solving the PRA model yields a list of cutsets representing events that result in reactivity insertion. Each cutset consists of either single- or multiple-failure events. These events define the execution environment of the Loop Operating Control System (LOCS) and also the RELAP5 model's simulation boundary under RIE situations. Ideally, the RELAP5 model can simulate all failure events. If this cannot be accomplished, as was the case in this study, the effects of some failures were approximated.

For instance, the original RELAP5 Loop 2A model does not include the secondary loop. However, in this study, some RIE cutsets include failures of the components of the secondary loop, so modeling them becomes necessary. Some of such components' failures may lead to a reduction in secondary loop's flow rate or an increase in the secondary side temperature, both result in a reduction of cooling to the primary (i.e., Loop 2A) side and an increase in reactivity. Therefore, the secondary-side failures can be modeled in RELAP5 by reducing the heat transfer at the heat exchanger. There are other failure events that may lead to the degradation of the heat exchanger's performance, but these events can be modeled in the same manner.

From the example described above, it is reasonable to group cutsets with similar failure effects into one failure effect category and model them in the same way in RELAP5. This approach confers the ability to group all cutsets obtained from the PRA analysis into a limited number of failure effect categories and reduce the effort of RELAP5 modeling. Table 6-1 shows 13 categories of failure effects. A majority of the cutsets belong to the RFW130 category that represents failures affecting the secondary-side of the heat exchanger. It is modeled as a reduction of the rate of heat removal from the primary loop. In the RELAP5 model, the secondary loop is modeled as a boundary condition with a fixed temperature. Therefore, a reduced flow rate of the coolant in the secondary side cannot be modeled directly. However, there are multiple ways to approximate this event, such as by increasing the boundary temperature, lowering the heat-transfer coefficient of the heat exchanger, or decreasing the heat-transfer area. Some of these approximate methods have side effects. For instance, increasing the boundary temperature can

engender scenarios wherein heat is transferred from the secondary-side to the primary side, resulting in unrealistic system behavior. This study approximated the flow reduction scenario by lowering the heat-transfer coefficient. The last column of Table 6-1 describes how the failure-effect categories were simulated. Tables 5-1 and 5-2 provide more information about the probabilistic failure models associated with these failure-effect categories. Their use facilitates capturing the variability in the failure effects in testing.

Another example of the use of the grouping concept lies in modeling the pressurizer. The original RELAP5 model does not contain the pressurizer heaters and sprays, which are the major means of controlling 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 the pressurizer heater were assigned to the gPipe failure-effect category and simulated the same way as was the small-break loss of coolant accident (SBLOCA) cutset even though the two scenarios clearly differ.

Table 6-1 also shows that some categories are divided further into subcategories. The gPump category represents all cutsets that ultimately cause the pump to fail. However, there are multiple ways (failure modes) in which a pump can fail, and the different ways may lead to different reactivity transients. For example, it may trip, resulting in a flow rate that follows the pump's coastdown curve. A pump may seize, resulting in a more abrupt reduction in flow. The original PRA analysis does not differentiate between these two failure modes (i.e., a cutset may only show that a pump failure occurs but not the failure mode). In this study, however, it is important to model these two failure modes as they lead to different inputs to the LOCS. Other examples of subcategories are gFlow (flow blockage category; subcategories are block locations) and gPipe (pipe break category; subcategories are break locations).

It is noted that some cutsets have a wider impact on the system and may belong to multiple categories. One example is a loss-of-power event that leads to loss of the 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 event was assigned to both the gFCtrlO and gTctrlHO categories. Table 6-2 shows some examples of cutsets assignments to different categories. A complete list is given in Appendix A.

Table 6-1 Failure effect categories and their modeling in RELAP5

#	Category	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 loop's temperature rise.	Decrease the heat transfer coefficient at the heat exchanger to zero over a given (but variable) period of time.
2	gPump	Primary pump failure – Trip	Forced circulation in loop 2A stops.	Shift (in time) the coastdown curve by a (variable) multiplicative constant.
3		Primary pump failure – Seizure	Forced circulation in loop 2A stops.	Linearly reduce pump speed to zero over a (variable) period of time.
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 given (but 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 given (but 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 given (but variable) amount.
7	gPipe	Pipe break – IPT Inlet	Volume and flow rate of loop 2A coolant decrease.	Introduce a pipe break of a given (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 AIM)	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 AIM)	Failure to increase loop flow- rate in response to transients resulting in flowrate reduction	Reduce flow rate by adjusting output from the flow controller by a given (but variable) amount.
11	gTctrlHI	Temperature control components (line heater) failure (sensor and AIM)	Failure to decrease coolant's temperature via reduction in line heater's output in response to temperature-increase transients.	Increase coolant temperature by increasing line heater's output by adjusting input to the controller (CV-1) by a given (but variable) amount.
12	gTctrlHO	Temperature control components (line heater) failure (DPU and AIM)	Failure to decrease coolant's temperature via line heater output reduction in response to transients resulting in temperature increase.	Increase coolant temperature by increasing line heater output by adjusting output from the controller (CV-4) by a given (but variable) amount.
13	gTctrlV	Temperature control components (TCV-3-1) failure	Failure 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 given (but variable) period.

Table 6-2 Assignment of example cutsets to failure effect categories

#	Probability	Basic Event ID	Basic Event Description	Category ID
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 Grouping into Failure-Effect Categories

Manually grouping all the cutsets would be very time consuming. Therefore, a Python [Rossum] script was developed to semi-automate the process that was possible due to two properties of the PRA model. First, although 200 cutsets were considered, these cutsets were comprised of various combinations of only 44 unique 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 a pump are all under the same subtree. These subtrees are transfer gates in the reactivity insertion tree. Another example involves failure of the secondary system's components that appear under a transfer gate, viz., "insufficient cooling flow from RFW header" (RFW130). Those basic events that cannot be categorized in these ways were manually assigned to the categories in Table 6-1 according to the impact of their failure. The script contains a database linking these basic events to the categories. A detailed algorithm is described below. It 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 categories of failure effects, all the cutsets for a subtree belong to the same category.

The high-level algorithm used in the script is shown in Figure 6-1 with more details described in the next paragraph. The script first reads the output file from the SAPHIRE model containing a list of cutsets for reactivity insertion. Each cutset has the basic event identifier, the basic event's description, and either its occurrence frequency or its probability. Next, the script populates the *component_list*, which is a list variable, with either subtrees or intermediate gates in a fault tree that determine the failure behavior. These subtrees and gates, which will be referred to as *components* herein, model the loop's primary pumps, the pressurizer heater's power source, the

secondary cooling system, and the remote processing unit (RPU) and its power sources. Each component is considered to belong to one or more category based on its failure effect. The final step in the script is to iterate through each cutset (repeating the first step) and assign that cutset to the appropriate categories.

1. Assign the list of cutsets read from SAPHIRE output file to *CS*.
2. Assign the list of component subtrees to the *component_list*
3. For each *component* in the *component_list*:
   a. Assign the list of cutset of the *component* to the array (indexed by component) *component_cs*[*component*]
   b. Assign the list of the group assigned to the *component* to the array (indexed by component) *group*[*component*]
4. For each *cutset* in *CS*:
   a. For each *component* in *component_list*:
      i. if *cutset* is a superset of *component_cs*[*component*]:
         (a) Assign *group*[*component*] to *cutset.group*

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

For those fault trees that contain subtrees, the subtrees (e.g., the DPU power supply, secondary system's components, and pressurizer heater's 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 the generation of a test scenario, the script could 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) were found in the list variable for "loss of pressurizer heater power supply" (the subtree), the script assigned this cutset to the appropriate failure effect category (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 the RFW header), and EXT-2AC-RPU (loop 2AC's RPU failure). The fault tree's basic events that are not part of any of the 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 failure effect categories. 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's bypass valve control, this failure event was manually classified into the gTctrlHI category. About 12 basic events were handled manually, and this rule was hard-coded in the script.

As discussed in Section 6.1.1, some cutsets were assigned to multiple failure-effect categories. For any cutset, the script checks each category in Table 6-1 to determine whether the current cutset is a superset of the category cutsets. If so, the cutset is assigned to that category. The assignment is not exclusive. The script maintains a variable for each cutset that represents a list of categories assigned to the cutset. This list may contain a single category or multiple ones. This

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

list of categories 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 Process Models in the RELAP5 Simulation of Test Scenarios

This section briefly discusses how probabilistic failure process models were used to capture the variability of the failure effect categories, how test scenarios were sampled, and how a Python script was used to automate the generation of the RELAP5 input. Section 6.2 provides a more detailed discussion.

The cutsets that were obtained from the PRA model represent combinations of failures events that can lead to a reactivity insertion. However, the cutsets may not specify exactly how, nor 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 coastdown rates. In Section 6.1.2, the cutsets are grouped into 13 failure effect categories based on high-level information about their effects, as shown in Table 6-1. Appendix A has a complete list of the top 200 cutsets that were used in this study and their assignments to failure-effect categories. These categories must be developed further to capture the variability within each of them. Chapter 5 gives detailed descriptions of the probabilistic failure process models of the categories of failure effects. Each such 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 position in which the valve closes. This random parameter is important because in the RELAP5 input file, the position of the valve as a function of time must be specified. It is assumed that a random parameter is distributed uniformly over a certain range such that in order to specify the state of a component, the parameter is drawn from a uniform distribution over the fixed range, as discussed in Section 5.2.2. The range itself was determined by either physical considerations or sensitivity analyses. A sample taken from the distribution would define a test scenario to be simulated using the RELAP5 model. It is noted that cutsets that belong to more than one category of failure effects will have multiple associated random parameters.

For a component with multiple failure modes (e.g., a pump may seize or trip), both the failure mode and its frequency of occurrence must be known. In most cases, these failure mode frequencies are either assumed or estimated from the literature. Section 6.2 discusses in more detail the failure mode's frequency.

To create the RELAP5 input file for a test scenario, a Python script was used to (1) sample a cutset from the cutset list based on its frequency, (2) determine the failure effect category or categories of the cutset, (3) sample the relevant parameter(s) (e.g., break size or valve closure rate) from its probabilistic failure process 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 Scenarios

6.2.1 Sampling of Cutsets

Section 4.3 described how the list of cutsets for reactivity insertion accidents was generated from the PRA analysis. Section 6.1 detailed how each cutset was assigned to one or more failure categories and to the associated probabilistic failure process models. Section 5.2.2 further established how the 13 failure effects categories 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 cutset 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 to as "samples" in the following discussion) were used for the simulation. These samples were generated by a Python script, with each sample selected according to its probability. The script used 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 of data structures that contains the category to which the particular cutset belongs. Some categories, such as pipe plugging, contain multiple subcategories (e.g., for the pipe-plugging category, the subcategories represent the blockage locations). In these cases, the script selected one subcategory randomly according to the subcategory probability. For this study and for demonstration purposes, all subcategories were assumed to have an equal probability, so that each one has an equal chance of being selected. The subcategory selected was then added to the list data structure.

Next, the script determined the parameters associated with each category. As shown in Table 5-1, each category or subcategory has an upper and a 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 category (category 1 in Table 5-1), the script picked a random number between 0 and 1670. This number represents the time at which the heat transfer coefficient reaches 0 for this sample. This time was used later by the script to generate the RELAP5 case (Section 6.2.2).

For all samplings (cutset list sampling, failure-effect-category 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 ensure the 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 automating the generation of the RELAP5 input file.
Automating the generation of the RELAP5 input file facilitated the conversion of the Monte Carlo samples (i.e., the accident scenario cutsets) into the corresponding RELAP5 input files/decks[20]. For each accident scenario (cutset), the RELAP5 deck was constructed by copying relevant sections from a RELAP5 template file and specifying changes from the steady state condition to

[20] The steady state input model was run until the initial transients disappeared (these transients appeared due to user-specified initial values to state variables which may not be self-consistent). Once steady state was reached, the system states were saved (along with other relevant information) in a steady-state restart file. All the transient calculations (based on the transient input decks generated as described in this section) used this restart file as the initial state.

simulate the scenario. For example, a pipe-break cutset was modeled by constructing an input file that contained the break's location and its size. This information was entered in the "transient" input deck that listed all the changes from the "steady state" input deck. The script automatically generates a transient deck for each of the 10,000 cutset samples by sampling the probabilistic failure process models of the failure effect category or categories associated with the cutset sample. Each sample contained information about 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 row represents one failed component.

Table 6-3 A portion of the sample file

Sample No.	Cutset No.	Category	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

*Note: NA = not applicable.

The algorithm of the script is shown in Figure 6-2. The high-level description of the script is as follows:

1. Read the sample information from the sample file into the *sample_list*. The sample file also contains the failure effect category (of categories) of the cutset. This is read into *sample.group,* which is a list variable containing all the failure-effect categories (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 categories of failure effects, the template file was constructed manually with notations to indicate which portion of the template file was to be used for which category. 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 6-3. The lines preceded by an asterisk denote a comment and are used to identify appropriate sections to copy to the transient input 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 6-2 Algorithm to generate RELAP5 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 6-3 Portion of the template file

After the RELAP5 input 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 a similar runtime. A Fortran program was used for each group to extract relevant information (e.g., the sensor's 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 milliamps) for each sensor (e.g., pressure, temperature, and mass flow rate). With four personal computers running in parallel, the cases were completed in a few days.

This output file contains the RELAP5 simulation results of the physical parameter at the sensors' locations. These numbers are calculated deterministically based on appropriate physical laws or correlations.

As described in Chapter 7, a test configuration that was developed by INL was used to execute the tests using the LOCS hardware and software with the RELAP5 output file as the input. BNL then evaluated the outputs of these tests to determine the success or failure of the protection system to generate a reactor trip (Chapter 8).

7 TEST CONFIGURATION AND EXECUTION

7.1 Introduction

This section describes (1) the establishment of the test configuration used to test the loop-operating control system (LOCS) and (2) the procedure followed in validating the test configuration and in executing the test scenarios. The work was conducted jointly by staff at Brookhaven National Laboratory (BNL) and Idaho National Laboratory (INL).

Figure 7-1 gives a high-level overview of the testing process. As described in Chapter 6, RELAP5 simulations of reactivity insertion scenarios derived from a probabilistic risk assessment (PRA) were used to generate input files for testing the LOCS. Each such file consists of time-stamped records with values of physical parameters. In addition, INL added a time-pulse analog-signal for estimating the cycle time of the LOCS[21]. The Testing Host Computer took the time-stamped records, converted the values of the physical parameters into analog signals, and fed them to the LOCS. It also received the output trip signals and an output heartbeat signal from LOCS as test results. The host computer then generated time-stamped records of these outputs, saving them in a file with the test results. These results were then evaluated to determine whether a trip signal was generated in time based on a predefined success criterion. The successes and failures of the tests were used to estimate the system's failure probability.

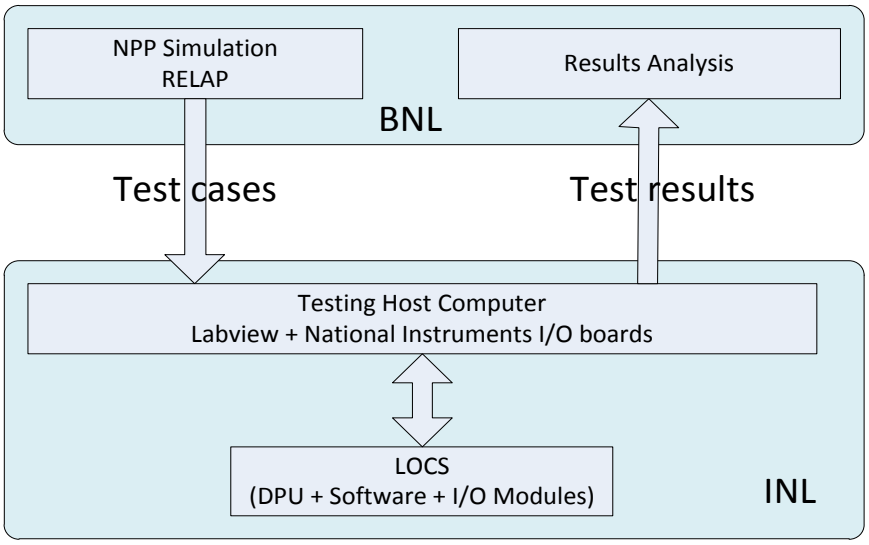


Figure 7-1 Work flow associated with performing the tests

[21] The time-pulse signal was added after an initial execution of the tests to estimate the cycle time of the LOCS, as will be detailed in Section 7.3 and Chapter 8.

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's Remote Processing Unit (RPU). Out of these 235 input signals only a few signals are considered safety-related, which are inputs to the LOCS protection functions. Therefore, only this small set of signals are required to be collected from the thermal hydraulic simulation and fed into LOCS test configuration to conduct this STM. During the test, the remaining loop-input channels were configured (i.e., placed in the simulation mode) to hold a software setpoint value that does not contribute to off-normal conditions nor do they produce non-safety alarms that require 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 thus were ignored by the Control Software Failure Test Signal Simulator (CSFT-INL-SS), that is, the host/test computer, throughout the test's entire execution.

Based on the preceding discussions, INL developed a computerized system for simulating signals that produce 14 analog current output signals representing the instrument signals in the normal real-world plant. An overall diagram of the CFST testing system and environment is provided in Figure 7-2 to provide a better understanding of the integration of the equipment. This Signal Simulator is connected to the Loop 2A DCS RPU development-and-test system, the primary purpose of which is to test the code and configurations before they are deployed 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 from runs of the RELAP5 model, each of which represents a test scenario. The values for each scenario are organized into a scenario file containing a set of time-stamped records that include information on the time steps along with the 14 signal values and the values of an added heartbeat signal. The hardware and software of the test configuration are described below.

Hardware

The test configuration, shown in Figure 7-2, enables testing 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 BNL RELAP5 model were collected in scenario files (with all 14 safety-related sensor inputs, the time-pulse signals, and the RELAP5 time steps) that were then used to drive the CSFT-SS signal simulator.

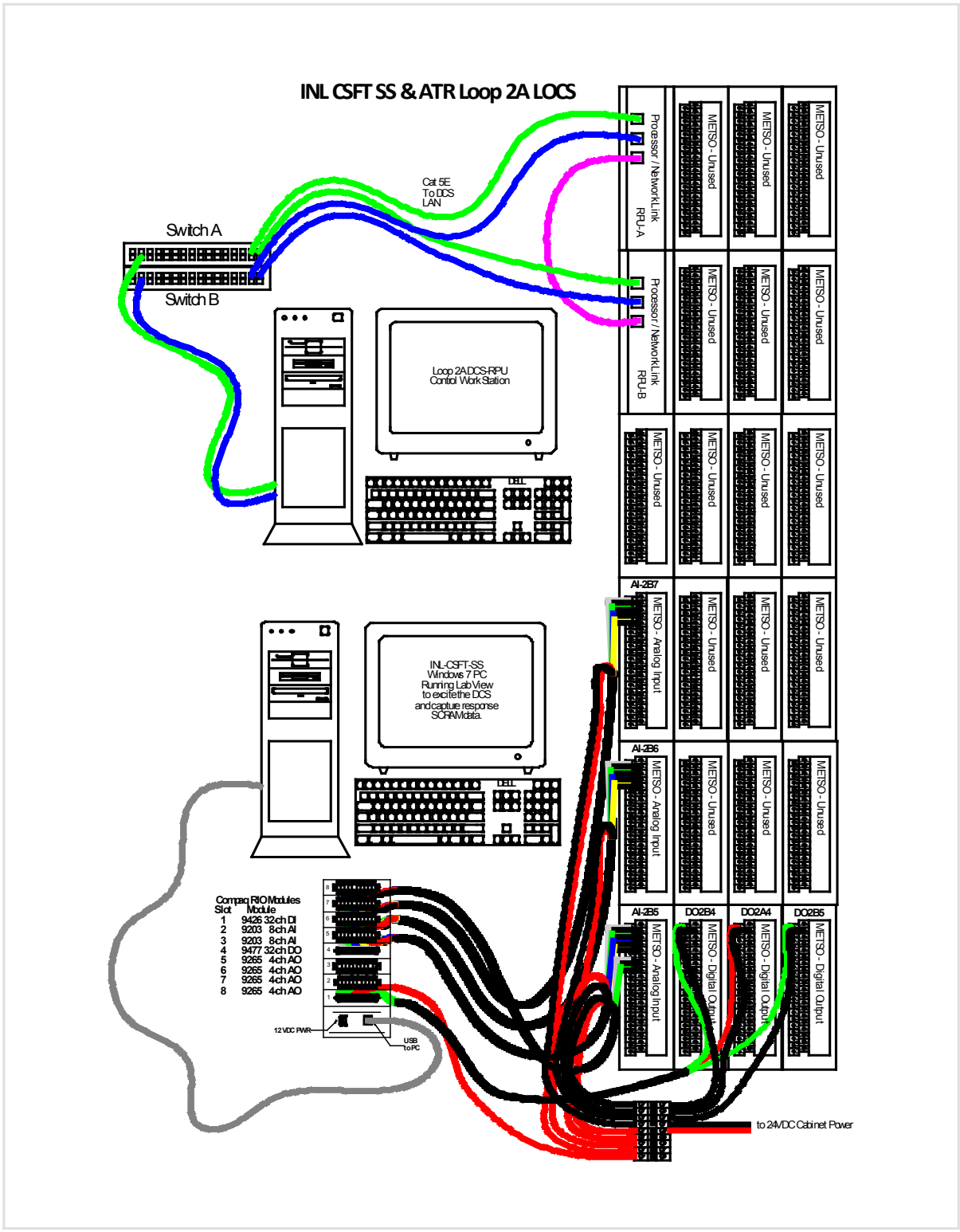


Figure 7-2 CSFT-SS testing environment

To provide the necessary real-time simulation function, this signal simulator uses National Instruments' (NI) Compact cDAQ rack and module hardware in conjunction with the LabVIEW

software development system [LabVIEW]. Simulator analog output channels were connected to proper DCS Loop 2A-input channels using copper-wire cables made for this application. Below is a list of items that comprise the testing system.

anufacturer	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 personal computer running Windows 7, w/ DVD writer

Software

A LabVIEW application program was developed that reproduces BNL's RELAP5-derived analog-signals on National Instrument (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 subsequently uses the in-record timing information to schedule and implement each record of the values for 14 channel outputs. Normally, a scenario file contains from 100 to 18,000 records. Sequentially, each record of 14 values, plus a time-pulse signal, is loaded into 15 output channel buffers and activated for the hold time period specified in the record (typically 0.1 s). Near the end of the hold time, the digital input channels for SCRAM A, B, and C, plus the output heartbeat signal, are sampled and recorded in the output array along with the time and the current input-record's number. This iterative process is repeated until the entire array has been run once; the output array is then written to a file using the same input name with "-out" appended to its name. The next scenario file then is read into memory and run until all files have been run once.

Figure 7-3 is a view of the CSFT-SS's 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's 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 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 scenario is a single file containing a series of these records. Two different versions of a scenario were produced, one containing 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 file type used as input to the CSFT-SS test. The engineering-unit file was used only if it was necessary to check the validity of a milliamp value.

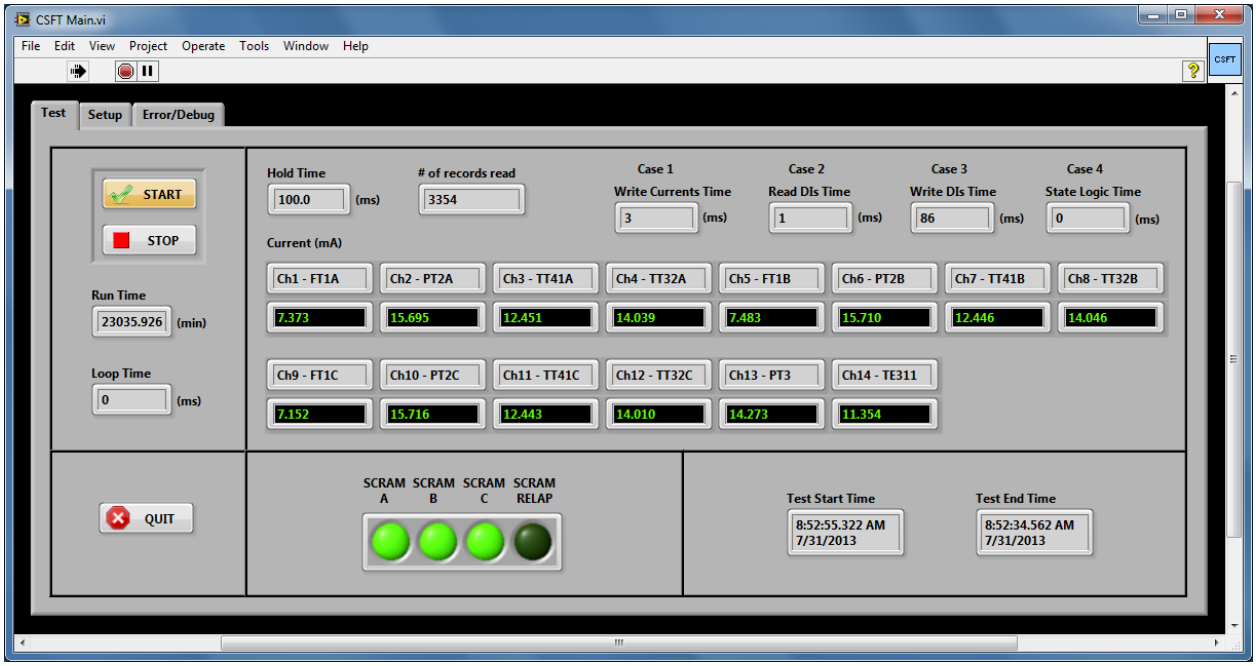


Figure 7-3 A view of the CSFT-SS's main window

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	Engineering Units	Range	DCS Trip Point
1	Time Step Interval	No output	Real	x.xx	Seconds	0-max	none
2	FT-1A	Mod5-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
3	PT-2A	Mod5-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
4	TT-41A	Mod5-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
5	TT-32A	Mod5-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
6	FT-1B	Mod6-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
7	PT-2B	Mod6-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
8	TT-41B	Mod6-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
9	TT-32B	Mod6-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
10	FT-1C	Mod7-Ch-0	Real	xx.xxx	milliamps	4 - 20	6.184 ↓
11	PT-2C	Mod7-Ch-1	Real	xx.xxx	milliamps	4 - 20	13.6 ↓
12	TT-41C	Mod7-Ch-2	Real	xx.xxx	milliamps	4 - 20	14.2 ↑
13	TT-32C	Mod7-Ch-3	Real	xx.xxx	milliamps	4 - 20	15.4 ↑
14	PT-3	Mod8-Ch-0	Real	xx.xxx	milliamps	4 - 20	No Trip
15	TE-31-1	Mod8-Ch-1	Real	xx.xxx	milliamps	4 - 20	No Trip
16	Time-pulse	Mod8Ch-2	Real	0.xxx	amps	0.04 – 0.020	No 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	Record number	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
6	DI-3	Heartbeat	Logical	x	0=true, 1=false	0 or 1

7.3 Execution of the Test Scenarios

Since testing required coordinating the work between BNL and INL, the process followed a phased approach. That is, some test scenarios 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's configuration by ensuring that the results were consistent with those expected. Due to difficulties in evaluating the test results, the production runs had to be repeated once, with an added heartbeat signal for estimating the cycle time of the LOCS.

Initial test runs

The RELAP5 model originally was developed to simulate two scenarios: a large LOCA and a heat-exchanger bypass. Accordingly, a few RELAP5 runs were performed to determine the required duration of the test scenarios and the time steps needed to properly simulate them. These test scenarios were sent to INL to aid their design of the Lab-VIEW software for 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 up to 0.3 seconds, and thus cannot recognize/capture the changes in very small time steps. Therefore, the RELAP5 model does not have to generate one output record every 0.01 second, which eases the constraint on cycle time for the CSFT-SS. In addition, we recognized that the input records to the CSFT-SS can be read into memory before a test is started, and that the output records of CSFT-SS can be saved in the memory before the test ends, such that the input and output operations do not affect the CSFT-SS's 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 up to 0.3 s, it was decided that a time step of 0.1 s was adequate. Depending on the reactivity scenario, the RELAPS5 model determines the time at which a physical parameter exceeds the threshold, generating a reactor-trip signal. It was decided that a RELAP5 simulation can be terminated 30 seconds after a threshold is exceeded for generating a trip signal. As described in Chapter 5, we disabled the built-in reactor trip logic of the RELAP5 model so that the RELAP5 simulation is still effective for producing post-trip reactor conditions that were later used for testing.

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 process model (PFPM) was developed for each category, so that samples taken from the PFPMs will represent a specific reactivity insertion scenario. There, one accident scenario simulation was forced to stop within 30 minutes based on an engineering judgment that if a reactor trip was initiated for 30 minutes, the operator would have recognized the problem and terminated the accident manually. The 30-minutes criterion was used to determine the upper or lower bound of the uniform distributions representing the 13 PFPMs. Before the production runs of the test scenarios, it was decided that 26 bounding cases corresponding to the upper and lower bounds of the 13 PFPMs should be tested to ensure that the production runs would be executed without any problems. These cases could also be used to develop success criteria for evaluating the results. Accordingly, BNL generated a set of 26 scoping scenarios, and sent them to INL to run the tests and acquire outputs from the CSFT-SS. The success of this scoping test allowed BNL to produce the final set of test scenarios for this project.

Production runs of 10,000 cases

BNL provided INL with 10,000 test scenarios that were organized into 4 groups of approximately 2,500 files each. As described in Chapter 5, these 4 groups were each generated by running the RELAP5 model on a personal computer. INL sequentially ran group 1 followed by groups 2, 3,

and 4. As each group was completed, the associated output files were zipped and transferred to BNL. Overall, the INL CSFT-SS system and environment were very efficient and effective for executing test scenarios that require accuracy in timelines and signal reproduction.

As summarized in Section 2.7, the production run of 10,000 cases was repeated once. The above description is applicable to both runs. In the initial run and the subsequent analysis, it was assumed that the LOCS has a fixed cycle-time of 0.3 seconds that resulted in anomalies that were difficult to explain. In the rerun of the cases, a few changes were made. For example, artificial noises intended to simulate the inaccuracy of the sensors were no longer added to the results of RELAP5 simulations. In addition, "heartbeat signals" were added to the input and output files so that the variability of the LOCS cycle time, which is between 0.1 and 0.3 seconds, could be estimated. Chapter 8 documents the results of the 10,000 rerun cases. Appendix B contains the details of the initial runs of each of the cases.

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 identified as relevant to the protection function under test. The remaining signals were deemed to have no effect on the LOCS protection functions; consequently, these signals were set to dummy values during the testing.

2. The input to the LOCS was 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 real sensor inputs that change constantly. This limitation also reflects the fact that the RELAP5 simulation only generates a new set of values every 0.1 seconds. 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 windows for protection functions. Each protective function has an associated hysteresis window that prevents a trip condition 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 °F (0.04 mA). Thus, if a TT-41 channel indicates a temperature above 510 °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 °F. Chapter 8 has more discussions on hysteresis reset windows.

   The hysteresis reset windows are set by the LOCS software and were used to determine when a trip should be reset. When evaluating the test outputs of the initial run of the test scenarios, the windows 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 accounting for 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 host computer cycle time, and the LOCS execution time, as discussed in Appendix B, a time window in which the trip should take place was determined and used to decide whether an actual trip signal was generated in sufficient time.

   This description of the hysteresis reset carefully was considered in the initial run of the 10,000 test scenarios assuming a LOCS cycle time of 0.3 seconds. In the final run of the

cases, this assumption is no longer used, making it impossible to know which preceding record was read by the LOCS. Therefore, the hysteresis reset was no longer considered (making the tests more black-box- than white-box-oriented). Instead, a total delay of 0.5 seconds was used as the criterion for determining if a test result is successful.

4. The LOCS and the host computer are not synchronized, that is, the LOCS has a cycle time between 0.1 and 0.3 seconds while that of the host computer is 0.1 second. Therefore the following timing considerations were used to determine the time-window in which an actual trip signal should be generated:

The LOCS will generate a trip signal whenever the 2-out-of-3 trip logic is satisfied for a given time step. This signal is expected to last up to 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.

8 EVALUATION OF TEST RESULTS

This chapter describes how the test results were analyzed using the inputs to the loop operating control system (LOCS) generated from the RELAP5 model; this assessment determines whether the LOCS successfully performs its protection functions against each test scenario. The results were evaluated by (1) estimating, based on input records, a time window in which a trip signal should be generated considering the cycle times of the LOCS and the test computer (See Section 8.1), and (2) determining, based on the output records, the actual time when a trip signals was generated (Section 8.2). Section 8.2 also compares the test outputs with the corresponding time-windows. Those cases in which the trip signal was not generated in the time window, that is, early and late trips, are called anomalies. Section 8.3 summarizes the findings and insights of the evaluation.

As summarized in Section 2.7, 10,000 test scenarios were run in an initial execution/run and a final execution/run of the data. The initial run is documented in Appendix B. Its results were evaluated assuming that the cycle time of the LOCS was constant at 0.3 seconds though the actual time could vary between 0.1 and 0.3 seconds. Because simulation records were generated every 0.1 seconds, by assuming a constant 0.3 second cycle time, it was presumed that the LOCS would read every third record (which is not really the case since the cycle time varies from one cycle to another). For each test, based on input records, we estimated a time window in which a trip signal should be generated and compared the actual time at which a trip signal was generated with the time window to decide if the test was a success or failure. Many anomalies were observed that are difficult to explain, including a suspected failure to trip that was not reproducible and was attributed to a test equipment issue. Appendix B also documents the investigation of the reproducibility of some anomalous test scenarios. Because the test computer and the LOCS are not synchronized, different input records may be read in different runs with the same test input file, leading to different outputs. Regardless, the different runs all were expected to result in success in the timely generation of the trip signal.

The experience from the initial run of the test scenarios led to modifications to the way in which the tests were performed and evaluated in the rerun, as listed below:

1. In the original tests, noise was added to the RELAP5-generated test inputs. The original intent of the artificial noise was to simulate noise in the sensor outputs. However, after discussions with staff at Idaho National Laboratory (INL) and the Nuclear Regulatory Commission (NRC), it was decided that the inaccuracy of the analog output modules of the test should adequately represent sensor's noise. (Note that these analog output modules are a part of the test system but are not a part of the actual LOCS system.) Therefore, the artificial noise that was originally superimposed onto the RELAP5 output of all the test scenarios was removed.

2. In the original analysis of the results, it was assumed that the cycle time of the LOCS was a constant 0.3 second interval; that is, if the LOCS reads an input record, then it was assumed that it will read the record that is 3 time-steps later, and continue reading all subsequent records that are 3 time-steps apart. However, the actual cycle time varies between 0.1 and 0,3 seconds. The 0.3 second cycle time was estimated based on testing conducted by INL and represented an upper bound of the actual cycle time. The analysis of delayed- and early-trip cases used in the initial run was very sensitive to the LOCS cycle time assumption. Additionally, a variable response time will have a large impact (a deviation of up to several seconds) on the predicted trip time. The assumption of a constant 0.3 second cycle time was no longer used to evaluate the rerun of the test scenarios.

To obtain more information about the cycle time of the LOCS, a heartbeat signal was added to each record of the input and output files. After reading an input record, the LOCS generated an additional digital output signal in accordance with the heartbeat-signal in the input (Table 7-2). The digital output signal was then recorded by the test computer. INL added an extra column to the mA input files (RELAP5 output) that has a value of either 4 mA (Low), or 20 mA (High). This heartbeat-pulse produces a 300 ms long pulse every 2 s (20 records) in one of the analog output channels. This signal is fed into an AIM of the LOCS. When the LOCS reads an input record, it will change the state of the response channel (i.e., the digital output corresponding to the heartbeat-pulse input) if the signal crosses a 12 mA threshold (i.e., goes from Low to High, or vice versa).

By comparing the delay between the record in an input file when the heartbeat level is “High” and the corresponding “High” record in the output, the LOCS’s cycle time can be estimated. Figure 8-1 plots an example of such a comparison. As shown in the figure, the output “High” lags the input by two records, meaning that the cycle time is two records (0.2 s) for the period shown in the figure. For other periods of the same test scenario or other test scenarios, situations in which LOCS can respond to an input within one record (0.1 s) were observed. In these cases, the “High” output occurs one record after the input “High”. Therefore, the LOCS’ cycle time can be as short as 0.1 s. Similarly, there were situations in which it took 0.3 second for LOCS to respond.

Regarding the timing requirement for generating a trip signal, INL indicated that 0.5 s is the appropriate window to use based on their experience using the LOCS. This means that a trip is considered to be delayed if LOCS fails to initiate a trip within 0.5 s of reading an input record exceeding the threshold.

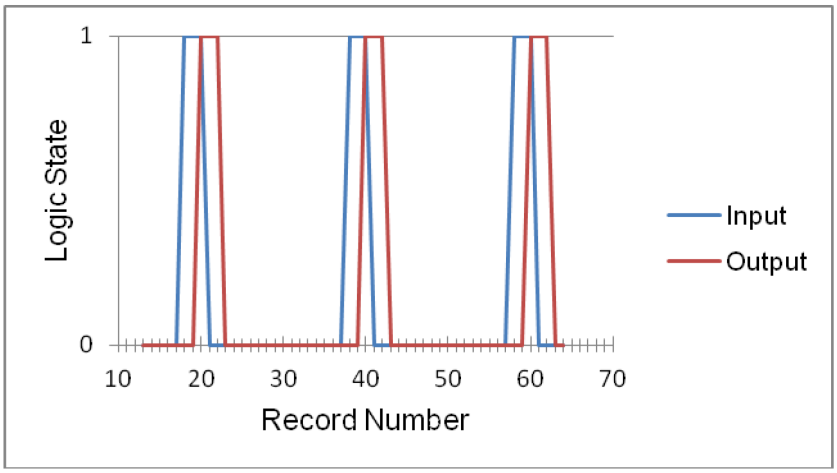


Figure 8-1 Comparison of the heartbeat pulse between the input and output to LOCS

3. The test configuration was calibrated by closely matching the mA value of each parameter that the LOCS reads to the mA value that the test computer sends as an output; the value obtained is accurate to within 0.003 mA. This calibration accounted for every component between the test computer and LOCS.

4. The input files used in the tests contain sensor readings in units of mA. However, the LOCS internally converts the mA values into engineering units before comparing them to the trip setpoint (also expressed in engineering units) to determine the trip action. This feature is an

important consideration since, for the flow rate, the conversion is not linear. Given a value for the flow sensor in mA, the conversion to engineering units depends on both the pressure and temperature. The script used to analyze the results was therefore rewritten to include this conversion such that the resulting parameters are in engineering units, enabling direct comparison with the thresholds.

5. The final modification to the input file is the addition of a record of 2 seconds at the end of the input file to reset the LOCS to a non-alarming state; this ensures that LOCS always starts a scenario in the same state.

8.1 Success Criterion

Based on the testing method described above, a means of evaluating the results to determine whether a test is a success or a failure (i.e., an early or delayed trip) was developed. Similar to the original analysis, for each case, a time window in which a trip signal is expected to occur was deterrmined. The expected trip-time window was determined as follows:

(1) The earliest time a LOCS can trip is the first record where 2 out of 3 sensors (any one of the monitored parameters) exceed the trip setpoint. A trip that occurs before this record is considered an “early trip”.

(2) The latest time that LOCS is expected to trip is 0.5 s after the LOCS detects the tripped condition.

Based on the analysis of LOCS cycle time described earlier, the LOCS samples the sensor values once within 0.3 s (3 records). Therefore, to ensure that the LOCS samples a record that is in a trip condition, that condition must exist for three consecutive records. That is, the LOCS is expected to generate a trip signal (as recorded by the output file) within 0.5 s (5 records) after at least three consecutive input-records show a trip state. For example, in the table below, it is expected that the trip should occur, at the latest, by time step (n + 2) + *5*.

Time Step	Input [2/3 in trip?]
n-1	No
n	Yes
n+1	Yes
n+2	Yes

Note that the lower bound of the expected trip-time window may be triggered by a single record exceeding the threshold if, by chance, it is read by the LOCS, while the upper bound requires 3 consecutive records. Therefore, the two bounds of the time window may be far enough apart, with the lower bound determined by one or two records exceeding the threshold and the upper bound determined later by 3 consecutive records exceeding the threshold.

8.2 ATR LOCS Testing Results

This section presents the results of the evaluation of the 10,000 test scenarios and the qualitative observations that were made about them. Of the 10,000 test cases simulated, 9,939 cases generated trip signals within the expected time window. Forty-five cases initially appeared to generate trip signals at a longer time delay than predicted by the time window and 16 cases

involved the generation of a trip signal before the time window. After a detailed evaluation, which is described below, all suspected delayed trips were determined to fall within the required trip window and only 4 cases of early trips (all attributed to inaccuracies in the I/O equipment) remained.

Table 8-1 shows 16 cases of an early trip. Here, the delay is defined as the number of records before the first occurrence of 2/3 sensor channels exceeding the trip threshold, which would trigger the LOCS to trip. Therefore, the entries with delays <0 means an early trip since, under ideal conditions, the LOCS should not trip before a trip condition is sensed.

Table 8-1 also shows the distribution of the 45 delayed trips for the 10,000 tests. Based on the criterion for the expected trip time, LOCS is expected to trip with a delay (relative to first occurrence of three consecutive trip records) of no longer than 7 records. (This criterion is derived from the requirement of three consecutive trip readings, plus a 0.5 s maximum delay as INL specified).

Table 8-2 shows the same delayed trip data categorized according to the physical parameters that initiated the trip. All delayed trips were triggered by the TT-32 outlet temperature channels. All early trips were initiated by the PT-2 (inlet pressure) channels. These data suggest that the early and delayed trips may be caused by some systematic property of these two channels.

To further investigate these anomalies, INL tested the test configuration in Figure 8-2 by comparing the mA values that the test computer generates (Point A) with the mA values that the LOCS reads (Point D). This comparison allows us to estimate the inaccuracies inherent in the test configuration and take them into consideration when evaluating the results. Ideally, the mA values at Points A and D should be the same. They are not exactly the same due to the inaccuracies of the test configuration (i.e., the AIMs of the test computer and the AIMs of the LOCS). In the test, the test computer was programmed to generate mA values representing each of the physical parameters that RELAP5 generates such that each value remains the same long enough for the LOCS to read and subsequently output these values.

Table 8-1 Distribution of trip delays derived from re-test

Delay (x 0.1 s)	# Cases	Delay (x 0.1 s)	# Cases	Delay (x 0.1 s)	# Cases
-10	**2**	-3	**3**	4	1
-8	**2**	-1	**2**	7	4
-7	**1**	0	568	8	2
-6	**1**	1	1037	9	29
-5	**3**	2	7648	10	13
-4	**2**	3	681	12	1

Table 8-2 Distribution of trip delays according to the variable that initiated the trip

FT1		PT2		TT41		TT32	
Delay	Count	Delay	Count	Delay	Count	Delay	Count
0	340	-10	**2**	0	1	0	9
1	73	-8	**2**	1	851	1	11
		-7	**1**	2	7642	2	6
		-6	**1**	3	679	3	2
		-5	**3**	4	1	7	4
		-4	**2**			8	2
		-3	**3**			9	29
		-1	**2**			10	13
		0	218			12	1
		1	102				

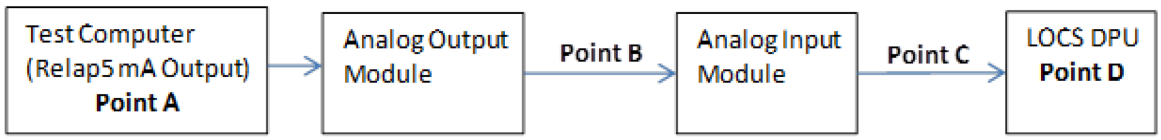


Figure 8-2 Sensor-signal pathway from the test computer to the LOCS DPU

INL researchers performed a linear regression analysis of the test results from the above tests. They found that, for each input parameter (designated as X) that the RELAP5 simulation produced, the values processed by the DPU (designated as *Y*) can be approximately represented by a linear fit of the input values. In the linear regression analysis, it was assumed that

$$Y = a * X + b$$

where the two parameters *a* and *b* are estimated using the data on *X* and *Y* collected in the test. The analysis found that the linear fit is very good for all input parameters (i.e., R squared is very close to 1).

The regression-analysis-adjusted input data (at point D) as opposed to data sent by the test computer (at Point A) was then used to determine the expected trip time window in the same way as described previously. The use of the linear regression was expected to correct the inaccuracies of the system in an average way. This approach was used to re-evaluate all 10,000 cases.

Table 8-3 shows the distribution of the delays after this adjustment was made. All the delayed-trip cases disappeared, and only four early-trip cases remained with a maximum of 2 time steps too early, which can be explained by inaccuracy of I/O modules (i.e., the corrections introduced by the regression analysis are correct only in an average way). This suggests that the system's inaccuracies caused by the AIMs of the test computer and the AIMs of the LOCS are responsible for early and delayed trips.

Based on the preceding analysis of the results of the reruns, the anomalies observed (i.e., 45 delayed trips and 16 early ones) were caused by the inaccuracy of the AIMs of the test computer, and the input modules of the LOCS due to faults in the hardware, and are not related to the software. The hardware inaccuracy is within the error range specified in the channels datasheet [INL 2010], however, it is still caused the early- and delayed-trips. The test results in Chapter 10 were used to estimate a software-failure probability, and a system (hardware and software) failure probability.

Table 8-3 Distribution of trip delays after correction with linear regression

Delay (x 0.1s)	# Cases
-2	1
-1	3
0	8773
1	1144
2	31
3	42
4	5
5	1

8.3 Summary of Findings and Insights of the Evaluation

- The findings and insights gained from the evaluations of the test scenarios are summarized here.

1. Due to the fact that (1) the LOCS and the test computer are not synchronized, and (2) the LOCS cycle time varies, it cannot be known whether the LOCS will read a specific input record. Based on INL's tests performed and the time pulses added to the input records, it was determined that the LOCS cycle time is between 0.1 and 0.3 seconds. This variability in the cycle time should be much smaller for a real safety-related software program at a nuclear power plant that does not use interrupts and performs dedicated functions only. When estimating the latest time at which a trip should occur, only the situations in which the threshold is exceeded for at least 3 consecutive input records were considered to ensure this condition would be read by the LOCS.

2. In general, the timing requirements of a protection system should be based on the physical conditions under which the system is expected to perform its protection functions. In the case of LOCS, the channel response times described in Appendix B can be considered the applicable timing requirements. BNL used the 0.5 second timing requirement that INL recommended. This is a more stringent requirement than the channel response times that are at least 0.78 seconds [INL 2010].

3. The results of the retesting initially identified 45 delayed trips and 16 early trips. Based on a regression analysis of the test data, it was determined that these testing anomalies were caused by inaccuracies in the analog output modules of the test computer and the AIMs of the LOCS. Therefore, they are considered hardware issues rather than DI&C failures.

4. During the execution of the test scenarios, INL experienced a few cases of power interruption. Use of uninterruptable power supplies would prevent such occurrences.

9 ESTIMATION OF SOFTWARE PROBABILITY OF FAILURE ON DEMAND

A Bayesian approach was used in this study to estimate the probability of DI&C failure on demand using the test results of zero failures 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 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 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, while 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 can also generate an upper bound of the DI&C failure probability, 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 a confidence γ. For example, if $\gamma = 0.95$, an analyst can be 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

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

that reduces to

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

Solving this equation for θ_u yields

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

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), and the test result of no failure in 10,000 tests, the posterior distribution for the failure on demand is *Beta* (1, 10001), with a mean failure probability of 1/10002~1 x 10^{-4} (Equation 9-4). The 5th and 95th percentiles of the *Beta* distribution are, respectively, 5 x 10^{-6} and 3 x 10^{-4}. Table 9-1 summarizes the results of the analysis.

Similarly, for 45 delayed trips[22] failures caused by hardware inaccuracy, the probability is given by *Beta*(46,9956) with its mean value equal to ~ 4.6 x 10^{-3} and the 5th and 95th percentiles equal to 4 x 10^{-3} and 6 x 10^{-3}, respectively. The probability of a delayed trip still is lower than the probability of LOCS hardware failure, 7.2 x 10^{-3} (Table 4-3). Similarly, considering the 16 early trips, the probability of an early trip is given by Beta(17, 9985) with a mean value of ~ 1.7 x 10-3 , and the 5th and 95th percentiles equal to 1 x 10-3and 2 x 10-3, respectively.

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

Table 9-1 Estimated failure probabilities

Failure Mode	Distribution	5th Percentile	Mean	95th Percentile
LOCS software	*Beta*(1, 10001)	5×10^{-6}	1×10^{-4}	3×10^{-4}
LOCS hardware (delayed trip)	*Beta*(46, 9956)	4×10^{-3}	4.6×10^{-3}	6×10^{-3}
LOCS hardware (early trip)	*Beta*(17, 9985)	1×10^{-3}	1.7×10^{-3}	2×10^{-3}

10 CONCLUSIONS AND INSIGHTS

Summary and Conclusions

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 on the actual LOCS, they also serve as tests of the hardware and the possible interactions among the LOCS components (including the hardware and software). The application used the reactor's probabilistic risk assessment model (PRA) to define the testing environment and the thermal-hydraulic model to realistically simulate the experimental loop conditions that are the inputs to the LOCS. A test configuration was established to execute test scenarios generated from the thermal-hydraulic simulation. Thirteen probabilistic failure process models (PFPMs) were developed to capture the variability of the failure effects, and to specify which scenarios will be simulated using the RELAP5 model. The test outputs from the LOCS were evaluated to determine if a trip signal was generated in time by considering the cycle times of the LOCS and the test's host computer. The result of no failure in 10,000 tests was used to estimate the probability of failure of the software on demand. Since the tests were done on the actual LOCS system, both its hardware and software were tested. The results can also be used to estimate system failure probability. In this study, some anomalies were identified, including 45 delayed trips and 16 early ones. The cause of these anomalies was identified as inaccuracies of the analog input/out modules as a result of the investigation described in Chapter 8.

In addition, the PRA was used to determine the importance of the LOCS in terms of the total core-damage frequency. The PRA results show that the reliability of the LOCS system, based on the results of statistical testing, is consistent with its stated reliability goal of 10^{-04} [INL 2008]. The PRA results also indicate that LOCS failure is a minor contributor to the core damage frequency, and a larger failure probability does not significantly affect the total core damage frequency. This in turn can lead to fewer test scenarios required to demonstrate LOCS reliability. The main reason for the low contribution is that the plant protection system always serves as a backup to the LOCS.

A number of issues arising from the use of simplified assumptions that could impact the realism of the study were resolved. The lessons learned with respect to these issues are described briefly below.

Insights and lessons learned

This study attempts to simulate the actual demand on the system and use the results to estimate the failure probability of the LOCS. It is very important that the simulation be realistic. However, there are practical limitations of 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 given in earlier sections. Note that the ATR PRA was modified for this study to define the scenarios used in testing.

1. *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 both control functions and protection functions, failures associated with the former may lead to reactivity insertion accidents that may be mitigated by the same system's protection functions. Two fault trees had to be modeled in the ATR's PRA: one modeling the reactivity insertion events caused by equipment failures of the experiment loop, including the LOCS, while the second fault tree models the LOCS's protection functions that would generate a reactor-trip signal in different scenarios. BNL changed the original ATR

PRA model to better account for this dependency and to ensure 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.

2. *PFPMs that capture the variability of failure effects of PRA-defined scenarios had to be developed.*

   The need to develop the 13 PFPMs arose because the PRA model only specifies the failure events at a high level that lacks the details needed in a RELAP5 simulation of the failure events. The RELAP5 simulation in this study uses the PFPMs to generate test scenarios and therefore considers the variability they represent. 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 can be varied.

   Some PFPMs used in this study are generic. For example, for a pump trip, randomness was introduced to simulate the variation in the trip's coastdown curve. In addition, some PFPMs were developed to use the simplified RELAP5 mode to simulate some failure effects. For example, due to lack of modeling of the secondary side of the experiment loop, a PFPM was developed to represent all those failure events associated with the secondary-side failures by varying the heat-transfer coefficient at the interface with the secondary side.

3. *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 control components, the effects of which have to be simulated using the RELAP5 model. It was decided that changing the RELAP5 model of the control functions to simulate the failure events was not possible due to lack of design information. 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 since pressure control is not modeled in the RELAP5 model.

4. *The RELAP5 model could be further enhanced to refine the results of statistical testing.*

   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 knowledge. In addition, a thermal-hydraulic model typically does not model redundant sensors. In this study, a single sensor value at a node was used to represent redundant sensors that should take on somewhat different values.

   A more general question centers on how far to go in thermal hydraulic modeling to make it more realistic. For example, the experiment loop has a secondary- and a tertiary-system that are further cooled by water from a lake or river that is atmospherically cooled. One might argue that they need to be explicitly modeled in a RELAP5 model, including the dynamic weather conditions, because they can all affect the condition the LOCS sees. It may not be necessary to consider the effects of the constantly-changing weather because the effects on LOCS are indirect and slow compared to the timing associated with reactivity accidents. A

basic requirement probably lies in being able to model the specific effects of what is modeled in the PRA.

5. *The test configuration is a simplification of real systems*

   The test configuration used in the study was intended to simulate the condition that the LOCS being tested experiences in the field. Two 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, nor the processing of, the protection functions.

   - The inputs to the LOCS were supplied by a host computer that periodically (with a cycle-time of 0.1 s) 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 not slower than the rate at which the LOCS is reading its inputs with a cycle time between 0.1 and 0.3 s. In turn, this cycle time determines the time step of 0.1 s used to generate the RELAP5 simulation results.

6. *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 this time window. It represents a realistic way of evaluating the test results. In this approach, the 5-second delay that may be introduced by the watchdog timer upon failure of the DPUs was not considered. Allowing the delay would extend the time window by approximately 5 seconds. This is a factor that was not recognized at the beginning of the study, and thus not accounted for therein.

7. *One suspected failed test was observed during the initial testing run.*

   As described in Appendix B, the testing group that included this suspected failure was performed in a slightly different manner than the other tests. Subsequent attempts to reproduce the failure by re-running the case 100 times were not successful (i.e., the LOCS digital system performed as designed during the retests). Additionally, follow-up testing during the second test run of 10,000 cases, which included more accurate equipment calibration and improved measurement of LOCS cycle times, did not result in an observed test failure. Based on the retesting results and consideration of potential causes of the suspected trip failure, it was determined that the suspected failure was caused from the test setup itself (rather than from a LOCS failure) and therefore did not represent an actual failure of the LOCS digital equipment.

8. *Reruns of test scenarios in general produced results that are similar to those of the original runs.*

   The 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 its own cycle time. Other possible explanations, such as instrument noises, were postulated. In general, the irreproducibility is related to software-hardware interaction and may need to be further explored

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.

[CSNI 2015] Nuclear Energy Agency, Committee on the Safety of Nuclear Installations, "Failure Modes Taxonomy for Reliability Assessment of Digital I&C Systems for PRA," NEA/CSNI/R(2014)16.

[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 200

APPENDIX A
TOP 200 CUTSETS OF RLHIE FAULT TREE

This appendix lists the 200 cutsets from which the test scenarios 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 (see 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 to generate the test scenarios.

#	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
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

#	Fraction	Group	Cut Set	Description
			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	AIM 1A2 (channel A - flow pressure temperature) fails to function
18	1.80E-03	gPipe	EXT-AIM-FF-002AC1A3-0000	AIM 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	Analog control module 1E3 fails to control temperature
21	1.80E-03	gRFW130	DCS-AIM-FF-001NE1A2-0000	High level AIM 1NE-1A2 fails to function/operate
22	1.80E-03	gFctrlO gPipe gTctrlHO gTctrlV	DCS-AOM-FF-02AC1A7-0000	AIM 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
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

#	Fraction	Group	Cut Set	Description
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
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

#	Fraction	Group	Cut Set	Description
			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
			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

#	Fraction	Group	Cut Set	Description
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
			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 auto-start)
			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
			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

#	Fraction	Group	Cut Set	Description
			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 AIM common cause event
88	1.46E-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-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

#	Fraction	Group	Cut Set	Description
			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
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

#	Fraction	Group	Cut Set	Description
			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
			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

#	Fraction	Group	Cut Set	Description
			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
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
			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

#	Fraction	Group	Cut Set	Description
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	AIM 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
			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	AIM 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

#	Fraction	Group	Cut Set	Description
			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 auto-start)
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
			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

#	Fraction	Group	Cut Set	Description
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
			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 auto-start)
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	AIM 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 auto-start)
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

#	Fraction	Group	Cut Set	Description
			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
			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 instrument 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
			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

#	Fraction	Group	Cut Set	Description
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 under-voltage 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
			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

#	Fraction	Group	Cut Set	Description
			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
			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

#	Fraction	Group	Cut Set	Description
			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
			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 auto-start)
			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

#	Fraction	Group	Cut Set	Description
			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)
			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
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

#	Fraction	Group	Cut Set	Description
				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)

A.1 Evaluation of Test Results of Initial Run

This appendix describes how the test results of the initial run of the 10,000 test scenarios were analyzed using the inputs to the loop operating control system (LOCS) generated from the RELAP5 model. It determines whether each test scenario 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 account the cycle times of the LOCS and the test computer as well as the hysteresis windows implemented in the LOCS software (See Section B.1.1); and (2) determining, based on the output records, the actual time when a trip signal is generated (Section B.1.2). The timing consideration explains some test results. For example, few test scenarios 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 at which the LOCS reads the input record, it may or may not read the record with the threshold exceeded. Section B.2 discusses the comparison of the test outputs with the corresponding time windows. Those test scenarios in which the trip signal was not generated in the time window are called anomalies. The anomalies observed include a suspected 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 scenarios were done to determine if the anomalies could be reproduced. An issue of reproducibility was identified and investigated, as discussed in Section B.3.

A.2 Determination of a Success Criterion

The input file of a test scenario consists of records containing the values of the sensors at different times. The results of a test are saved in a file containing the output of the LOCS digital output channels 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 was established. The criterion used to determine whether 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 s[23]) and the host computer with a cycle time of 0.1 s, and the hysteresis reset windows of the protection functions. Table B-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 °F (0.04 mA). This means that if a TT-41 channel indicates a temperature above 510 °F at one LOCS cycle, then that channel will remain in a trip state for subsequent LOCS cycles for 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 B-1 lists the trip setpoints and hysteresis windows for different trip functions. These windows were accounted for in predicting the time at which a trip signal is generated.

Table A-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	$\leq$ 25 gpm	1 gpm
PT-2A, PT-2B, PT-2C	IPT inlet pressure	$\leq$ 1800 psig	5 psig
TT-41A, TT-41B, TT41C	IPT inlet temperature	$\geq$ 510 °F	2 °F
TT-32A, TT-32B, TT-32C	IPT outlet temperature	$\geq$ 570 °F	2 °F

A.2.1 Estimating a Predicted Trip Time Window

Predicted trip window

The upper boundary of the predicted trip window is the latest time at which 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 B-1.

[23] INL approximated the LOCS cycle time to be 0.3 s based on the observation that when the 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.

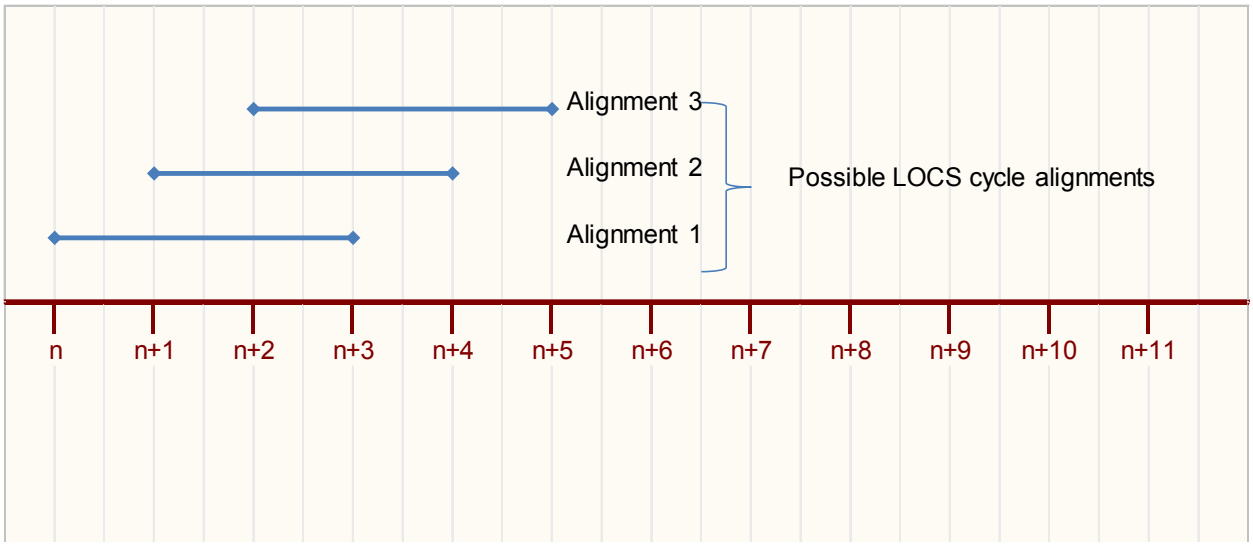


Figure A-1 Relationship between LOCS cycle and host computer cycle

In alignment 1, the LOCS cycle starts somewhere in the interval [*n*, *n+1*) of the host computer cycle. Assuming that the 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 $[\min_i A_i, 4 + \max_i A_i]$. 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*.

A.2.2 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.

A.3 ATR LOCS Testing Results

- In this section, the output files of the tests were evaluated based on the criterion described in Section B.1, and the anomalies are discussed.

- Figure B-2[24] shows the distribution of the difference between the actual trip record number and the predicted trip window (each record corresponds to 0.1 s). If 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

$$deviation = \begin{cases} r_{actual} - r_{min}, & r_{actual} < r_{min} \\ r_{max} - r_{actual}, & r_{actual} > r_{max} \\ 0, & r_{min} \leq r_{actual} \leq r_{max} \end{cases}.$$

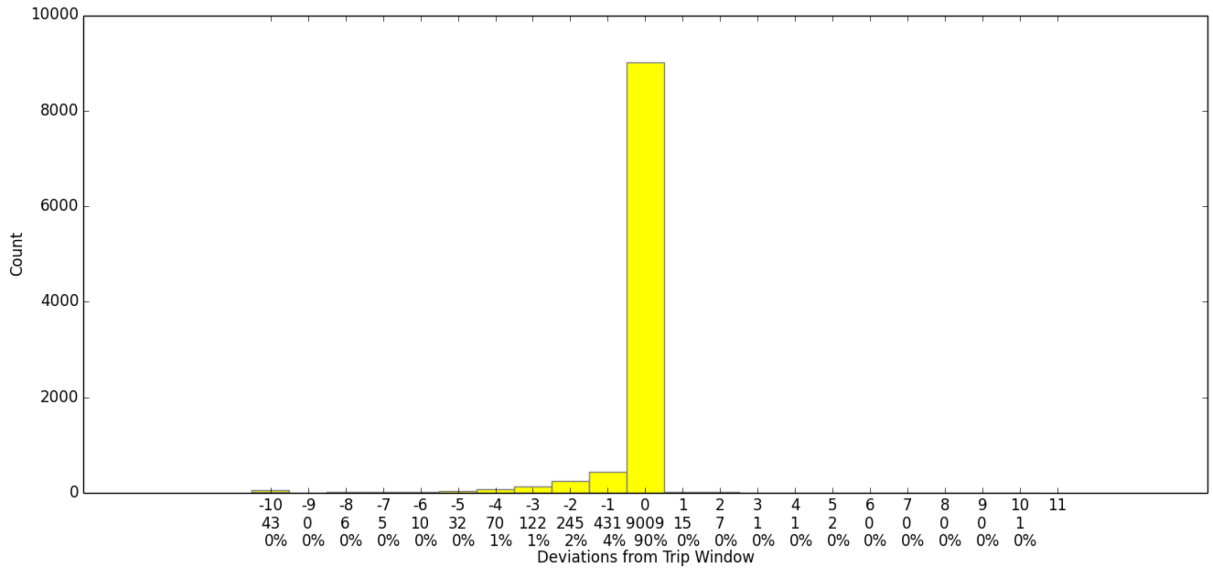


Figure A-2 Distribution of the deviation of the actual trip record from the predicted trip window

Figure B-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 B-2 and B-3 show the delayed and early trip counts breakdown in more detail.

[24] 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.

Table A-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 A-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 B-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's 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, this single trip failure is included in Table B-4 for completeness but for subsequent analyses, this case will not be considered as a failure.

Table A-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.

- From inspecting the early trip cases, it appears that all trips initiated by the TT-32 channels (IPT outlet temperature) are early trips. Although the nominal trip setpoint for TT-32 is 570 °F, the trip actually occurred around 569.5 °F based on examination of the output files. Therefore, scenarios in which there is large delay from the time the temperature first reached 569.5 °F to the time it exceeded 570 °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. Upon inspecting the input file for some of these cases, it was found that the mass flow rate dropped below the trip setpoint rapidly (in 0.1 s) and recovered the next record. To gain a 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 (simulating 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 a very small time step size of 0.001 s (original cases were run with $\Delta T = 0.01$ s) to ascertain whether the predictions are reasonable. The new results show the same behavior as the originals. This indicates that the sudden reduction of the flow rate is a result of the sudden change of flow condition and is physically reasonable flow behavior.

- It was also observed that there are 398 cases in which the three DCS outputs do not agree (i.e., 2-of-3 vote logic). However, they are not considered to be a failure and are included in the table for completeness.

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

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 B-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 a flow value slightly lower than 25 gpm did not register as a trip-level reading.

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 the assumption that the criterion is only applicable for cases in which the threshold is exceeded for at least one LOCS cycle (3 records) reveals that this case is not considered a delayed trip. (A low-flow trip condition did not last 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 B-2, the channel response time was not exceeded.

B. Early trip

- Case HI_217 (line heater control failure) is an example of a case in which the actual trip occurred before the predicted trip. Figure B-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 was within 0.1 °F of the setpoint. Although 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.

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

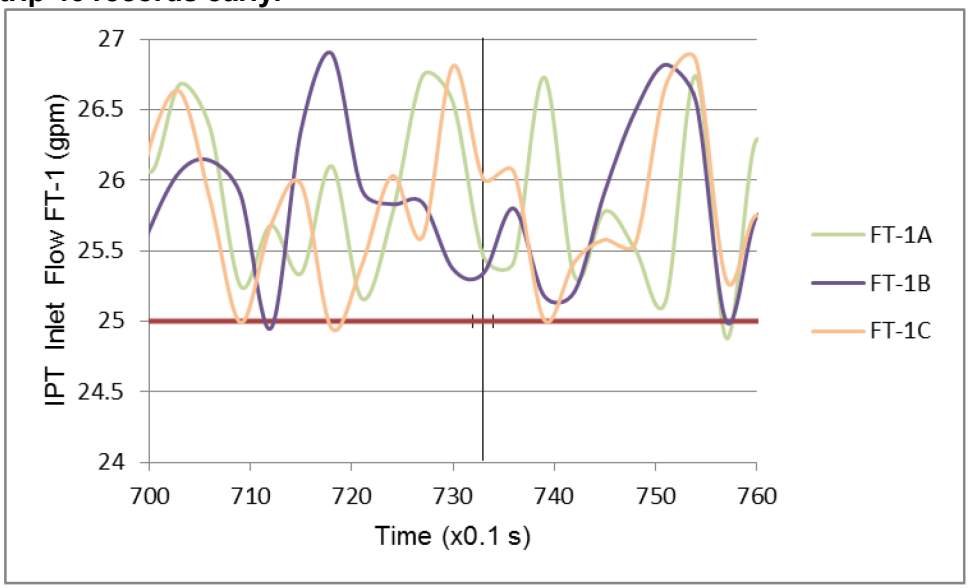


Figure A-3 LO_FO_HO_TV_2994 is an example of a delayed trip case

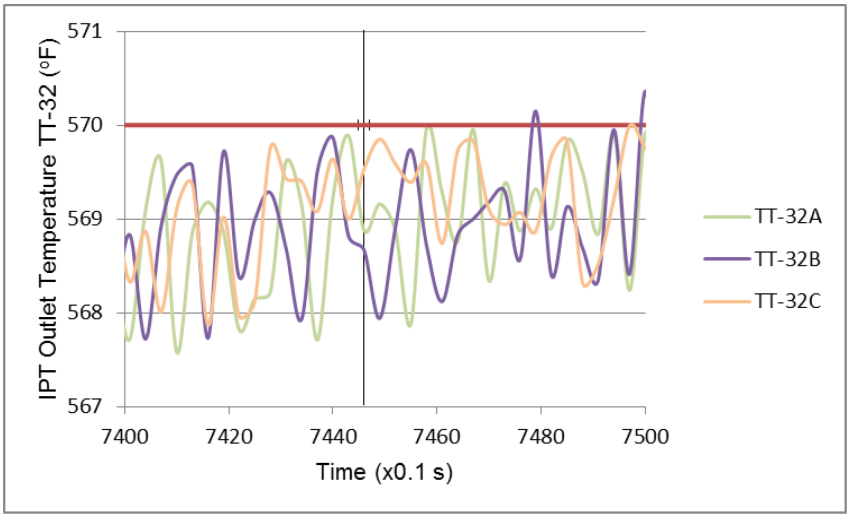


Figure A-4 HI_217 is an example of an early trip case

A.4 Reproducibility of the Test Scenarios

Due to observation of one failed test and many other anomalies, after discussion with INL, it was agreed that some of the test scenarios should 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 a 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 that the delay was caused by transient hardware failures. Therefore, all cases in this group were rerun using the same procedure that was used for other cases (i.e., without the trip channel written). The results discussed in Section B.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 B-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 B-5, there was no case where a trip failed to be generated in the rerun.

Table B-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 s). 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., the sensor values recover quickly) as in a case in which there are large oscillations in sensor readings, then only one alignment of the LOCS cycle may capture that trip. Electronic noise may also cause an early trip if the sensor readings are very close to, but do not yet reach, the trip setpoint. In these cases, although the predicted trip will occur later, noise may add a positive number (for temperature channels) to the sensor reading, which causes 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.[25]

[25] 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.

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

Case	Actual Trip Record	Number of Runs with Indicated Actual Trip Record	Expected Trip Window
LI_5472 (pipe break)	4	7	[2, 417]
	5	1	
	409	2	
LO_9360 (failure of AIM 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	

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-7234

2. TITLE AND SUBTITLE

Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability

3. DATE REPORT PUBLISHED

MONTH	YEAR
May	2017

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

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], Nancy Johnson[2], and Ming Li[3]

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

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

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington DC, 20555-0001

10. SUPPLEMENTARY NOTES

M. Li

11. ABSTRACT (200 words or less)

A statistical testing approach for quantifying on-demand failure probabilities for safety-related digital systems has been developed and applied to the loop-operating control system (LOCS) of an Advanced Test Reactor (ATR) experimental loop at Idaho National Laboratory (INL). This work is the result of a collaboration between Brookhaven National Laboratory (BNL), INL, and the Korea Atomic Energy Research Institute (KAERI).
The objectives of the study include:

1. development of a statistical testing approach for estimating digital system failure probability, the results of which are suitable for including in a probabilistic risk assessment (PRA); and
2. application of this approach to the LOCS, and insights into the feasibility, practicality, and usefulness of the estimation in models of digital systems for inclusion in nuclear power plants' PRAs.

The study used the ATR's PRA to define the testing environment, that is, the conditions under which the safety system would be called upon to initiate a safety function. Based on the PRA accident sequence information, a thermal-hydraulic model (RELAP5) was used to simulate the experimental loop conditions (e.g., pressure, temperature, and flow) during the selected accident sequences in order to provide realistic input signals to the LOCS test platform. To ensure that the test cases provided adequate coverage of operational conditions, thirteen probabilistic failure process models (PFPMs) were developed to represent the varieties associated with timing, component failure modes, and process variable control. An automated test platform was developed to supply input signals for each test case to the LOCS digital system and monitor when a trip signal was generated. The testing results were then used to quantify the on-demand failure probability of the digital LOCS system.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Digital Instrumentation and Controls, PRA, On demand failure probability

13. AVAILABILITY STATEMENT

unlimited

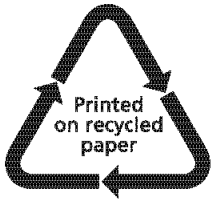
14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMSSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS

NUREG/CR-7234 Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability May 2017