SANDIA REPORT

SAND2017-10307
Unlimited Release
Printed September 2017

Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis (LDRD 17-0958) FY17 Report

Timothy Wheeler, Matthew Denman, R.A. Williams, Nevin Martin, Zachary Jankovsky

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2017-10307
Unlimited Release
Printed September 2017

Nuclear Power Plant Cyber Security Discrete Dynamic Event Tree Analysis (LDRD 17-0958) FY17 Report

Timothy Wheeler, Matthew Denman, Zachary Jankovsky
Risk & Reliability Analysis
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-MS0748

R.A. Williams
Resilient Control Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-MS0757

Nevin Martin
Statistical Sciences
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-MS0829

Abstract

Instrumentation and control of nuclear power is transforming from analog to modern digital assets. These control systems perform key safety and security functions. This transformation is occurring in new plant designs as well as in the existing fleet of plants as the operation of those plants is extended to 60 years. This transformation introduces new and unknown issues involving both digital asset induced safety issues and security issues. Traditional nuclear power risk assessment tools and cyber security assessment methods have not been modified or developed to address the unique nature of cyber failure modes and of cyber security threat vulnerabilities.

This Lab-Directed Research and Development project has developed a dynamic cyber-risk informed tool to facilitate the analysis of unique cyber failure modes and the time sequencing of cyber faults, both malicious and non-malicious, and impose those cyber exploits and cyber faults onto a nuclear power plant accident sequence simulator code to assess how cyber exploits and cyber faults could interact with a plants digital instrumentation and control (DI&C) system and defeat or circumvent a plants cyber security controls. This was achieved by coupling an existing Sandia National Laboratories nuclear accident dynamic simulator code with a cyber emulytics code to demonstrate real-time simulation of cyber exploits and their impact on automatic DI&C responses.

Studying such potential time-sequenced cyber-attacks and their risks (i.e., the associated impact and the associated degree of difficulty to achieve the attack vector) on accident management establishes a technical risk informed framework for developing effective cyber security controls for nuclear power.

Acknowledgments

The author wish to acknowledge the following:

- Seth Hanson (6613) for contributions to the development of the cyber exploit model,
- Bibiana Seng (66131) for contributions to the development and implementation of the sequence clustering and pruning model, and
- Jeffrey Cardoni (8832) for creation of the physical plant model.

Contents

Executive Summary ix
Nomenclature xv
1 Introduction 1
1.1 Structure of the Report 2
1.2 Conclusions 2
1.3 LDRD Publications 4
2 Background 7
2.1 Cyber Exploitation of D&IC Systems 7
2.2 RHR System 8
2.3 RHR ISLOCA 10
2.4 Plant and Operator Response 13
3 Emulated Cyber Intrusion of a Nuclear Plant Control System 15
3.1 Target Systems 15
3.2 Physical Plant Model 16
3.3 Cyber Exploit Modeling 18
3.3.1 Sceptre 18
3.3.2 hacker.exe 22
3.4 Integration of Cyber-Physical Models 23
4 ADAPT and General DET Advancements 27
4.1 Enhancements to ADAPT 27
4.1.1 Extension of the ADAPT Framework for Multiple Simulators 28
4.1.2 Conditional Tree Reduction in the ADAPT Framework 31
4.2 Advances in Dynamic Event Tree Methods 32
4.2.1 Pruning of Discrete Dynamic Event Trees using Density Peaks and Dynamic Time Warping 33
4.2.2 Measures of Importance in Dynamic Event Tree Analysis 36
References 39

Figures

1 Hypothetical Plant Layout with Residual Heat Removal Component Locations [22] 9
2 Layout of the Auxiliary Building Lower Level 11
3 Representative RHR System Layout 12
4 MELCOR Model Layout 17
5 Emulytics Environment 19
6 Live Adversary Exploit of Emulated System 20
7 Human Adversary Behavior 21
8 Automated hacker.exe Behavior 23
9 CDF for RHR Component Capacities 25
10 Data Flow Process for ADAPT with Multiple Generic Simulators (Sim 1 & Sim 2) 30
11 Clustering using ED. 34

12 Clustering using DTW. 35
13 An example of the optimal path through the pairwise distance matrix of two time series [54]. 36

Tables

1 Potential Attack Scenarios 22
2 Required Input & Sample Input for Rules 31
3 Parameter and Time Operator Values for Rules 32

Executive Summary

Introduction

Industrial control systems, including these in Nuclear Power Plants (NPPs), have historically relied upon supply chain integrity, physical isolation from outside networks, and physical access control for security. With the shift toward increased connectivity and Digital Instrumentation & Control (DI&C) systems, new vulnerabilities to cyber intrusion have been introduced [1]. Nuclear facilities have been compromised in the past both by an open network connection [2] and by software apparently brought in on removable storage media [3]. In the former case, plant operators lost access to a safety display system for hours. In the latter case, the settings on a specific hardware controller were altered.

In order to evaluate the effects of a cyber intrusion, a hypothetical plant model was created based on common Pressurized Water Reactor (PWR) design features [4]. To enable study of a cyber intrusion, the hypothetical plant was assumed to have been upgraded at least in part to digital Supervisory Control and Data Acquisition (SCADA) systems as has been proposed and implemented in multiple existing plants [5, 6]. In particular, the Residual Heat Removal (RHR) isolation system is assumed to have been upgraded [7]. RHR isolation offers an appropriate demonstration of an integrated cyber security risk methodology as it contains multiple active instruments and controlled components and may challenge plant safety if control is lost.

This Laboratory Directed Research and Development (LDRD) project developed a methodology to integrate the study of the progression of a cyber intrusion with modeling of its potential effects on the physical plant for a holistic cyber risk analysis. This methodology brings together emulation of physical control components and network devices as well as industry-standard nuclear power plant safety computer codes under the Analysis of Dynamic Accident Progression Trees (ADAPT) Dynamic Event Tree (DET) scheduling software [8] to generate a coupled dynamic analysis. The cyber intrusion was evaluated with two tools. The first tool used to evaluate the cyber intrusion was the Sandia National Laboratories (SNL) Emulytics[1] methodology with which a network of virtual computers was assembled to represent the architecture of the hypothetical RHR isolation system with high fidelity. A human representative of an adversary was tasked with gaining access to the virtual computer network and altering key control parameters relating to the RHR isolation system.

[1] SNL designation for emulative network computing and analytics

Key Technical Accomplishments

The technical accomplishments of this LDRD are summarized below:

- Developed an integrated analysis of the progression of and consequences of a cyber exploit of a complex system (Section 3.3).
- Developed the first known unified computer model of a cyber intrusion and its effects on the control system of a nuclear power plant (Section 3.4).
- Unlocked DET analysis for any arbitrary combination of simulator codes under ADAPT (Section 4.1).
- Implemented a new clustering algorithm for grouping together similar branches in a DET. This algorithm was modified to be more computationally efficient and it was automated so that it could run alongside a growing DET without user input (Section 4.2).
- Developed a method for pruning a user-defined percentage of branches based on clustering results (Section 4.2).
- Employed a method for analyzing the effect of pruning by comparing the probability distributions of DET end states before and after pruning (Section 4.2).
- Developed a flexible and adaptable form of importance measures for DET analyses (Section 4.2).

Potential Mission-Relevant Impacts

This LDRD contributes to the Energy and Climate Investment Area (IA) by enhancing nuclear power safety advanced accident modeling. The advancements developed here for DET are applicable for both life-extension of existing fleet and for analyzing and evaluating the safety case for "inherently safe" advanced reactors. This capability has a high technology readiness level now. This LDRD also contributes to the Global Security IA by establishing techniques for efficient and partially automated characterization of physical impacts and mitigation of threats on production networks and systems. Additional maturation of this capability over the near term (i.e., FY18) would be required to bring this capability to a high technology readiness level.

Next Steps

The advancement relating to the use of multiple arbitrary simulators in a DET is already in use within SNL. In one LDRD (System Theoretic Framework for Mitigating Risk Complexity in the Nuclear Fuel Cycle, LDRD 17-0969), a set of computer codes relating to the safety, security, and safeguards of spent nuclear fuel are being coupled under ADAPT to generate a single DET from which a comprehensive transportation risk metric may be developed [9]. In another analysis funded by the Department of Energy (DOE) Boiling Water Reactor (BWR) severe accident management guidelines are being evaluated using ADAPT and leveraging the code improvements that have resulted from this LDRD for performance and reliability of ADAPT.

Department 8851 will target integrated Emulytics System Simulator capabilities in its FY 18 Program Development outreach to such organizations as DOE, Department of Homeland Security (DHS), the United States Nuclear Regulatory Commission (NRC), and Electric Power Research Institute (EPRI).

Summary of Lessons Learned

The key lessons learned from this LDRD are summarized here:

- Cyber emulytics requires continued advancement to supplement and expand nuclear power plant network emulation capability.
- To properly take advantage of DET branching, any computer model simulating or emulating a control system or network must be of a size, scale, and design conducive to copying and parallel execution.
- Expanding ADAPT to the SNL supercomputers would allow for analysis on a wider array of multidisciplinary analyses than can be conducted on local clusters.
- ADAPT has been developed on a project-by-project basis with only results-focused documentation in journals and reports. ADAPT user manuals and training materials are need to ensure the continued usability of this tool.

Project Publications

Refereed Journal Publications (in preparation or review)

- N. Martin, et al., "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," In preparation for *Reliability Engineering and System Safety*, 2017.
- Z. Jankovsky, et. al., "Dynamic Event Tree Analysis with the SAS4A Safety Analysis Code," Submitted to *Annals of Nuclear Energy*, 2017.
- Z. Jankovsky, et. al., "Safety Analysis using Coupled Simulator Code in the ADAPT Dynamic Event Tree Framework," In preparation for *Annals of Nuclear Energy*, 2017.
- Z. Jankovsky, et. al., "Comparison of Measures of Importance in Dynamic Event Tree Analysis," In preparation for *Annals of Nuclear Energy*, 2017.
- R. Williams, et. al., "Emulated Cyber Intrusion of a Nuclear Power Plant Control System: Unified Computer Model," In preparation for *Computers and Security*, 2018.
- R. Williams, et. al., "Computer Modeling of Successful Cyber Intrusion in a Nuclear Power Plant," In preparation for *Journal of Sensitive Cyber Research and Computer Engineering*, 2018.

Conference Papers and Presentations, Internal Intern Presentations

- N. Martin, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- N. Martin, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," Invited Speaker, University of New Mexico Math and Statistics, Albuquerque, NM, 2016.
- B. Seng, "Clustering and Pruning DETs in ADAPT," Intern Mini-Symposium, Sandia National Laboratories, Albuquerque, NM, 2016.
- M. Denman, "Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- J. Cardoni, "Severe Accident Modeling for Cyber Scenarios," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.

- Z. Jankovsky, "Extension of the ADAPT Framework for Multiple Simulators," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "Dynamic Importance Measures in the ADAPT Framework," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "Conditional Tree Reduction in the ADAPT Framework," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "A Dynamic Assessment of Auxiliary Building Contamination and Failure due to a Cyber-Induced Interfacing System Loss of Coolant Accident," International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants, Vienna, Austria, 2017.
- Z. Jankovsky, "Improvements to Usability and Reliability in ADAPT," Intern Mini-Symposium, Sandia National Laboratories, Albuquerque, NM, 2017.

Nomenclature

ADAPT Analysis of Dynamic Accident Progression Trees

ADS Accident Dynamics Simulator

BWR Boiling Water Reactor

CCW Component Cooling Water

CDF Cumulative Distribution Function

CS Containment Spray

CST Condensate Storage Tank

DET Dynamic Event Tree

DHS Department of Homeland Security

DI&C Digital Instrumentation & Control

DP Density Peaks

DOE Department of Energy

DPRA Dynamic Probabilistic Risk Assessment

DSC Dynamic Simple Cyber

DTW Dynamic Time Warping

DYI Dynamic Importance

ECCS Emergency Core Cooling System

ED Euclidean Distance

EDF External Data File

EDG Emergency Diesel Generator

EPRI Electric Power Research Institute

FLEX Diverse & Flexible Coping Strategy

HPSI High Pressure Safety Injection

HX Heat Exchanger

IA Investment Area

IM Importance Measure

ISLOCA Interfacing System Loss of Coolant Accident

LDRD Laboratory Directed Research and Development

LPSI Low Pressure Safety Injection

MCC Motor Control Center

MCDET Monte Carlo Dynamic Event Tree

MD-DTW Multi-Dimensional Dynamic Time Warping

MOV Motor Operated Valve

NRC United States Nuclear Regulatory Commission

NPP Nuclear Power Plant

PORV Pilot-Operated Relief Valve

PRA Probabilistic Risk Assessment

PWR Pressurized Water Reactor

RCP Reactor Coolant Pump

RCS Reactor Coolant System

RHR Residual Heat Removal

RWST Refueling Water Storage Tank

SCADA Supervisory Control and Data Acquisition

SI Safety Injection

SNL Sandia National Laboratories

SOARCA State-of-the-Art Reactor Consequence Analyses

1 Introduction

Industrial control systems, including these in Nuclear Power Plants (NPPs), have historically relied upon supply chain integrity, physical isolation from outside networks, and physical access control for security. With the shift toward increased connectivity and Digital Instrumentation & Control (DI&C) systems, new vulnerabilities to cyber intrusion have been introduced [1]. Nuclear facilities have been compromised in the past both by an open network connection [2] and by software apparently brought in on removable storage media [3]. In the former case, plant operators lost access to a safety display system for hours. In the latter case, the settings on a specific hardware controller were altered.

In order to evaluate the effects of a cyber intrusion, a hypothetical plant model was created based on common Pressurized Water Reactor (PWR) design features [4]. To enable study of a cyber intrusion, the hypothetical plant was assumed to have been upgraded at least in part to digital Supervisory Control and Data Acquisition (SCADA) systems as has been proposed and implemented in multiple existing plants [5, 6]. In particular, the Residual Heat Removal (RHR) isolation system is assumed to have been upgraded [7]. RHR isolation offers an appropriate demonstration of an integrated cyber security risk methodology as it contains multiple active instruments and controlled components and may challenge plant safety if control is lost.

This Laboratory Directed Research and Development (LDRD) project developed a methodology to integrate the study of the progression of a cyber intrusion with modeling of its potential effects on the physical plant for a holistic cyber risk analysis. This methodology brings together emulation of physical control components and network devices as well as industry-standard nuclear power plant safety computer codes under the Analysis of Dynamic Accident Progression Trees (ADAPT) Dynamic Event Tree (DET) scheduling software [8] to generate a coupled dynamic analysis. The cyber intrusion was evaluated with two tools. The first tool used to evaluate the cyber intrusion was the Sandia National Laboratories (SNL) Emulytics[2] methodology with which a network of virtual computers was assembled to represent the architecture of the hypothetical RHR isolation system with high fidelity. A human representative of an adversary was tasked with gaining access to the virtual computer network and altering key control parameters relating to the RHR isolation system.

Insights gained from the comprehensive cyber intrusion model were applied to the second tool which was a piece of custom software developed to simulate the possible choices of a human adversary once within the plant network. Due to the large number of sequences that may be generated within a DET, it would have been infeasible to use the human adversary stand-in to determine the cyber intrusion strategy every time it was required. The custom software tool was controlled under ADAPT along with the physical plant model in MELCOR [10] to determine the consequences of each control state that the adversary may impose upon the system with consideration for the likely response of automated protection systems and plant personnel.

[2] SNL designation for emulative network computing and analytics

The opening of RHR isolation valves during operation has the potential to cause an Interfacing System Loss of Coolant Accident (ISLOCA), which occurs when a low-pressure system is overwhelmed by inadvertent communication with a high-pressure system [11]. This is possible because RHR, a low pressure system, interfaces with the Reactor Coolant System (RCS), a high pressure system. Components within the RHR system are designed (with some uncertain margin) for its operating pressure. Operating plants rely on RHR isolation valves to remain closed to separate the systems during regular operation and to open to allow flow through RHR heat exchangers for heat removal during shutdown. If the valves are opened while the RCS is at full pressure, there is a chance that components rated for lower pressures will fail and spill RCS water outside of containment. This has the potential to both challenge the integrity of the fuel (through loss of coolant) and cause an early release of radionuclides past containment [11].

Section 1.1 gives an outline of the remaining sections of this report. Section 1.2 presents the conclusions that were drawn from this effort. Section 1.3 gives a listing of the works associated with this LDRD that have been published or are nearing publication.

1.1 Structure of the Report

The balance of this report is arranged as follows:

- Section 2 gives a background on the challenge addressed by this LDRD.
- Section 3 presents the combined analysis of a cyber control system intrusion and its impact on a plant model.
- Section 4 describes the enhancements made to ADAPT and the general DET methodology to support the unified model developed for this LDRD.

1.2 Conclusions

This integrated dynamic analysis has advanced the state of the art in the assessment of cyber-induced nuclear power plant accidents. The LDRD has also provided new tools for DETs generation and processing that are already in use for other NPP analyses and may be extended to non-nuclear systems. DETs may now be pruned to eliminate branches that constitute similar sequences to allow a greater diversity of sequences to be run with the same computing and time resources [12]. Additionally, DETs may be generated with an arbitrary number of arbitrary simulators greatly expanding the potential scope of a single DETs [13]. DETs processing has been enhanced with tools to reduce a tree based on physical conditions [14] and to calculate the importance of branched parameters [15].

Key technical accomplishments can be summarized as:

- This research is the first open unified computer model of a cyber intrusion on a nuclear power SCADA system and its ensuing impact on the plant systems
- Advances the fidelity of analysis of cyber exploits on nuclear safety. Industry is struggling to understand scope of cyber risks
  - Facilitates comprehensive and robust assessment and validation of cyber security methods
- Positions SNL to assist Department of Energy (DOE) and United States Nuclear Regulatory Commission (NRC) with assessment and validation of cyber safety case for digital control systems
- Advances the utility of dynamic event trees for analysis of advanced reactor technology severe accidents
  - Addresses NRC expectations for advanced risk analysis methods on advanced reactors with inherent safety features
  - Extends analysis to include multiple simulators to address multidisciplinary analyses

The specific cyber exploit considered in this LDRD, which was the compromise of a NPP DI&C system resulting in the establishment of an ISLOCA by opening the RHR isolation Motor Operated Valves (MOVs) at full RCS operating pressure, was evaluated from multiple viewpoints. The combined cyber-physical analysis described in Section 3 resulted in a DET that is examined for insights in the papers listed in Section 1.3. These papers investigate the relationship between different adversary strategies (see Section 3.1) and the final state of the NPP. The physical effects upon a nuclear plant of the type of ISLOCA induced by the hypothetical cyber exploit have been evaluated in References [15] and [16]. Insights drawn from these analyses include the importance of timing in operator mitigation of the initial MOV opening event as well as the interdependency of emergency systems on support systems such as Component Cooling Water (CCW) which may be damaged in an ISLOCA.

The potential scope of DET analysis has been expanded by this work through the development of the capability to link multiple arbitrary simulators as described in Section 4.1.1. This development is already in use by LDRD 17-0969 *System Theoretic Framework for Mitigating Risk Complexity in the Nuclear Fuel Cycle* to link simulator codes representing different aspects of spent nuclear fuel transportation risk [9]. Additional developments in pruning DETs, evaluating the importance of branching parameters, and reducing a DET based on rules are expected to be fully integrated into ADAPT and used for new analyses in the coming year.

This initial integration of cyber-physical models has led to an increased level of development of both emulytics and DETs as tools to solve advanced cyber security problems for complex systems. Future work is expected to focus on refinement of cyber security models as well as their expansion to a wider variety of components and systems.

1.3 LDRD Publications

A number of journal papers associated with this LDRD are in preparation and review:

- N. Martin, et al., "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," In preparation for *Reliability Engineering and System Safety*, 2017.
- Z. Jankovsky, et. al., "Dynamic Event Tree Analysis with the SAS4A Safety Analysis Code," Submitted to *Annals of Nuclear Energy*, 2017.
- Z. Jankovsky, et. al., "Safety Analysis using Coupled Simulator Code in the ADAPT Dynamic Event Tree Framework," In preparation for *Annals of Nuclear Energy*, 2017.
- Z. Jankovsky, et. al., "Comparison of Measures of Importance in Dynamic Event Tree Analysis," In preparation for *Annals of Nuclear Energy*, 2017.
- R. Williams, et. al., "Emulated Cyber Intrusion of a Nuclear Power Plant Control System: Unified Computer Model," In preparation for *Computers and Security*, 2018.
- R. Williams, et. al., "Computer Modeling of Successful Cyber Intrusion in a Nuclear Power Plant," In preparation for *Journal of Sensitive Cyber Research and Computer Engineering*, 2018.

Conference and invited presentations associated with this LDRD are as follows:

- N. Martin, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- N. Martin, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," Invited Speaker, University of New Mexico Math and Statistics, Albuquerque, NM, 2016.
- B. Seng, "Clustering and Pruning DETs in ADAPT," Intern Mini-Symposium, Sandia National Laboratories, Albuquerque, NM, 2016.
- M. Denman, "Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- J. Cardoni, "Severe Accident Modeling for Cyber Scenarios," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "Extension of the ADAPT Framework for Multiple Simulators," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.

- Z. Jankovsky, "Dynamic Importance Measures in the ADAPT Framework," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "Conditional Tree Reduction in the ADAPT Framework," American Nuclear Society Winter Conference, Las Vegas, NV, 2016.
- Z. Jankovsky, "A Dynamic Assessment of Auxiliary Building Contamination and Failure due to a Cyber-Induced Interfacing System Loss of Coolant Accident," International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants, Vienna, Austria, 2017.
- Z. Jankovsky, "Improvements to Usability and Reliability in ADAPT," Intern Mini-Symposium, Sandia National Laboratories, Albuquerque, NM, 2017.

2 Background

This section describes the challenges associated with the introduction of DI&C systems into NPPs and the background of the hypothesized cyber exploit and its expected effects on the plant. It is important to note that while the plant being evaluated is hypothetical, the individual design features that are present exist in operating plants [17].

Section 2.1 briefly describes the benefits and challenges of DI&C and how it may be exploited. Section 2.2 describes the control system being targeted for this analysis. Section 2.3 walks through how a successful cyber exploit may translate to a plant transient. Finally, Section 2.4 gives the anticipated operator and plant response to the transient.

2.1 Cyber Exploitation of D&IC Systems

Most operating NPPs were built with analog instrumentation and control systems in which continuous electrical signals from instruments are processed by a number of signal modifiers to produce control signals for devices. Control circuits are generally independent which keeps the number of logical states that could exist for each circuit small. The signal modification provided by each device is dependent on its electromechanical properties and thus a change to the control scheme often requires physically adjusting a device or switching to a different one. DI&C offers more flexible control over systems as well as a significant reduction in wiring and the number of control devices. These advantages are realized by passing signals for multiple systems over the same network and by combining many signal modifiers into a single microprocessor. Digital controllers have a large degree of software definition and can be switched to another state with relatively simple commands.

With the addition of digital SCADA systems in new and existing NPPs, there are new failure modes for controlled systems. In addition to failures related to hardware and human operators, which have always been present, there are also potential failures related to software and computer networks. These new failure modes contribute to the likelihood of core damage in ways that cannot be readily captured using traditional Probabilistic Risk Assessment (PRA) techniques [18]. Within this LDRD, a cyber exploit is considered to be the malicious introduction of a software state not intended by the designer which may interfere with accurate transmittal of an instrumented physical parameter or cause a change of state of a piece of hardware being controlled.

Standards have been established for the design and testing of digital SCADA systems in NPPs [19]. Rather than designing costly custom microprocessors and software with a well-defined set of potential states, cyber security standards generally focus on reducing the attack surface of commercially-available systems. Recommendations have been developed based on theoretical understandings of computer systems as well as lessons learned from historical events. Some commonly recommended considerations include:

- Disabling remote access
- Disabling write access in certain operational states
- Disabling removable storage media in certain operational states
- Air gapping sensitive systems
- Data diodes or firewalls

In an NPP, the business network and process-related networks are typically separated by air gapping or a firewall [1]. Cyber exploits may be initiated from the internet and applied to the business network [2], introduced directly to process-related networks through the supply chain, or carried to the process-related networks by inadvertent or intentional insider action [3]. The scope of this LDRD did not include the nature of the introduction of the cyber exploit and it is assumed that access had been gained to a process-related network.

Once within the process-related network, an adversary must identify the features (hardware, software, protocols, etc.) of the network in order to understand how to exploit it. In this work, the adversary was assumed to target features related to the RHR DI&C system specifically instrumentation of primary system pressure and control of isolation valves. With this knowledge and control, the adversary may be able to open the valves when the primary system is at a high pressure (see Section 2.3) in order to ensure that damage is likely.

2.2 RHR System

The relevant portions of the RHR system and their locations relative to containment are represented in Figure 1. The RHR isolation (or suction) valves, which are MOVs, are located inside containment while the rest of the relevant RHR components are outside of containment. The valves are protected against inadvertent opening by interlocks against the RCS pressure which are designed to only allow the valves to open or remain open when the RCS is at a low enough pressure to avoid damage to RHR components. Both PWR [20] and Boiling Water Reactor (BWR) [21] plants have procedures in place to override this interlock in current analog systems, often to hasten the entry into cooling after reactor shutdown. This procedure has failed in the past leaving the system isolated when shutdown heat removal is necessary [21].

Even when the main RHR isolation MOVs are operating properly, relief and venting valves may cause issues. In one case, a relief valve was opened improperly resulting in the loss of approximately 68,000 gallons of water from the RCS to the auxiliary building [23, 24]. On a different occasion at the same plant, the main isolation valve was opened while a vent valve was still open leading to a loss of 620 gallons of RCS water as well as injury and contamination of operators [25]. Both of these events were considered significant ISLOCA precursors by the NRC.

A survey of relevant events reveals a number of similar ISLOCA precursors including [26]:

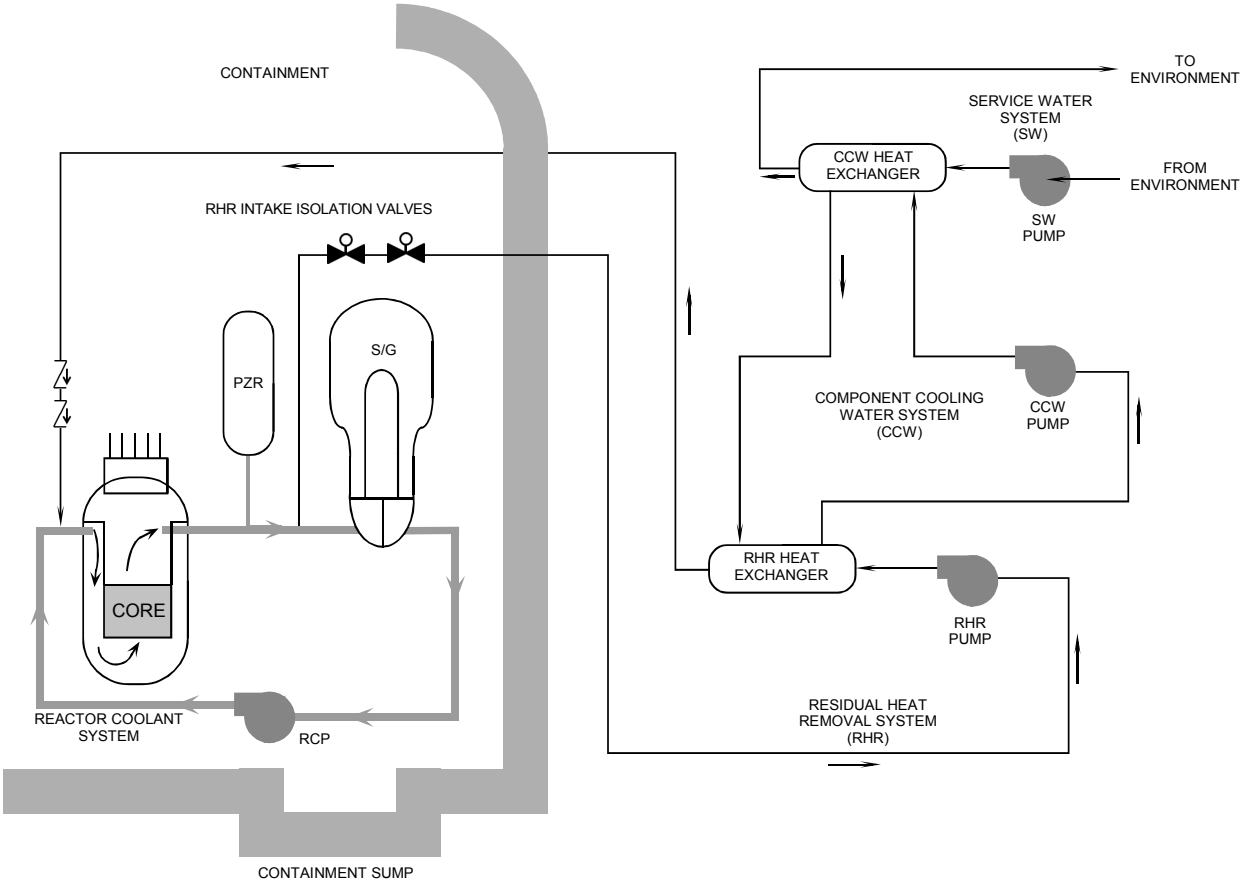

Figure 1: Hypothetical Plant Layout with Residual Heat Removal Component Locations [22]

- *The RHR automatic isolation function had not been tested prior to placing the RHR in operation.*
- *Pressure interlock for RHR suction valve (from RCS hot leg) was bypassed. Operator error and design deficiency.*
- *The pressure interlock setpoint for the RHR suction valve was set above the limits. Pressure transmitter had electrical problems.*
- *LPI containment isolation valve failed to close. A control power fuse blew.*
- *RHR isolation valve would not close. Torque switch was found to be out of adjustment.*
- *RHR discharge isolation valve failed to close. Valve operator torque switch failed due to condensation.*
- *RHR pump suction valve from RCS had leaked due to seat wear.*
- *RHR pump suction isolation valve from RCS hot leg leaked through due to normal wear.*

Such events have become less frequent over time, but new vulnerabilities may present themselves during or after a transition to DI&C. It is assumed that, due to the preference for occasionally overriding the pressure interlocks, in the hypothetical plant such a capability has been implemented using the digital control system and is subject to cyber exploit.

It is assumed that the RHR MOVs will be repeatedly given the command to open making efforts to close them from the control room ineffective. In order to gain full authority over isolation of the RHR system, operators will be required to travel through the auxiliary building to the Motor Control Center (MCC) for at least one of the MOVs and manually send a signal to close the valve (see *MCC1* in the nominal auxiliary building layout in Figure 2).

2.3 RHR ISLOCA

The layout of the lower level of the hypothetical plant's auxiliary building is shown in Figure 2 with *Containment Building* representing to the area inside heavy gray line in Figure 1. Acronyms appearing in Figure 2 that have not been previously defined are: Refueling Water Storage Tank (RWST), Condensate Storage Tank (CST), High Pressure Safety Injection (HPSI), and Emergency Diesel Generator (EDG). This level houses many of the pumps and heat exchangers for systems that interface with the RCS to provide makeup and emergency or shutdown cooling. A number of pipes are routed under and through this level in order to connect tanks, pumps, and the legs of the RCS. A flood may simultaneously disable important emergency systems and make it difficult for personnel to reach those systems for restoration [27].

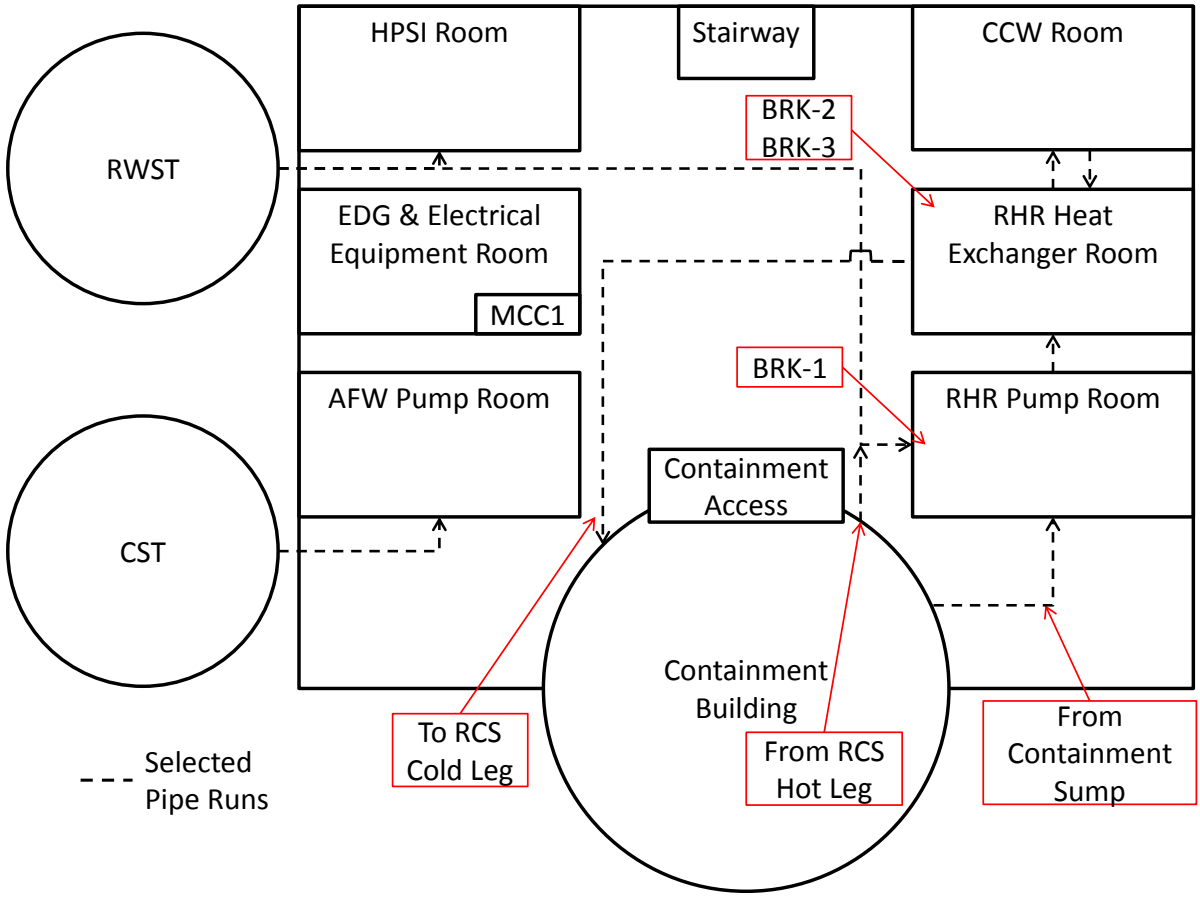

Figure 2: Layout of the Auxiliary Building Lower Level

The relevant components of the RHR system are shown in Figure 3. Acronyms appearing in Figure 3 that have not been previously defined are: Safety Injection (SI), Containment Spray (CS), and Heat Exchanger (HX). In the hypothetical plant, RHR and Low Pressure Safety Injection (LPSI) share pumps and a significant portion of piping. The combination of RHR outside of containment and shared RHR/LPSI exists in operating plants [17]. Water for the LPSI function is provided by the RWST or the containment sump. Flow for RHR enters from RCS hot leg and is cooled by flowing through the HXs which reject heat to the CCW system (shown in Figure 1). Output of the combined system is typically routed to the RCS cold legs.

The general ISLOCA sequence and RHR ISLOCA in particular have been studied both for general plant designs [28, 29] and for specific operating plants [26]. The opening of the RHR isolation MOVs (*RHR-1* and *RHR-2* in Figure 3) at high RCS pressure has the potential to cause damage to both the suction pipe and the HXs. The suction pipe may rupture at some point between the RCS and the RHR pumps as represented by *BRK-1* in Figure 3. The dangerous rise in pressure may continue to propagate damaging the HXs represented by *RHR-HX1* and *RHR-HX2* in Figure 3. If the tubes are overpressurized, ruptures *BRK-2A* and *BRK-2B* may occur. If the pressure pulse from the ruptured tubes is sufficient, the HX shells may rupture causing breaks *BRK-3A* and *BRK-3B*.

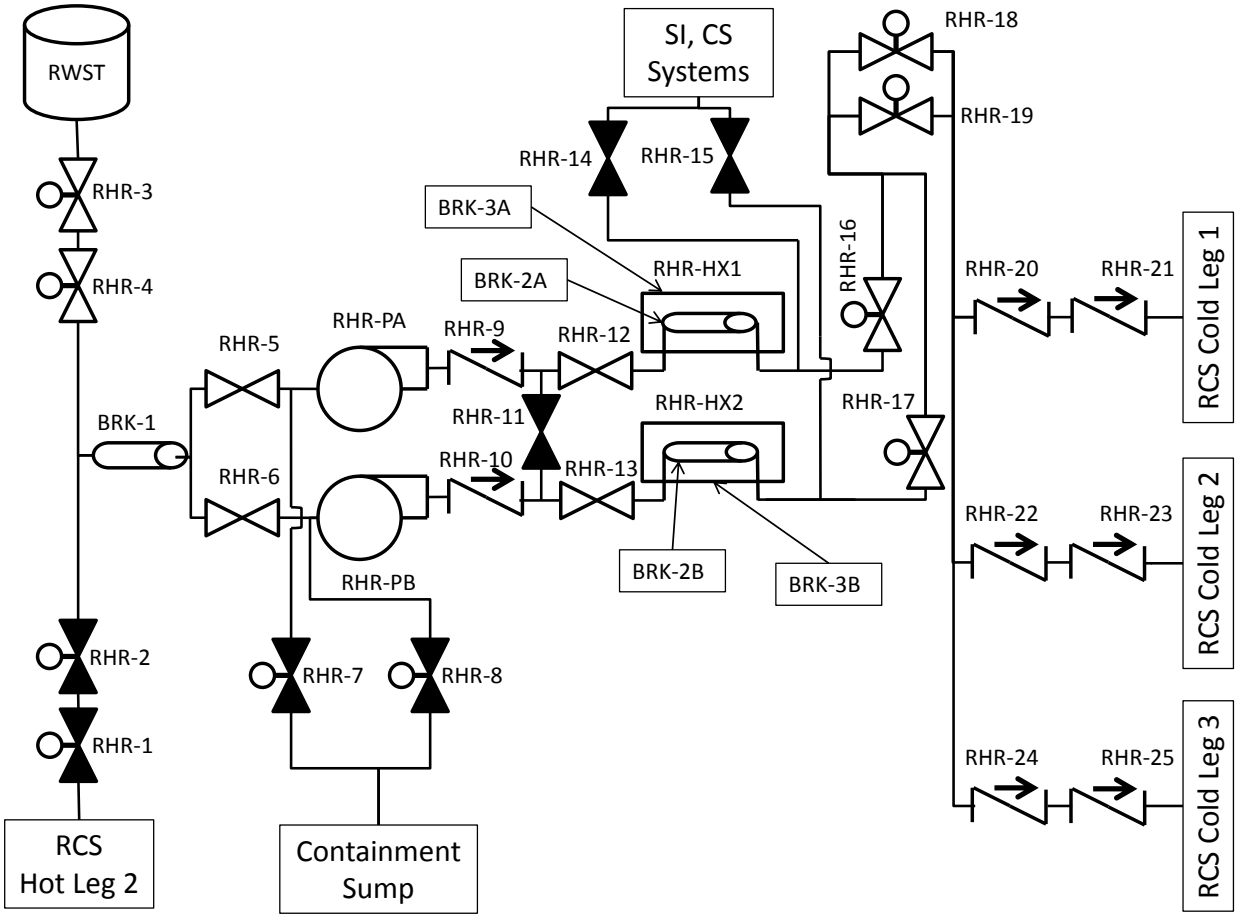

Figure 3: Representative RHR System Layout

An RHR pipe rupture (*BRK-1*) is assumed to disable RWST as a source for LPSI (see Figure 3). Due to the routing of pipes, LPSI may be enabled from the containment sump (if there is sufficient water in the sump) by closing the manual valves (*RHR-5* and *RHR-6*) to isolate the rupture and opening the appropriate MOVs (*RHR-7* and *RHR-8*) to allow flow through the pumps. *BRK-1* will also cause a leak into the RHR pump room (see Figure 2).

An RHR HX tube rupture (*BRK-2*) will not cause a leak to auxiliary building but will overpressurize the CCW system which operates at a significantly lower pressure than RHR. A number of systems depend on cooling from CCW including the pumps for HPSI and RHR/LPSI as well as seal cooling for the Reactor Coolant Pumps (RCPs). Until such a rupture is isolated, the systems that depend on CCW are assumed to be out of service and an RCP seal leak is assumed to initiate. An HX tube rupture may be isolated by aligning manual valves in the RHR HX room (see Figure 2).

An RHR HX tube rupture may in turn cause the HX shell to fail (*BRK-3*) as it is typically rated for a lower pressure than the tubes [28]. This will cause a leak of RCS and CCW water into the RHR HX room (see Figure 2). Additionally, systems that depend on CCW will be out of service until the rupture is isolated by aligning manual valves in the CCW room (see Figure 2). The HXs may be bypassed entirely at the expense of shutdown cooling capacity.

Although multiple pumps and HXs are shown in Figure 3 there is a single suction line from the RCS and failures are assumed to affect both paths equally.

2.4 Plant and Operator Response

If either RHR MOV is opened, there is likely to be an indication in the control room [30]. In this study, no attempt was made to model the success and timing of operators properly diagnosing a cyber exploit. Instead, operators were assumed to issue commands to close the valves in response to open indications (See Section 2.2). After a short time of observing their commands being apparently ignored or reversed, operators were assumed to send teams into the auxiliary building to override the digital controllers for the MOVs. Overriding one controller is assumed to be sufficient to isolate RHR from the RCS. Isolation will stop the loss of RCS inventory arresting the ISLOCA phase of the transient.

If RHR suction pipe or HX shell ruptures occur (see Section 2.3), some RCS inventory will be lost to the auxiliary building. This will initially present to the automated plant protection system as a loss of primary pressure. The ISLOCA considered in the State-of-the-Art Reactor Consequence Analyses (SOARCA) study was smaller than the one considered in this work but the general order and timing of early automated plant actions are similar [31]. Reactor scram and feedwater trip are expected around 20 seconds after a break with Emergency Core Cooling System (ECCS) activation (via HPSI if available) around 26 seconds. The RCPs trip on low pressure around 3 minutes. The exact timing will vary with the extent of the RHR system failures with more damage (and thus more flow into the auxiliary building) leading to a faster progression.

The RCS pressure will tend to fall as long as the pathway to RHR is open. The accumulators, which are small pressurized tanks of water, will passively inject their contents into the RCS within a few minutes. The potential routes for injection of water into the RCS are HPSI using the RWST and LPSI using the containment sump. HPSI may not be available if CCW is out of service. Using the containment sump requires both that any RHR ruptures have been isolated and that sufficient water exists in the sump.

One strategy available to operators is to open the pressurizer Pilot-Operated Relief Valves (PORVs) early in the accident [31]. These valves open a route from the RCS pressurizer (see Figure 1) into containment and are typically used to manage transients in RCS pressure. Opening the PORVs provides an alternative pathway for the RCS depressurization that occurs during an ISLOCA. This has the advantages of keeping more radionuclides inside containment, reducing the extent of flooding in the auxiliary building, and allowing some of the lost RCS water to collect in the containment sump for later recirculation.

The progression of the transient will depend on the time required to isolate leaks and restore emergency and support systems and actions taken within the first minutes to hour will be of utmost importance [31]. The transient is assumed to be terminated by 24 hours by the introduction of Diverse & Flexible Coping Strategy (FLEX) equipment for RCS makeup [32].

3 Emulated Cyber Intrusion of a Nuclear Plant Control System

This section describes the approach used in generating a unified cyber-physical model of the hypothetical plant and assessing the results of the applied cyber exploit. The loss of power generation has been described as part of an existential cyber threat to the United States [33]. The risk has led to regulatory requirements [34, 35] as well as significant research into the reliability of DI&C systems [36, 37, 38]. It should be noted that NPPs have been shown to be vulnerable to some degree of cyber exploitation even without significant deployment of DI&C systems [2].

The method of cyber intrusion was not specified for this work but may influence the scope of the exploit. A pre-programmed piece of code in a controller, which represents a supply chain threat, may be more limited than the threat posed by a live adversary who may have compromised multiple systems simultaneously [34]. This work examined a range of threat sophistication from a single actuation of a set of valves to persistent control of multiple systems (see Table 1).

This research first considered the major physical systems of an NPP to identify a potential target for the demonstration cyber exploit. Systems were compared based on the extent to which active control is used and the likely layout of the instrumentation and control network. Next, the targeted systems were modeled and a nominal path to cyber exploitation was devised. This was accomplished using two tools: one that depends on a human stand-in for the adversary and another that automates the possible adversary choices. The modeled cyber exploit was then linked to a physical plant simulator under a DET driver code to produce a unified model of the exploit from initiation to potential damage to the reactor. This section is laid out as follows:

- Section 3.1 describes the chosen target systems and the effects that their exploitation may have on the plant.
- Section 3.2 briefly diagrams the physical model of the hypothetical plant in MELCOR.
- Section 3.3 details the modeling of the cyber exploit of the target systems.
- Section 3.4 describes how the models of the cyber exploit and the physical system were combined under ADAPT to produce a unified dynamic analysis.

3.1 Target Systems

The primary adversary target in this case is the RHR isolation system (see Section 2.2) which uses a number of instruments and active controls to maintain separation between the RHR system and RCS during power operation. RHR and RCS must be open to each other during shutdown to allow cooling of the RCS and so isolation is achieved using MOVs. Opening these MOVs at high

RCS pressure has a high likelihood of damaging RHR components which may jeopardize long-term shutdown cooling [30]. In addition to opening the MOVs the first time, the adversary may continue to command the MOVs to open after plant operators attempt to close them. It is for this reason that the operators must reach an MCC and override the controller to maintain full control (see Section 2.2).

In addition to RHR isolation, the adversary may target two other systems that are important in an ISLOCA. The first is the set of accumulators which passively inject borated water into the RCS in the event of low pressure (see Section 2.4). These pressurized tanks each sit behind an MOV and a check valve. During operation, the MOV is open and the check valve will open if RCS pressure drops below the tank pressure. During shutdown, the MOV is closed to prevent inadvertent depressurization of the tanks. The adversary may attempt to close the MOV on each accumulator which will prevent it from injecting into the RCS. This potential action was assumed to affect all three accumulators equally. As with the RHR MOVs, the adversary may persistently close the accumulator MOVs against operator attempts to open them.

Finally, the adversary may choose to interfere with the pressurizer PORVs. The PORVs are pathways from the pressurizer to containment with an MOV (sometimes referred to as a block valve) and a pilot-operated valve along the path. The pilot-operated valve is designed to open when RCS pressure exceeds a setpoint and close when pressure drops below a lower setpoint. The MOV is left open except during maintenance and when troubleshooting leaks [39]. If the adversary closes the PORV MOVs, the PORV may be unavailable during the ISLOCA. One potential strategy for managing an ISLOCA is to vent the RCS to containment through the PORVs to reduce the inventory lost outside of containment [31] and this interference would prevent that.

The RHR isolation valves, accumulator MOVs, and PORV MOVs are assumed to be on separate subnets of the plant network. Therefore, assuming control of the RHR isolation valves does not necessarily imply control of any other system and vice versa. While the methods by which an attacker may gain access to separate systems were not the focus of this work, the threat model (see Table 1) recognizes that different levels of access may have different impacts on the physical system.

3.2 Physical Plant Model

The content in this section borrows from Reference [4], which gives a more detailed description of the physical plant model. The MELCOR code (version 2.1) was chosen to model the severe accident progression and source terms for the hypothetical PWR. MELCOR is a severe accident and source term analysis code developed by SNL for the NRC [10]. MELCOR is capable of modeling an NPP accident from initiation (e.g., loss of offsite power or a pipe break) to the timing and extent of radionuclide releases to the environment. This encompasses phenomena related

to thermal-hydraulics, fuel damage and degradation, radionuclide transport, and combustion of flammable gases. This project called for a fast and stable model that was capable of simulating many variations and sensitivity/uncertainty studies of the chosen base accident sequences. The result was referred to as the Dynamic Simple Cyber (DSC) model.

Figure 4 depicts the nodalization of the RCS. Each coolant loop is separated into four volumes (2 hot leg volumes and 2 cold leg volumes) and the surge line and pressurizer each have one volume. The rupture disk flows to the relief tank cubicle in the containment. The rupture disk is assumed to open if the relief tank pressure reaches 100 psig. Dynamic flow paths are implemented for potential creep rupture for each hot leg and the surge line.

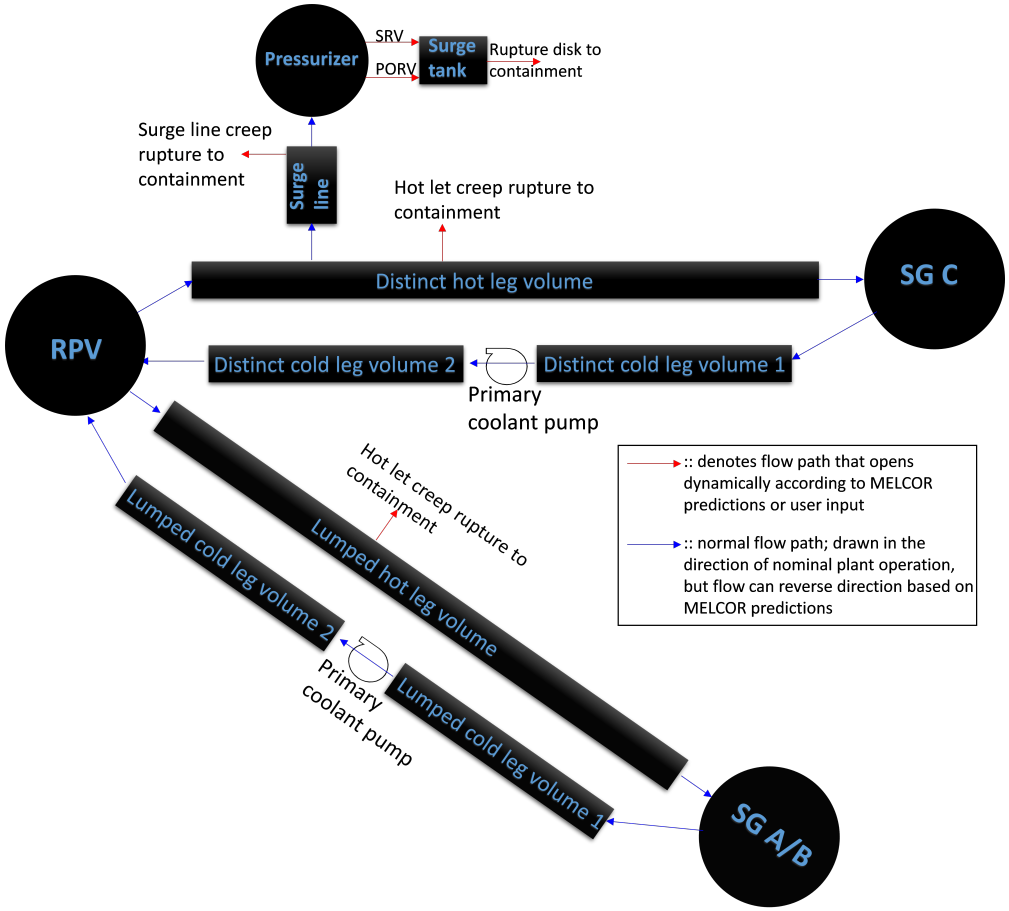

Figure 4: MELCOR Model Layout

Portions of control systems may be modeled in MELCOR using mathematical/logical relationships between variables and the Control Function package. However, this capability was determined to be insufficient for modeling a cyber exploit of a DI&C system. It was decided that the end-to-end scenario would join cyber exploit modeling using another piece of software (see Section 3.3) with the DSC physical plant model in MELCOR. To facilitate this, external interfaces were established for MELCOR process state variables that would be read and written by the cyber exploit models. The External Data File (EDF) package was used to produce files that can be read by the cyber exploit models. These files represent network-addressable instruments such as pressure transducers

and valve position indicators that in reality could be queried over the plant network for their values. The EDF package can also be used to input new data to a MELCOR model. This was used to allow the cyber exploit model to assign new valve states if the adversary took action in a given branch. A full description of the DSC model may be seen in Reference [4].

3.3 Cyber Exploit Modeling

Computer modeling was used to represent the network subject to the cyber exploit rather than assembling a network of the actual hardware and software to be examined. This is common in cases where experimenting with the actual system of interest is prohibitively dangerous or expensive [40]. The models were designed to be of a fine enough granularity to provide actionable insights while simultaneously being capable of running many thousands of times in a reasonable time period for a Dynamic Probabilistic Risk Assessment (DPRA) analysis.

First, a model was created using the SNL emulytics tool Sceptre as described in Section 3.3.1. This provided a high fidelity platform for a human stand-in for the adversary to attempt to penetrate the network and interfere with systems. Because this model required a human stand-in, it was considered unsuitable for DPRA and its insights were distilled into a custom piece of software referred to as hacker.exe which is described in Section 3.3.2.

3.3.1 Sceptre

A network topography was created to represent the hypothetical RHR isolation system in the SNL emulytics tool Sceptre. The general emulytics process is shown in Figure 5 and involves the use of both physical and virtual devices to represent a target network. Represented devices may include programmable logic controllers, remote terminal units, front end processors, human machine interfaces, and protection relays. The SCADA protocols Modbus, DNP3, and IEC61850 may be implemented in Sceptre to communicate between devices. Physical hardware may also be integrated into the Sceptre network but was not available for this work. Sceptre integrates these simulated and real components under a single platform to allow a human adversary to interrogate network features and identify weaknesses.

The human adversary interfaced with the outward-facing components of the hypothetical plant network (see Figure 6) with the goal of accessing a virtual valve controller. The adversary used a personal computer connected to the network. The first line of defense was the virtual firewall, which is designed to allow only approved connections from outside of the plant network. The firewall, router, and valve controller were represented by virtual machines run under the Sceptre platform. After defeating the firewall the adversary had to navigate internal network routing and identify a targeted valve controller. A model of the plant running at steady state in the MELCOR

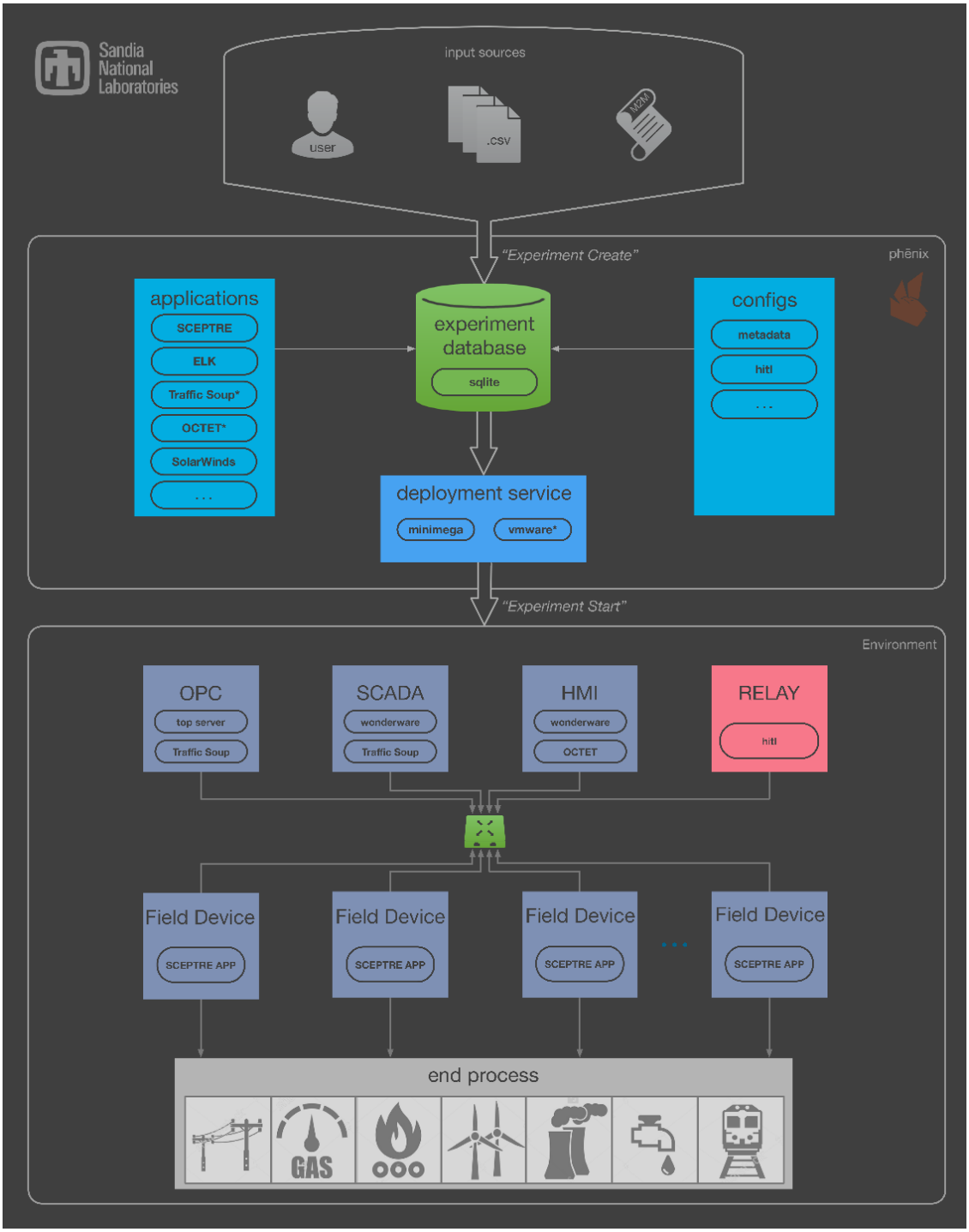

Figure 5: Emulytics Environment

simulator code was executed on a computer cluster to represent the physical state of the plant including the RCS pressure and RHR isolation valve states. The computer cluster was connected to the virtual plant network through a router but not a firewall as it was considered to be within the plant network. Plant state information was linked to the virtual network to represent instrumentation of RCS pressure and valve position status. This plant state information was read by the

adversary to decide when to issue a valve open command to the controller as seen in Figure 7. Because an ISLOCA is most damaging at high RCS pressure, the adversary ensured that the pressure was high and that the RHR valves were closed before issuing a command to open them. The adversary also decided at that point whether to interfere with the accumulators and PORVs.

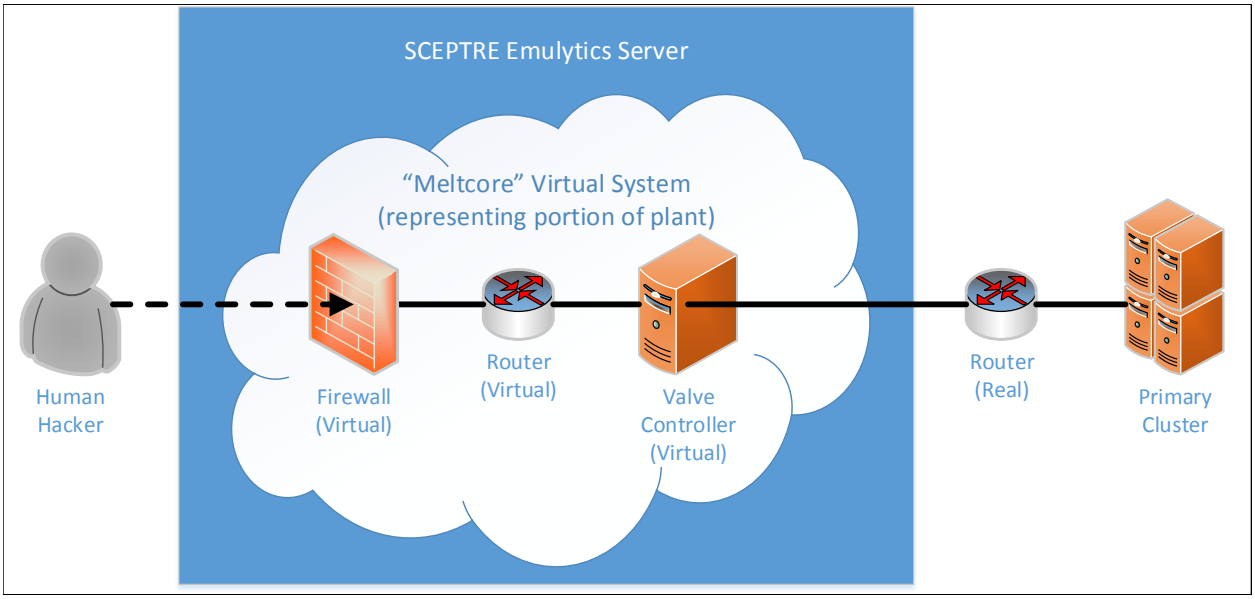

Figure 6: Live Adversary Exploit of Emulated System

In this model the valve opening command was linked to a script that stopped MELCOR execution, modified an input file with appropriate new valve states, and restarted MELCOR. This unified the cyber and physical models in an end-to-end analysis allowing different adversary strategies to be evaluated for their immediate effects on the physical plant. Pathways were established for the adversary to gain control of the valve controllers for each of the three targets. However, the Sceptre method was determined to be incompatible with a DPRA analysis of the scenario. Each sequences required a large network of virtual machines to be spawned as well as a human to make multiple decisions. Instead, the Sceptre analysis was used to draw insights into the potential paths of the cyber exploit to be applied to a reduced-order model that could be used for DPRA (see Section 3.3.2).

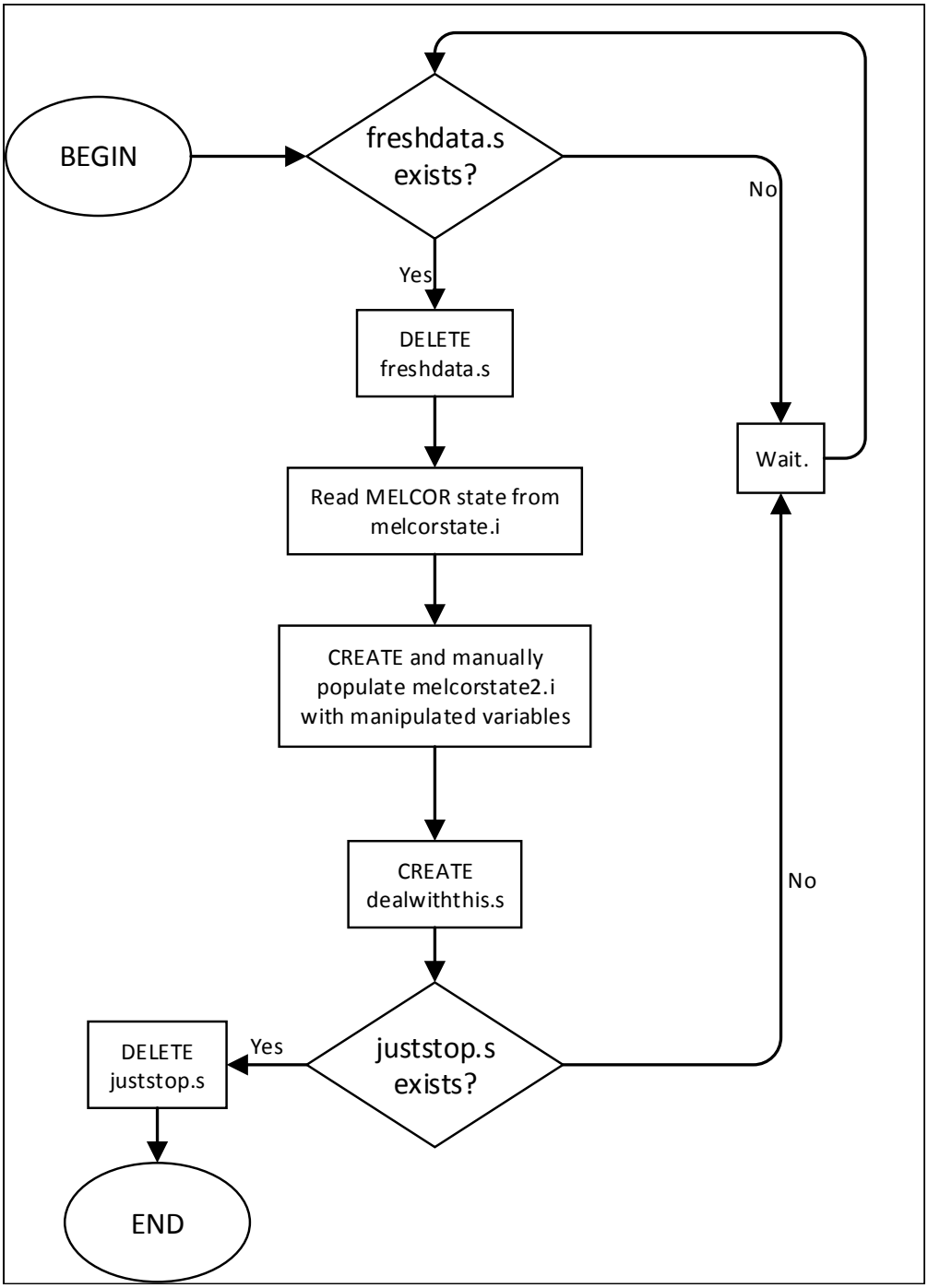

Figure 7: Human Adversary Behavior

3.3.2 hacker.exe

The insights gained from the process of using Sceptre were encoded into a custom piece of software called hacker.exe. This software captured the range of possible actions taken by the adversary as described in Section 3.3.1. These are tabulated in Table 1. The advantage of hacker.exe for DPRA is that it provides the same process state variable changes to MELCOR as Sceptre without the use of a human actor. This allows hacker.exe to be applied in a DET that may produce many thousands of branches without requiring excessive human attention.

Table 1: Potential Attack Scenarios

Scenario	RHR Valve Attack	Accumulator Valve Attack	PORV Attack
1	**Instantaneous**	**None**	**None**
2	Instantaneous	None	Instantaneous
3	Instantaneous	None	Persistent
4	Instantaneous	Instantaneous	None
5	Instantaneous	Instantaneous	Instantaneous
6	Instantaneous	Instantaneous	Persistent
7	Instantaneous	Persistent	None
8	Instantaneous	Persistent	Instantaneous
9	Instantaneous	Persistent	Persistent
10	**Persistent**	**None**	**None**
11	Persistent	None	Instantaneous
12	Persistent	None	Persistent
13	Persistent	Instantaneous	None
14	**Persistent**	**Instantaneous**	**Instantaneous**
15	Persistent	Instantaneous	Persistent
16	Persistent	Persistent	None
17	Persistent	Persistent	Instantaneous
18	**Persistent**	**Persistent**	**Persistent**

The process followed by hacker.exe is shown in Figure 8. This is similar to that followed by the human adversary as diagrammed in Figure 7. The strategy used in hacker.exe is determined by the scenarios in Table 1 and is given to the model in an input file. This input file has three input parameters (RHR strategy, accumulator strategy, and PORV strategy) and was designed to be easily modified in order to facilitate the dynamic analysis described in Section 3.4. Once a valid strategy is loaded, hacker.exe waits until a new MELCOR EDF file exists. This represents querying digital assets across the plant network and waiting for a reply. Once data is received it is read and action may or may not be taken according to chosen strategy. If action is taken, new process states are written to a MELCOR EDF file and a signal file is produced to indicate that hacker.exe has finished. This process iterates until hacker.exe is commanded to stop (via the presence of a specific signal file) which allows for a persistent valve opening strategy to be applied.

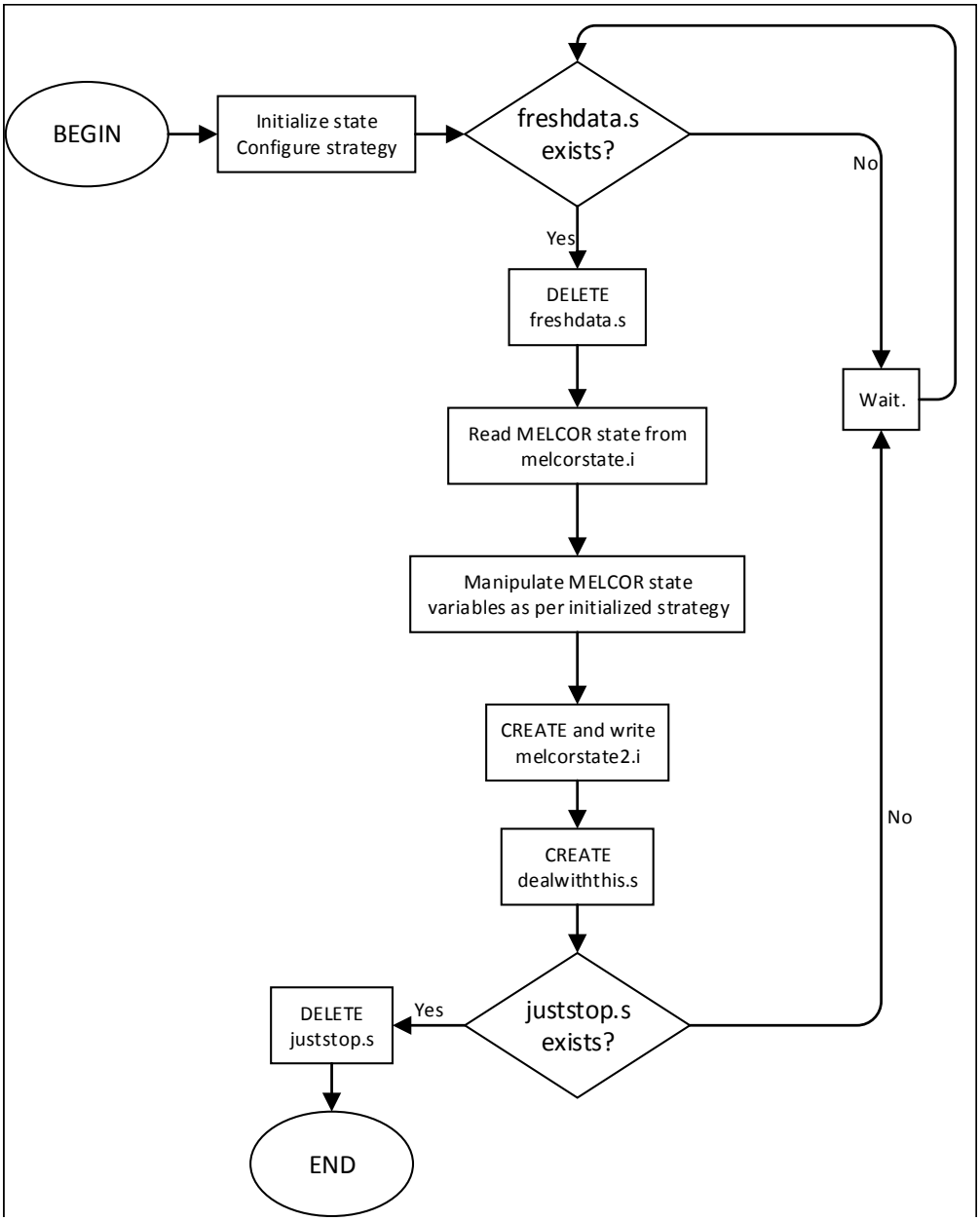

Figure 8: Automated hacker.exe Behavior

3.4 Integration of Cyber-Physical Models

The separate cyber and physical models address different phenomena related to the cyber exploit which are each of value in assessing the risk to the hypothetical plant. However, the integration of the models into a single dynamic platform offers greater flexibility in perturbing the models and better tractability of the results. The DET approach implemented in ADAPT has been applied to numerous accident scenarios and reactor technologies [41, 42, 43, 44] and the lessons learned from

these previous analyses have been applied in this case. For example, it is important to tailor the scope of a DET to uncertainties of significant interest due to the computational time cost of each additional branching condition [41]. Each binary branching condition, assuming it occurs once and only once per sequence, results in a doubling of the number of end states in the DET.

The ADAPT DET generator was expanded for this work to allow the linking of multiple arbitrary simulators (see Section 4.1.1). The hacker.exe and MELCOR models were combined into a single set of DET input and run on a computer cluster. The scenario begins with the MELCOR model running at a steady state which represents a normal day of operation. At a pre-determined time a branching condition is triggered for the adversary strategy. At this point the analysis splits for every strategy to be considered. The strategies in Table 1 that were chosen as transient initiators for the dynamic analysis are bolded. Scenario 1 was selected as a baseline cyber exploit of the RHR isolation system. This required a single manipulation of one control system. Scenario 10 represented an increased level of sophistication as it required continuous communication with the plant network to effect a persistent exploit. Scenarios 14 and 18 represented further increases in sophistication as multiple systems were compromised which in reality would be on separate sections of the plant network and thus require more effort to compromise.

Numerous aleatory and epistemic uncertainties were modeled in the MELCOR model that relate to how the ISLOCA could be expected to progress. Insights from the literature were applied to ensure that a reasonable scope was maintained and that risk-significant uncertainties were addressed. For example, the impact of the cyber exploit was assumed to be dependent on the pressure capacity of RHR components. The opening the RHR MOVs is modeled in MELCOR as a flow path opening which may result in a pressure pulse in the control volumes that represent RHR components. If the pulse does not exceed the sampled capacity of a component, it is assumed to remain intact.

Cumulative Distribution Functions (CDFs) for the capacities of the RHR suction piping and HXs were taken from References [45] and [28], respectively, and are shown in Figure 9. Initially-sampled points are starred for each CDF. These were reduced to two or three samples in most cases to reduce the computational cost. For a detailed listing of the physical and operator uncertainties considered in the analyses performed under this LDRD, please see References [7] and [16].

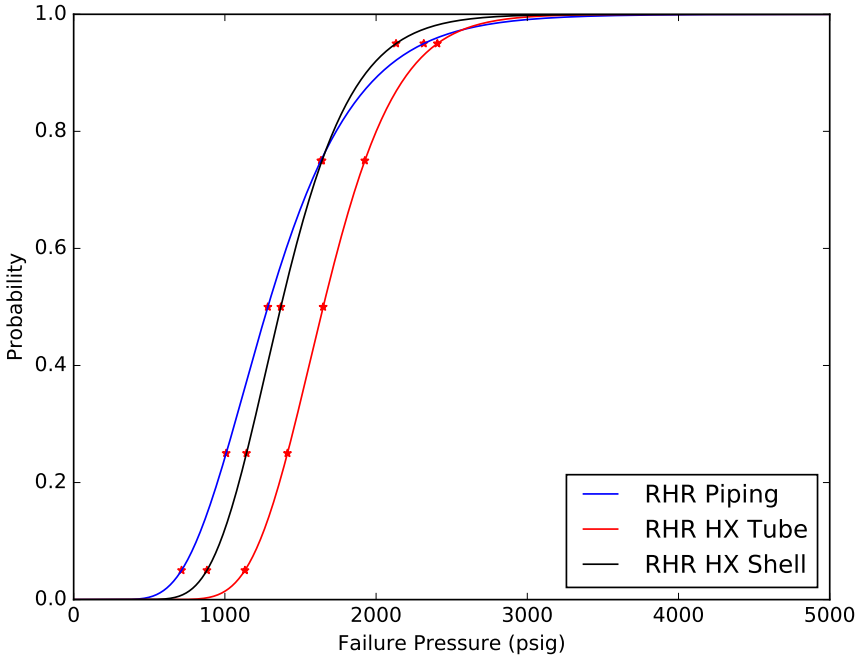

Figure 9: CDF for RHR Component Capacities

4 ADAPT and General DET Advancements

This section describes modifications made to the ADAPT DET driver code to accommodate the models used for the cyber intrusion event initiation and plant response (see Section 3). The first set of enhancements are focused on ADAPT as a platform and are presented in Section 4.1. Changes were made to allow ADAPT to use multiple simulators and to have the capability to retrieve a reduced version of a chosen DET. The second set of enhancements given in Section 4.2 focus on the DET generation and analysis processes. One effort allows the sequences of a DET to be clustered and pruned as the DET is growing, allowing a greater diversity of sequences to be run in the same computation time. The final enhancement was the development of a flexible set of importance measures for DET input parameters.

An NRC white paper laid out a number of desired characteristics for advanced PRA tools which include the following that are addressed by this work [46]:

- *Makes process and results more scrutable*
- *Allows for consideration of alternative risk metrics*
- *Leverages advances in computational capabilities and technology developments, but is computationally tractable*
- *Allows for ready production of uncertainty characterization*
- *Permits simplification for regulatory application at a later time (i.e., after it has been sufficiently developed and applied)*

4.1 Enhancements to ADAPT

In order to generate the combined DET proposed in Section 3, ADAPT was extended to allow the use of an arbitrary number of arbitrary simulators as described in Section 4.1.1. A DET analysis, particularly one combining the uncertainties of multiple simulator codes, may generate an overwhelming amount of data. One strategy to cope with this data is to reduce the scope of the DET being examined. Section 4.1.2 presents a tool that takes user-specified time-dependent rules and applies them to the DET returning sequences that meet the rules. These sections borrow from References [13] and [14], respectively.

4.1.1 Extension of the ADAPT Framework for Multiple Simulators

One limitation of the DET driver codes developed to date, namely ADAPT [8, 41], Accident Dynamics Simulator (ADS) [47], and Monte Carlo Dynamic Event Tree (MCDET) [48], is that the tree is typically driven by a single simulator[3]. This generally limits the parameter space that may be explored in a single DET to that which may be covered by a single simulator. The goal of this effort was to produce a generalized multi-simulator driver. This capability will increase the depth and breadth of phenomena that may be analyzed in a single DET.

The initial development of ADAPT focused on flexibility and as such it has been linked to a wide range of simulators including MELCOR [8], RELAP5 [49], SAS4A [44], and MAAP4 [50]. However, an initial design choice was that it would be used with a single simulator at a time. The primary changes required to allow ADAPT to manage multiple simulators were in the handling of branching rules and the spawning of new jobs.

The changes to handling of branching rules in ADAPT are best exhibited by comparing the old (Listing 1) and new (Listing 2) input forms of the branching rules file. The branching rules handler script previously received the elapsed simulation time and the name of the branching rules file as inputs. In addition to those, the name of the simulator (i.e., *melcor-pri*) that just finished is now passed as well which allows the handler to prepare information about the branch for the database. First, the handler must determine which message file to read to determine the branching condition that occurred. It should be noted that, where changed, the new field name (as reflected in Listing 2) is used in this report.

Listing 1: Sample of Original ADAPT Branching Rules

```
1  Input file: sbo.inp.tpl
2  Stopping Rule: sbo.mes ADAPTSTOP 2
3  Separator: "{" "}"
4  T1 5 0.764 1.000 1.310 1.931 1e20
5  T1p 5 25 50 75 95 95
6  INIT V30903 0.518
7  INIT V69801 0.0
8  310 1 V30903 T1
9  310 2 V30903 1e20
10 6982 1  V69801  1.0
11 6982 2  V69801  0.0
12 terminate_early after 60 seconds 310/2 6982/1
```

[3]While ADS-IDAC typically produces a DET using both RELAP5 and IDAC, these codes are tightly coupled into a single package.

Listing 2: Sample of New ADAPT Branching Rules

```
1  InputFile 1 sbo.cor.tpl
2  StoppingWord 1 sbo.mes ADAPTSTOP 2
3  VarSeparator 1 "{" "}"
4  SimulatorExecutable 1 melcor-pri
5  InitialSimulator 1
6  BranchingSimulator 310 1
7  BranchingSimulator 6982 1
8  TableProbabilityType T1 CDF
9  T1 5 0.764 1.000 1.310 1.931 1e20
10 T1p 5 25 50 75 95 95
11 INIT V30903 0.518
12 INIT V69801 0.0
13 310 1 V30903 T1
14 310 2 V30903 1e20
15 6982 1  V69801  1.0
16 6982 2  V69801  0.0
17 terminate_early after 60 seconds 310/2 6982/1
```

The simulator name that was passed to the script as an input is translated to a number using the field *SimulatorExecutable* in Listing 2. The message file containing the reason for stopping associated with that simulator number is found in the *StoppingWord* field along with where to search within the file. In the case of Listing 2 for Simulator 1, ADAPT will search the file *sbo.mes* using the 2nd word on the line that contains the word *ADAPTSTOP* as the branching condition. If new branches are required, the handler must determine which simulator input file is to be modified. The field *BranchingSimulator* associates each branching condition with a simulator to be run after it is reached. Finally, the name of the appropriate input file is found in *InputFile*. Within each template input file, ADAPT variables are set off using separators as defined in *VarSeparator*. It is important that these symbols do not appear elsewhere within the template input file. As codes have differing input requirements, these may vary between simulators. The simulator to run for the first branch is defined by *InitialSimulator*.

These changes preserve the ability to function with a single simulator and do not establish an upper limit on the number of simulators ADAPT may manage. Error handling has also been added giving the user feedback on the location of any detected improper input. When new branches are required according to the branching rules, they are added to a queue in the form of an entry on a database table. Information such as the branch's probability, parent branch, and location of input files are stored in this entry. When the ADAPT driver pulls the branch from the queue to run, it prepares the necessary environment variables so that the appropriate executables and input files may be found. This includes the simulator as well as any post-processing tools.

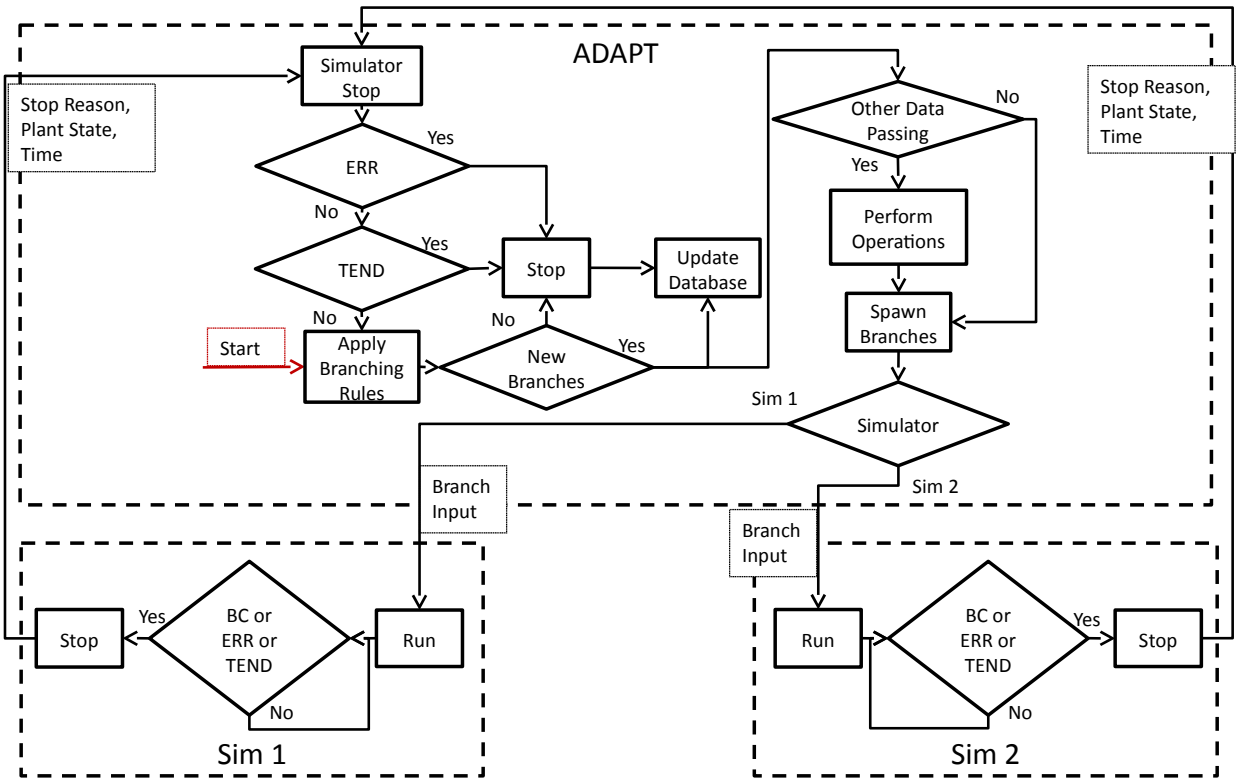

Figure 10: Data Flow Process for ADAPT with Multiple Generic Simulators (Sim 1 & Sim 2)

To facilitate the use of multiple simulators, it was necessary to carry the name of the simulator for each new branch through to the database and to instruct the driver how to handle it. The former is accomplished by adding a field to the branch database table which indicates the simulator to be run. This field has also been incorporated into the visualization of the tree to inform the analyst of how control of the sequence passes between the simulators. When the ADAPT driver prepares a new branch to run, it now passes the simulator name as an environment variable. This is visible to the wrapper script (see Figure 10) and is used to determine which input file and simulator to run.

The data flow process shown as Figure 10 represents a general multiple simulator linking between ADAPT and two generic simulators (Sim 1 and Sim 2). Note that *BC* represents a simulator stop for a branching condition, *ERR* represents a stop on a simulator error, and *TEND* represents a stop due to reaching maximum problem time. Stops for *ERR* and *TEND* both result in no additional branches being created. The appropriate simulator for each new branch is determined by the branching rules.

This enhancement is expected to increase the potential scope of a DET in three ways. First, initiating conditions that have historically been static may now be treated dynamically. This decreases subjectivity in the case of initiating events that may adapt based on the plant's response to the initial perturbation, such as a cyber exploit of a DI&C system. Secondly, complex phenomena may be handed off to a specialized code when necessary. Previously this required coupling the simula-

tors in a way that would be invisible to a DET driver code. The modifications will lead to a more visible and tractable approach when refined treatment is necessary. Finally, it will be possible to mechanistically combine codes that handle different stages of an event such as MELCOR (which calculates radioactive releases) and MACCS (which calculates the consequences of a release) [43].

4.1.2 Conditional Tree Reduction in the ADAPT Framework

A DET may be orders of magnitude larger than a traditional event tree for the same initiating event as more of the uncertainty space is likely to be explored and the tree does not require manual assembly. Because of the size, manual inspection of the entire DET is often infeasible. A method has been added to ADAPT to take a "slice" of the DET applying user-input time-dependent rules to decide which sequences to return for closer examination.

When taking a slice of a DET, the first step is to create a copy of the DET. This is done within the ADAPT database and proceeds from the initial branch to end states preserving heritage and probabilities. Copying the target DET allows easier manipulation of the sliced tree and recalculation of probabilities conditional on the slicing rules if desired. Three tables are updated. First, a new experiment is added to the *experiments* table with a description indicating it is a copy. The branches are copied next proceeding iteratively by generation. This is to preserve the heritage of branches and thus the shape of the DET. Finally, each job is copied in order to locate output data files associated with each branch. The files from the original DET are referenced rather than copied to minimize the impact on storage space as a large DET may require terabytes of storage.

A slice of a DET may be manipulated in the database and viewed in the web interface in the same way as its parent. This includes updating the conditional probabilities of branching conditions. When building a sliced DET the user first chooses a DET to examine from among those that have finished running. A complete copy is created to be trimmed later in the process. Next, rules are created which are comprised of the 6 Fields shown in Table 2. A set of sample input is also shown in Table 2.

Table 2: Required Input & Sample Input for Rules

Input Field	Sample Input
Name	*Low primary pressure early*
File	*plot_CVH-P_520*
Parameter Value	*8 MPa*
Parameter Operator	*2*
Time Value	*3600 s*
Time Operator	*2*

Using the sample rule in Table 2, ADAPT will expect the file *plot_CVH-P_520* to exist in each branch directory and to have two columns which give simulation time and value. Parameter Operator and Time Operator types given in Table 3 define whether the plotted simulator data must be greater than, less than, or equal to the rule value in order to pass. The sample rule is satisfied if at any time less than 3,600 seconds there is a pressure value less than 8 MPa. It is anticipated that Parameter Operator 3 and Time Operator 3 in Table 3 will be used only where a parameter has a limited set of discrete values or when the data plotting time interval is prescribed, respectively.

Table 3: Parameter and Time Operator Values for Rules

Operator	Intent
1	Plot value greater than rule value
2	Plot value less than rule value
3	Plot value equal to rule value

Once all rules are entered, the DET is searched for end states. These are identified by finding branches that are finished and are not listed as parent branches. The heritage of each end state is identified by following parentage until the root branch is reached. An outer loop is performed over all end states and an inner loop is performed over all rules. For each end state and rule, data is assembled by reading the file specified by the rule for all branches from the root to the end state and combining the values in order. Next, the data is searched for entries within the relevant time period that meet the rule. Once all end states have been evaluated, branches that are marked for deletion are removed creating the sliced DET.

Calculations related to results and probabilities may be performed on a sliced DET in an identical manner to its overall DET. This technique will simplify the analysis of complex DETs by empowering the analyst to interrogate a narrow section of the DET.

4.2 Advances in Dynamic Event Tree Methods

Three techniques were identified and developed for reducing and interpreting a DET. First, Section 4.2.1 summarizes a methodology to identify similar sequences and if desired prune them from the DET reducing the computational time requirement. Section 4.2.2 presents a new methodology for determining the influence of a chosen branching condition on a continuous measure of consequence (e.g., core damage extent). These sections borrow from References [12] and [15], respectively.

4.2.1 Pruning of Discrete Dynamic Event Trees using Density Peaks and Dynamic Time Warping

One of the challenging aspects of the DET method is that a large number of branches are produced for each initiating event. This can result in data that is difficult to organize and time consuming to analyze. A DET often has sequences that do not contribute to variability of the overall results and their predictive capabilities. Therefore, a pre-pruning algorithm was proposed which works to remove low-value sequences and consequently reduce the complexity and computational cost of the tree.

Pre-pruning works as the DET is growing by preventing the growth of branches that do not improve the predictive power of the tree [51]. Therefore, it reduces the time needed to both grow and analyze the tree. The critical choices that must be made are when and where to prune the tree. The chosen pre-pruning algorithm stops the growth of a branch when its time series is sufficiently similar to that of another branch. Before pruning can occur, branches with similar features must be clustered together. There are a few key points to consider when choosing a clustering algorithm:

- Scalability - how well can this algorithm perform with large data sets?
- Arbitrary-Shaped Clusters - can this algorithm find clusters that are non-spherical?
- Parameters - how many user-defined parameters are required? How sensitive are these parameters?
- Noisy Data - how does this algorithm handle deviations in the data?
- High Dimensionality - will preprocessing of high-dimensional data be necessary?

The clustering algorithm chosen for this effort is Density Peaks (DP), which was recently proposed in [52]. This algorithm has the following advantages over other available clustering algorithms:

- DP is able to find clusters of arbitrary shapes.
- It only requires 2 user-defined parameters neither of which are exceptionally sensitive.
- The algorithm has the ability to deal with noisy data, which is particularly important with the data that is generated from the severe accident simulators.
- The distance measure used can be easily extended into multi-dimensions.

The DP algorithm works to cluster data points based on their local density. To determine cluster centers two values, ρ and δ, must be found for each point. The steps for these calculations are shown in Algorithm 1. The ρ calculation requires an input of a distance matrix D as well as a user-determined threshold d_c. Lines 2-4 show that for each point in the matrix the number of data

points within d_c is determined and denoted as ρ_i. The values of all ρ_i are then sorted in descending order and this sorted list is used as an input for the δ calculation. Lines 6-9 show that for each point the distance of the closest data point of higher density δ_i is found. Cluster centers are then defined as those points that have the highest values of $\rho_i * \delta_i$ as seen in Line 11. After the cluster centers have been decided, points are assigned to the nearest neighbor cluster center from the list of points with higher density [53].

Algorithm 1 Density Peaks

1: **procedure** ρ_CALCULATION(D, d_c)
2: **for** i = 1:n **do**
3: $\rho(i) = count(D(i, otherObjects) < d_c)$
4: $ord\_\rho = sort(\rho, 'descend')$
5: **procedure** δ_CALCULATION(ord_ρ)
6: **for** i=1:n **do**
7: $\delta(ord\_\rho(i)) = max(D(ord\_\rho(i)))$
8: **for** j=1:(i-1) **do**
9: $\delta(ord\_\rho(i)) = min(dist(ord\_\rho(i), ord\_\rho(j)))$
10: **procedure** CLUSTERCENTERS(ρ, δ)
11: $clusterCenters = top(sort(\rho * \delta))$

For time series data such as that produced by a simulator in a DET, there are numerous distance measures that can be used to create the distance matrix that is used in the density peaks algorithm. Many in the research community have determined that Dynamic Time Warping (DTW) is a superior choice as a time series distance measure and it has been found to regularly outperform the Euclidean Distance (ED) [53]. DTW is more robust than the ED due to the fact that it can identify similarities between two time series even if there is a lag between the two series. Figures 11 and 12 show how clustering using DTW is able to find similar time series paths even though they are temporally offset.

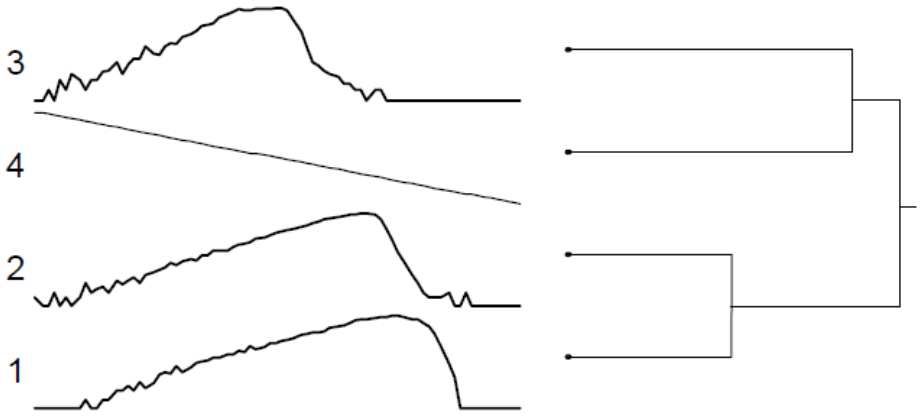

Figure 11: Clustering using ED.
Though series 3 is visually more similar to series 1 and 2 the ED clustering is unable to account for the time lag between them [54].

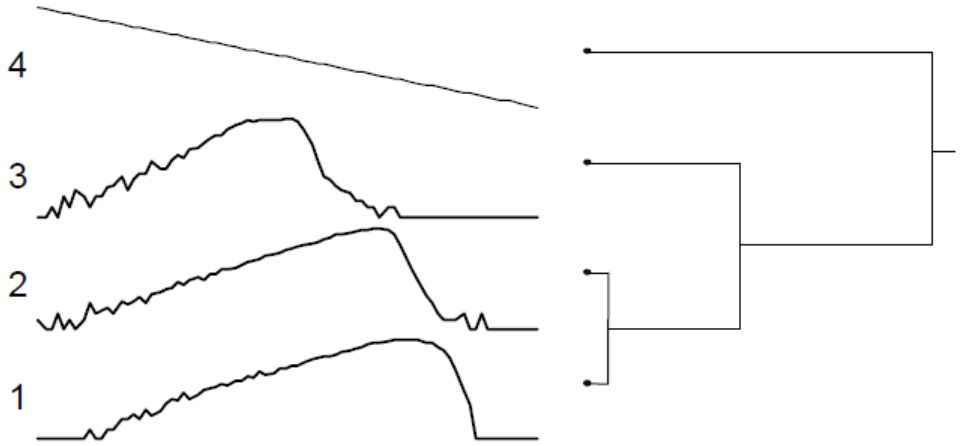

Figure 12: Clustering using DTW.
This is more intuitive in that it is able to identify that series 1, 2, and 3 are similar [54].

DTW is a relatively simple algorithm that first calculates the pairwise Euclidean distance between each time step in two time series. These pairwise distances form a matrix and the algorithm works to find an optimal path through the matrix that minimizes the Euclidean distance. The optimal path is formed as follows: let Q and C be two time series. Define $d(q_i, c_j)$ to be the squared Euclidean distance between points q_i and c_j. Then, we can create a distance matrix D as seen in Equation 1. Figure 13 shows an example of the optimal path that is formed through the distance matrix.

$$D(i,j) = d(q_i,c_j) + min[D(i-1,j-1), D(i-1,j), D(i,j-1)] \tag{1}$$

The extension to the multi-dimensional case is straightforward. In Multi-Dimensional Dynamic Time Warping (MD-DTW), it is assumed that each dimension is independent. The one-dimensional DTW distance is calculated for each dimension separately and then those values are summed to get a total distance measure. If $D(Q_m, C_m)$ is the DTW distance of the m^{th} dimension of Q and C then we can calculate the MD-DTW distance matrix as:

$$MD(Q,C) = \sum_{m=1}^{M} D(Q_m, C_m) \tag{2}$$

Pruning occurs after cluster centers have been determined using the DP algorithm. During initial testing, pruning was performed on fully grown DETs so that the DET could be used to evaluate the properties of the pruned tree. Implementation of online pre-pruning into ADAPT is under way along with tools to assist the user in choosing clustering and pruning parameters.

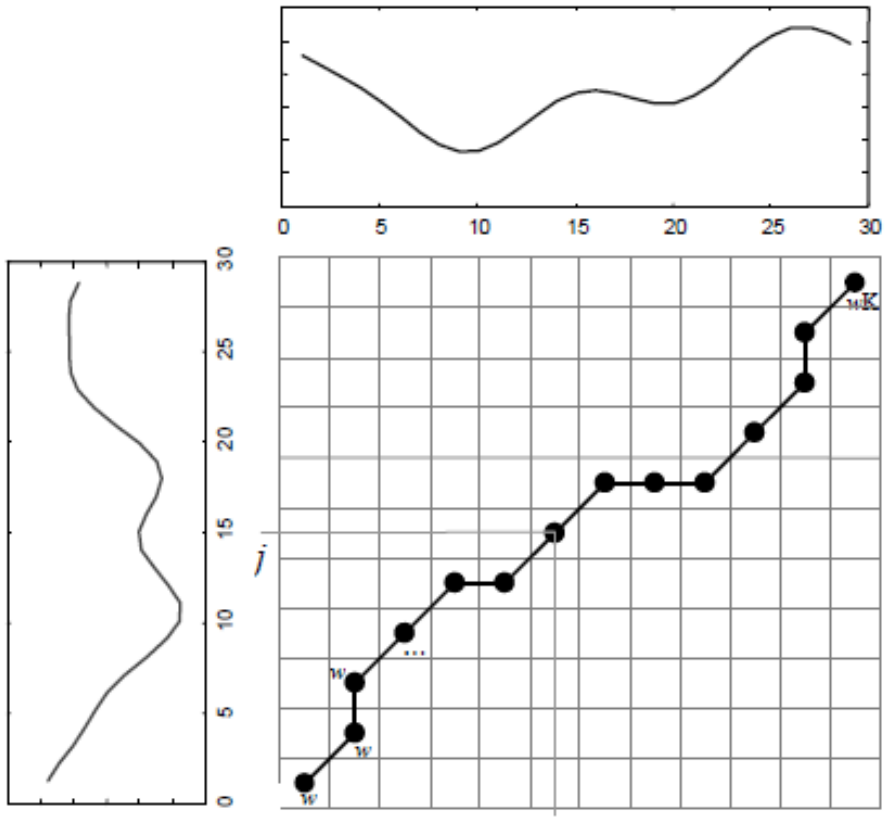

Figure 13: An example of the optimal path through the pairwise distance matrix of two time series [54].

4.2.2 Measures of Importance in Dynamic Event Tree Analysis

One current limitation of DETs is the assessment of results which is not as well developed as in traditional PRA [46, 55]. A concept that is used in PRA to assess the significance of a basic event is the concept of Importance Measures (IMs). In traditional PRA, IMs only consider the probability of occurrence and non-occurrence of a basic event. The application of importance measures to DETs must take into consideration not only the occurrence and non-occurrence of an event but also uncertain timing and/or severity.

A general platform for calculating Dynamic Importance (DYI) measures was developed with three general measures implemented in ADAPT at the time of publication. The measures account for the change in progression of the DET resulting from the different values of each uncertain variable under investigation. These measures facilitate comparison of the impact of any branching condition on a consequence of interest, allowing DETs to be used in prioritizing risk studies or plant investments.

DYI1 is described in Equation 3 and gives the ratio of expected consequences of occurrence of an event ($R(x=1)$) to the consequences of non-occurrence ($R(x=0)$). When used with DYIs, $R(x=1)$ refers to the weighted-average consequence measure of all branches where the event occurs. $R(x=0)$ refers to the weighted-average consequences of all branches where the event does not occur. DYI1 is valid as long as an aleatory bifurcation occurs and is still applicable when a further epistemic branching occurs. For example, branching may occur on whether a pump starts or not. If it does start, further branching determines its level of performance. The consequences for all sequences where the pump starts are averaged for $R(x=1)$ for DYI1. DYI1 yields a single value for each branching condition by which branching conditions may be compared for their impact on the consequence of interest.

$$DYI1 = \frac{R(x=1)}{R(x=0)} \tag{3}$$

DYI2 and DYI3 do not provide single values. Rather, they provide a distribution of the importance with values at each sampled epistemic value of the parameter being studied. DYI2 is described in Equation 4 where $x = 1_i$ denotes the parameter value being used to calculate the measure. DYI2 gives the ratio of consequences of each uncertain value of occurrence to the consequences of non-occurrence of the event. This measure is valid as long as an aleatory bifurcation occurs and is still applicable when a further epistemic branching occurs. A DYI2 comparison may be helpful, for example, in cases where attempts to reduce the likelihood of an event occurring increase the severity if it does occur.

$$DYI2(i) = \frac{R(x=1_i)}{R(x=0)} \tag{4}$$

DYI3 is applicable even when an aleatory bifurcation does not occur. This is particularly helpful in cases where material properties are sampled for their uncertainty, for example to account for aging. In these cases a branching condition is often used to explore the effects of the epistemic uncertainty in the value of the parameter. DYI3 is described in Equation 5 and gives the ratio of consequences of each uncertain value of the parameter to the expected consequences across all values of the parameter. DYI3 also yields a distribution which may be later manipulated if a single value is desired. The distribution may be used, for example, to compare the importance to radioactive releases of aging effects in steam generator tubes versus in primary steam lines. It may also be used to compare events that are difficult to prevent entirely but may be partially mitigated.

$$DYI3(i) = \frac{R(x=1_i)}{R(x=1)} \tag{5}$$

References

[1] J. T. Michalski and F. J. Wyant, "Secure Network Design," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-7117, June 2012.

[2] "Infection of the Davis Besse Nuclear Power Plant by the "Slammer" Worm Computer Virus - Follow-up Questions," United States Nuclear Regulatory Commission, ML032970134, October 2003.

[3] "Transcript of the Advisory Committee on Reactor Safeguards AP1000 Reactor Subcommittee Open Session on December 15, 2010," United States Nuclear Regulatory Commission, ML110140366, December 2010.

[4] J. Cardoni, M. Denman, and T. Wheeler, "Severe Accident Modeling for Cyber Scenarios," in *Transactions of the American Nuclear Society*, vol. 115, no. SAND2016-7735C. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 837–840.

[5] "Oconee Nuclear Station Units 1, 2, and 3, Issuance of Amendments regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protection System Digital Upgrade," United States Nuclear Regulatory Commission, ML100220016, 2010.

[6] "Evaluation of the Proposed Change: License Amendment Request 11-07 Process Protection System Replacement," United States Nuclear Regulatory Commission, ML11307A332, 2011.

[7] M. Denman, P. Turner, R. Williams, J. Cardoni, and T. Wheeler, "Preliminary Cyber-Informed Dynamic Branch Conditions for Analysis with the Dynamic Simplified Cyber MELCOR Model," in *Transactions of the American Nuclear Society*, vol. 115. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 787–790.

[8] A. Hakobyan, T. Aldemir, R. Denning, S. Dunagan, D. Kunsman, B. Rutt, and U. Catalyurek, "Dynamic Generation of Accident Progression Event Trees," *Nuclear Engineering and Design*, vol. 238, no. 12, pp. 3457–3467, Dec 2008.

[9] A. D. Williams, D. Osborn, K. A. Jones, E. A. Kalinina, B. Cohn, M. J. Parks, E. Parks, B. Jeantete, M. A. Thomas, and A. H. Mohagheghi, "Intermediate Results from a System-Theoretic Framework for Mitigating Complex Risks in International Transport of Spent Nuclear Fuel," in *Proceedings of the 58th Annual Meeting of the Institute of Nuclear Materials Management*, Indian Wells, CA, July 2017.

[10] L. Humphries, R. Cole, D. Louie, V. Figueroa, and M. Young, "MELCOR Computer Code Manuals - Vol. 1: Primer and User's Guide - Version 2.1.6840 2015," Sandia National Laboratories, Albuquerque, NM, SAND2015-6691R, 2015.

[11] "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, DC, NUREG-1150, 1990.

[12] N. S. Martin, M. R. Denman, and T. A. Wheeler, "Pruning of Discrete Dynamic Event Trees Using Density Peaks and Dynamic Time Warping," in *Transactions of the American Nuclear Society*, vol. 115. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 783–786.

[13] Z. Jankovsky, M. Denman, and T. Aldemir, "Extension of the ADAPT Framework for Multiple Simulators," in *Transactions of the American Nuclear Society*, vol. 115. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 557–560.

[14] Z. Jankovsky, M. Denman, and T. Aldemir, "Conditional Tree Reduction in the ADAPT Framework," in *Transactions of the American Nuclear Society*, vol. 115. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 553–556.

[15] Z. Jankovsky, M. Denman, and T. Aldemir, "Dynamic Importance Measures in the ADAPT Framework," in *Transactions of the American Nuclear Society*, vol. 115. Las Vegas, NV: American Nuclear Society, Nov 2016, pp. 799–802.

[16] Z. Jankovsky, M. Denman, and T. Aldemir, "A Dynamic Assessment of Auxiliary Building Contamination and Failure due to a Cyber-Induced Interfacing System Loss of Coolant Accident," in *International Conference on Topical Issues in Nuclear Installation Safety: Safety Demonstration of Advanced Water Cooled Nuclear Power Plants*, Vienna, Austria, June 2017.

[17] P. Lobner, C. Donahoe, and C. Cavallin, "Overview and Comparison of U.S. Commercial Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5640, September 1990.

[18] T. Aldemir, M. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. Mangan, D. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, and S. Arndt, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-6942, 2007.

[19] "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," IEEE Power and Energy Society, IEEE Std 7-4.3.2-2016, January 2016.

[20] D. Hintz, "Kewaunee Nuclear Power Plant - Documents Requested Prior to Appendix R Inspection," United States Nuclear Regulatory Commission, ML111751260, April 1987.

[21] G. Warnick, "River Bend Station - NRC Special Inspection Report 05000458/2016009," United States Nuclear Regulatory Commission, ML16133A174, May 2016.

[22] "Pressurized Water Reactor (PWR) Systems," in *Reactor Concepts Manual*. United States Nuclear Regulatory Commission Technical Training Center, ch. 4.

[23] "Intersystem LOCA Outside Containment," United States Nuclear Regulatory Commission, Information Notice 92-36, May 1992.

[24] "Inter-System Discharge of Reactor Coolant," United States Nuclear Regulatory Commission, Information Notice 90-05, January 1990.

[25] "Nuclear Plant Staff Working Hours," United States Nuclear Regulatory Commission, Information Notice 91-36, June 1991.

[26] G. Bozoki, P. Kohut, and R. Fitzpatrick, "Interfacing Systems LOCA: Pressurized Water Reactors," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5102, February 1989.

[27] A. Guler, J. Hur, Z. Jankovsky, H. Sezen, T. Aldemir, and R. Denning, "A Dynamic Treatment of Common Cause Failure in Seismic Events," in *Proceedings of the 2016 International Congress on Advances in Nuclear Power Plants*, San Francisco, CA, April 2016.

[28] D. Kelly, J. Auflick, and L. Haney, "Assessment of ISLOCA Risk-Methodology and Application to a Westinghouse Four-Loop Ice Condenser Plant," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5744, Apr 1992.

[29] D. Kelly, J. Auflick, and L. Haney, "Assessment of ISLOCA Risk-Methodology and Application to a Combustion Engineering Plant," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-5745, Apr 1992.

[30] J. Hewitt, E. Burns, T. Mairs, and K. Mohammadi, "ISLOCA Prevention and Mitigation Measures," Nuclear Safety Analysis Center, Palo Alto, CA, NSAC-167, September 1991.

[31] "State-of-the-Art Reactor Consequence Analyses Project Volume 2: Surry Integrated Analysis," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-7110 Vol. 2, August 2013.

[32] "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide," United States Nuclear Regulatory Commission, NEI 12-06 Rev 1, ML15244B006, October 2015.

[33] Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, "Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," Washington, DC, January 2013.

[34] "Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities," United States Nuclear Regulatory Commission, Washington, DC, RG 5.71, January 2010.

[35] C. Chenoweth, J. Green, T. Shaw, M. Shinn, G. Simonds, and J. Pezeshki, "The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-7141, November 2014.

[36] T. Aldemir, D. Miller, M. Stovsky, J. Kirschenbaum, P. Bucci, A. Fentiman, and L. Mangan, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-6901, 2006.

[37] T. Chu, G. Martinez-Guridi, M. Yue, J. Lehner, and P. Samanta, "Traditional Probabilistic Risk Assessment Methods for Digital Systems," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-6962, 2008.

[38] T. Chu, M. Yue, G. Martinez-Guridi, K. Mernick, J. Lehner, and A. Kuritzky, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods," United States Nuclear Regulatory Commission, Washington, DC, NUREG/CR-6997, 2009.

[39] "Analysis of Three Mile Island - Unit 2 Accident," Nuclear Safety Analysis Center, Palo Alto, CA, NSAC-80-1, March 1980.

[40] G. Wyss, J. Clem, J. Darby, K. Dunphy-Guzman, J. Hinton, and K. Mitchiner, "A Method for Risk-Informed Management of Enterprise Security (RIMES)," Sandia National Laboratories, SAND2013-9218P, October 2013.

[41] U. Catalyurek, B. Rutt, K. Metzroth, A. Hakobyan, T. Aldemir, R. Denning, S. Dunagan, and D. Kunsman, "Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees," *Reliability Engineering & System Safety*, vol. 95, no. 3, pp. 278–294, Mar 2010.

[42] K. Vierow, K. Hogan, K. Metzroth, and T. Aldemir, "Application of Dynamic Probabilistic Risk Assessment Techniques for Uncertainty Quantification in Generation IV Reactors," *Progress in Nuclear Energy*, vol. 77, pp. 320–328, Nov 2014.

[43] D. M. Osborn, T. Aldemir, R. Denning, and D. Mandelli, "Seamless Level 2/Level 3 Dynamic Probabilistic Risk Assessment Clustering," in *ANS PSA 2013 International Topical Meeting on Probabilistic Safety Assessment and Analysis*, Columbia, SC, Sep 2013.

[44] Z. K. Jankovsky and M. R. Denman, "Modification of the SAS4A Safety Analysis Code for Integration with the ADAPT Discrete Dynamic Event Tree Framework," Sandia National Laboratories, Albuquerque, NM, SAND2017-4764, May 2017.

[45] D. Wesley, "Interfacing Systems LOCA (ISLOCA) component pressure capacity methodology and typical plant results," *Nuclear Engineering and Design*, vol. 142, no. 2-3, pp. 209–224, August 1993.

[46] D. Helton, "Scoping Study on Advancing Modeling Techniques for Level 2/3 PRA," U.S. Nuclear Regulatory Commission, ML091320447, May 2009.

[47] Y. Chang and A. Mosleh, "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents, Part 1: Overview of the IDAC Model," *Reliability Engineering & System Safety*, vol. 92, no. 8, pp. 997–1013, July 2007.

[48] M. Kloos and J. Peschke, "MCDET: A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach," *Nuclear Science and Engineering*, vol. 153, no. 2, pp. 137–156, 2006.

[49] R. Winningham, K. Metzroth, T. Aldemir, and R. Denning, "Passive Heat Removal System Recovery following an Aircraft Crash using Dynamic Event Tree Analysis," in *Transactions of the American Nuclear Society*, vol. 100, 2009, pp. 461–462.

[50] V. Rychkov and K. Kawahara, "ADAPT-MAAP4 Coupling for a Dynamic Event Tree Study," in *ANS PSA 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis*, Sun Valley, ID, April 2015.

[51] F. Esposito, D. Malerba, G. Semeraro, and J. Kay, "A comparative analysis of methods for pruning decision trees," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 5, pp. 476–491, May 1997.

[52] A. Rodriguez and A. Laio, "Clustering by Fast Search and Find of Density Peaks," *Science*, vol. 344, pp. 1492–1496, 2014.

[53] N. Begum, L. Ulanova, J. Wang, and E. Keogh, "Accelerating Dynamic Time Warping Clustering with a Novel Admissible Pruning Strategy," in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Sydney, Australia, 2015, pp. 49–58.

[54] E. J. Keogh and M. J. Pazzani, *Principles of Data Mining and Knowledge Discovery: Third European Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 1–11.

[55] M. van der Borst and H. Schoonakker, "An Overview of PSA Importance Measures," *Reliability Engineering & System Safety*, vol. 72, no. 3, pp. 241–245, June 2001.

DISTRIBUTION:

1	MS	0748	Timothy Wheeler, 8851
1	MS	0748	Mitch McCrory, 8851
1	MS	0748	Matthew Denman, 8851
1	MS	0748	Zachary Jankovsky, 8851
1	MS	0757	R.A. Williams, 6613
1	MS	0829	Nevin Martin, 9436
1	MS	0899	Technical Library, 9536 (electronic copy)


Sandia National Laboratories