Requirements for a Computer Code System for the Development and Maintenance of Target Sets

A Thesis Presented for the
Master of Science
Degree
The University of Tennessee, Knoxville

Christopher Chwasz
August 2015

Copyright © 2015 by Christopher Chwasz
All rights reserved.

Dedication

I’d like to dedicate this work to my wife Jade and two daughters, Adah and Isla.

Acknowledgements

I'd like to thank the following people in the preparation of this Thesis:

My Advisor: Dr. Steven Skutnik, for agreeing to be my advisor and helping me navigate the process every step of the way.

My Graduate Committee: Dr. Howard Hall and Dr. Jamie Coble, for providing their insight into the preparation of this document.

Mr. Jalal Zamanali, for his support and expertise in the world of PRA.

Lastly, I'd like to thank my wonderful wife Jade, who has been my partner in pursuit of this goal day in and out over the last several years.

Thank you.

Abstract

In the field of commercial nuclear reactor security, the concept of target sets has matured since its invention in the late 1980s and early 1990s to the codification of target set regulations by the United States Nuclear Regulatory Commission in 2009 and publishing of official guidance in 2010. Target sets have evolved into a complex and useful tool to develop and test a protective strategy. By their definition, target sets are the "minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage" and are strongly related to probabilistic risk assessment. Though current guidance encourages the use of probabilistic risk assessment to inform the development of target sets, there exist no tools to assist in developing the hundreds of thousands of equipment combinations that meet the definition of target sets.

This report seeks to outline the requirements for a computer code system that would use a probabilistic risk assessment to provide the backbone for the development and maintenance of target sets for a commercial nuclear reactor or other complex facility.

Table of Contents

Chapter 1 Introduction 1
Background on Target Sets 1
Relationship of Target Sets to Probabilistic Risk Assessment 3
The Challenge of Target Sets 7
Chapter 2 Program Description 9
Target Set Development Process 9
Program Method of Use 11
Program Architecture 11
Target Set Basis Documents 12
Importing PRA Files 13
Target Set and Target Element Data Files 13
Challenge Frame 17
Validation and Review 19
Chapter 3 Method of Demonstration 20
Nuclear Power Facility Model 20
PRA Model of the SGNP 23
Chapter 4 Program Demonstration 30
Build Frame 30
Challenge Frame 40
Chapter 5 Conclusion 46
Bibliography 47
Appendix 49
Vita 74

List of Tables

Table 1: Data File Information Fields 14
Table 2: System Interdependencies 21
Table 3: Target Element #7.02 Data File after import 30
Table 4: Target Set #928 Data File after import 31
Table 5: SGNP Bibliographic Table 33
Table 6: Target Element #7.02 Data File with Complete Information Fields 34
Table 7: Target Set #928 Data File with Complete Information Fields 35
Table 8: Set Build List in with Complete Information Fields 35
Table 9: Target Element #9757.04 Data File 37
Table 10: Copy of Target Element #9757.04 Data File 38
Table 11: Target Set #201 Data File 39
Table 12: Target Set #9758 Data File (synonymous to TS 201) 40
Table 13: Mask 1 Data File 41
Table 14: Target Set List with Mask 1 applied 42
Table 15: Target Set #3666 Data File 43
Table 16: Mask 2 Data File 43
Table 17: Target Set 3666 with Mask 2 applied 44
Table 18: Target Set List with element 928.03 unavailable 45
Table 19: Element Build List after import from PRA data file 72
Table 21: Element Build List with Complete Information Fields 73

List of Figures

Figure 1: Selected PRA Cut Sets 25
Figure 2: SGNP P&ID 50
Figure 3: RCS-LBLOCA Event Tree 51
Figure 4: RCS-SBLOCA Event Tree 52
Figure 5: RX-TRIP Event Tree 53
Figure 6: SL-A-BREAK Event Tree 54
Figure 7: SL-B-BREAK Event Tree 55
Figure 8: Acc-A Fault Tree 56
Figure 9: ACC-B Fault Tree 57
Figure 10: EFWS-A Fault Tree 58
Figure 11: EFWS-B Fault Ttree 59
Figure 12: EFWS-A-SLB Fault Tree 60
Figure 13: EFWS-B-SLB Fault Tree 61
Figure 14: HHSI-A Fault Tree 62
Figure 15: HHSI-B Fault Tree 63
Figure 16: RHR-A Fault Tree 64
Figure 17: RHR-B Fault Tree 65
Figure 18: SD-ATM-A Fault Tree 66
Figure 19: SD-ATM-B Fault Tree 67
Figure 20: SD-CN-FW-A Fault Tree 68
Figure 21: SD-CN-FW-B Fault Tree 69
Figure 22: SL-A Fault Tree 70
Figure 23: SL-B Fault Tree 71

List of Acronyms

CAFTA	Computer Aided Fault Tree Analysis
CCW	Component Cooling Water System
CD	Core Damage
CFR	Code of Federal Regulations
CVCS	Chemical and Volume Control System
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater System
FOF	Force-On-Force
HHSI	High Head Safety Injection System
LBLOCA	Large Break Loss Of Coolant Accident
LOCA	Loss Of Coolant Accident
LOOP	Loss Of Offsite Power
MCR	Main Control Room
MSSS	Main Steam Supply System
NEI	Nuclear Energy Institute
NRC	US Nuclear Regulatory Commission
OSRE	Operational Safeguards Response Evaluation
P&ID	Piping and Instrumentation Diagram
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
RG	Nuclear Regulatory Commission Regulatory Guide
RHR	Residual Heat Removal System
RPS	Reactor Protection System
RSWS	Remote Shutdown Workstation
SAMG	Severe Accident Mitigation Guideline
SBLOCA	Small Break Loss Of Coolant Accident
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SGNP	Simplified Generic Nuclear Plant
SIS	Safety Injection System
SSCs	Systems Structures and Components
TSA	Target Set Analysis
WEC	Westinghouse Electric Company LLC

Chapter 1

Introduction

Background on Target Sets

The concept of Target Sets is based in the field of nuclear reactor facility security. The term was first used to describe the specific combination of equipment that would have to be made inoperable in order for an adversary to effect core damage. The current definition is found in the United States Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.81 "Target Set Identification and Development for Nuclear Power Reactors." RG 5.81 defines target sets as: "The minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., nonincipient, nonlocalized fuel melting and/or core destruction) or a loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations." The definition of and guidance on target sets took time to mature as the NRC staff focused efforts to review and update security regulations and guidance after the attacks of September 11, 2001.

Target sets were initially used as part of the NRC Operational Safeguards Response Evaluation (OSRE) Program conducted during the 1990s at licensed United States (US) commercial nuclear reactor facilities through 2001. In the OSRE program, the NRC requested licensees submit to Force-On-Force (FOF) exercises to test the effectiveness of a licensee's protective strategy. Target sets were used as an evaluation tool, providing the groups of targets that the mock adversarial force sought to destroy or compromise. For these evaluations, target set development guidance to licensees was unsubstantial, but was sufficient for the optional FOF exercises and accompanying evaluations at that time.

After the events of September 11, 2001, the NRC issued NRC Security Order EA-02-026 "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants," in 2002 and EA-03-086, "Design Basis Threat for Radiological Sabotage," in

2003 to licensees to increase security precautions at reactor facilities. The security orders dictated that FOF exercises be conducted at each commercial nuclear power plant at least once every three years, and required licensees to create and maintain target sets to inform the protective strategy and be used in the FOF program. The NRC did not issue guidance on target sets, and licensees instead used industry-developed guidance that was intended primarily for FOF exercises, that being Nuclear Energy Institute (NEI) 03-11, "Guidance for the Preparation and Conduct of Force-on-Force Exercises." In 2006, the NRC Staff planned a large power reactor security rulemaking (that included target sets), but in 2007 NRC Commissioners instructed the Staff to terminate the rulemaking and instead develop guidance for target sets. Preliminary work was conducted and guidance was given to new reactor applicants in September 2009. Target sets were planned to be included in a future rulemaking to update to Title 10 Part 73 Section 55, "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage," (10 CFR 73.55).

Security orders EA-02-026 and EA-03-086 were included in new and updated security regulations and guidance to licensees though the update of 10 CFR 73.55 on March 27, 2009. A part of this update, in subsection (f), is the first codification of target sets for a commercial nuclear reactor facility. Initial guidance to meet the requirements for target sets was published in RG 5.76, "Physical Protection Programs at Nuclear Power Reactors" in July 2009, but was limited in scope and detail. Expanded NRC guidance on meeting the new target set requirements was not published until November 2010, when the NRC staff issued RG 5.81.

RG 5.81 expanded greatly on what was previously available, providing more detail on documentation and thoroughness, especially concerning operator actions, plant operation modes, cyber-attacks and flooding and fire impacts. Though not determined to be an increase in regulatory scope, RG 5.81 outlined an expanded view of NRC staff expectations on meeting the new Target Set requirements in 10 CFR 73.55 published in 2009. RG 5.81 stressed the traceability of a target set's origin, to understand the original

safety basis and analysis for the inclusion of components and operator actions within the target sets.

Relationship of Target Sets to Probabilistic Risk Assessment

RG 5.81 stresses the use of site safety basis documents in developing target sets, specifically the usefulness of using a site's Probabilistic Risk Assessment (PRA). A PRA is a thoroughly developed and vetted tool that captures most of the equipment failure combinations that lead to core damage. The equipment combinations found in the PRA have an overlap with those found in target sets, and thus the PRA can be considered a natural starting point in developing target sets. There exist key differences between PRAs and target sets in the treatment and representation of several factors that must be considered when using a PRA to create target sets. PRAs and target sets differ on: initiating events, failure probabilities, component failure modes, inclusion of passive components, operator actions, non-safety related components, mitigating systems, flooding, fire, and cyber security.

PRA uses initiating events as the starting point for events that challenge the safety of the plant. These initiating events require the use of safety systems to return the reactor to a safe condition. Examples of PRA initiating events are: loss of coolant accident (LOCA), loss of offsite power (LOOP), and reactor protection system (RPS) trip. Initiating events in the PRA begin the challenge to the plant, and thus occur first chronologically. Target sets do not use an initiating event per se, in that the destruction or compromise of target elements does not need to occur in any specific order, and thus no target is necessarily "first," but one target element of each set must challenge the safety of the plant if the adversary wishes to cause core damage.

A PRA is composed of event trees that begin with initiating events. The event trees contain markers for systems whose failure or success determines the state of the reactor. Figure 3 through Figure 7 (in the appendix) show examples of event trees for several initiating events. The systems contained in the event trees are then modeled in individual fault trees, to represent the failure modes of the system with individual

components. Figure 8 through Figure 23 (in the appendix) show examples of the fault trees associated with the systems represented in the event trees of Figure 3 through Figure 7. Each different component failure combination, starting with an initiating event and including components from each applicable fault tree, is represented by a cutset. Each component in the fault trees has associated failure probabilities, and these probabilities are summed to give a failure probability for each cutset. In this way, PRA can determine those pieces of equipment that provide the greatest contribution of risk to a system or reactor. Target sets do not use failure probabilities, and instead assume that if an adversary reaches a target with the time and capability to compromise or destroy that target, then the target is compromised or lost. Target sets should consider if targets are "achievable," that the adversary is capable of compromising or destroying the target. For example, if the target is a 24" steel reinforced concrete wall, and the adversary is equipped with a manual chisel, the target could be declared "unachievable" and justified with an analysis on the time required to defeat the wall. Adversary characteristics are detailed in RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements."

PRAs will analyze different failure modes for components within fault trees. For example, a pump could fail by having a seal fail, having an incomplete electrical connection within the motor housing, or having a bearing failure. These different failure modes are often included separately within a PRA, as the different failure modes have different failure probabilities that contribute to the failure probability of the pump. Target sets do not consider different failure modes, as after the adversary reaches a target element, many different failures options exist, and thus an adversary reaching a target element is considered bounding. Target sets should consider different compromise states of components, as an adversary could cause a system to work against the safety of the plant (for example, activing a pump to remove coolant water from the reactor coolant system and dump it outside the building).

Internal event PRAs analyze the failure probability associated with random failures of active Systems, Structures, and Components (SSCs) (pumps, valves, etc…) within the site itself, and external event PRAs consider the effect of external events (winds, seismic events, external flooding) on SSCs within the plant. The internal events PRA usually does not consider the random failure of passive components (pipes, tanks, and flood and fire barriers). External events PRAs do include many of these passive components (as their failure is considered under the effect of specific conditions). Target sets fully include, with equal weight, passive components, as an adversary could attack passive or active component to the same effect.

A PRA will consider operator actions as events in a fault tree with human reliability of making mistakes or forgetting intentional actions in mind. Target sets also consider operator actions, but require that they meet six criteria set forth in RG 5.81 section 6.4 in order to be credited in target sets: "(1) sufficient time is available to implement these actions, (2) environmental conditions allow access where needed, (3) adversary interference is precluded, (4) any equipment needed to complete these actions is available and ready for use, (5) approved procedures exist which have entering conditions outside of severe accident mitigation guidelines (SAMG) or equivalent, and (6) training is conducted on the existing procedures under conditions similar to the scenario assumed." Target sets require greater guarantees on the completion of operator actions as random failures/mistakes are not taken into account. Operator actions are considered target elements, and the equipment, operator, or environment for the action could all be determined to be separate targets associated with one operator action.

A PRA is primarily composed of safety-related pieces of equipment, but can include non-safety related pieces of equipment if they are deemed risk significant. Similarly, target sets are primarily composed of safety-related equipment, but can also include non-safety related equipment. SSCs, such as extra purpose-positioned pumps, hose, and water sources for emergency makeup water addition to the reactor could be included within target sets.

A level 2 PRA addresses the probability, size and timing of offsite releases following core damage. Those SSCs that are included within the level 2 PRA are those that would limit or mitigate damage and release, including the containment structure, valves, filters, and environmental control systems. Target sets focus on SSCs that lead to significant core damage or spent fuel sabotage, and do not consider containment or mitigating systems.

The internal and external event PRAs consider the effect of flooding on plant safety systems. For internal events, flooding from active and traditional sources (pumps, LOCAs, etc.) is considered with the expected performance of interior flood barriers. External event PRAs consider expected external flooding based on the flooding history of the surrounding area. Target sets should consider interior or exterior flooding from a multitude of sources. As adversaries can defeat flood barriers and cause flooding in previously unanalyzed areas, target sets should consider flooding/water damage far beyond what is found in the PRA.

A fire PRA may be conducted (consistent with National Fire Protection Association (NFPA) 805) for internal or external events. Similar to flooding, a fire PRA would consider only traditional fire ignition sources with the expected performance of fire barriers. Target sets should consider the effects of fire beyond the PRA, as an adversary could cause a fire where accessible and use incendiary devices and flammable materials to propagate the fire across fire barriers.

PRAs analyze random failures of SSCs and operators, and not malicious actions, thus cyber-attacks are not considered in PRA. Target sets must consider cyber-attacks on any component susceptible to such an attack, consistent with 10 CFR 73.54, "Protection of digital computer and communication systems and networks" and RG 5.71, "Cyber Security Programs for Nuclear Facilities."

A site's PRA provides many of the different equipment and component combinations found as the result of target set development, but several key differences do not allow the direct translation from PRA cut-sets to target sets. These differences require that PRA and target sets exist as separate tools produced through separate

methods, but allow the use of PRA (in addition to other documents and analyses) to inform target sets.

The Challenge of Target Sets

Though the new regulation in 2009 was a codification of previous Security Orders, and by definition, Regulatory Guides are not requirements (they are the NRC staff's example of an acceptable method to meet regulation), the new regulations in 10 CFR 73.55(f) and issue of RG 5.81 communicate from the Staff that in order to meet regulation, a large effort from licensees is required to develop and maintain their target sets.

10 CFR 73.55(f) requires that licensees: document and maintain the process to develop and identify target sets; consider cyber security in target sets; document those target set elements that are not located within a protected or vital area; and that changes to the plant are considered in target sets and accounted for in the protective strategy. These requirements are challenging for licensees to meet due to the voluminous and complex nature of nuclear plant safety analyses. Development and management of target sets is done largely by hand using word processing and spreadsheet software. Each change to the target sets must be manually entered and updated throughout the documentation. Updating target sets to reflect site conditions or changes is open to delay, error, or accidental omission due to the onerous nature of updating every document. Though NRC and industry guidance exists, execution of target set development is left to the licensee with limited review, possibly exposing the target sets to accidental omission, errors, or obfuscation of data. There are no computer programs specifically designed for target sets, and target sets differ from PRA enough such that current PRA codes have only limited usefulness for target sets.

This report will outline the requirements for a computer code system (computer program) for the development and maintenance of target sets. The proposed program would allow the populating and updating of target set data with commonly used nuclear industry safety data codes, provide a step by step process for users to add to and enrich entered data, provide multiple standard and user generated grouping and sorting options

for users to identify certain aspects of the target sets, and provide several report generating and data output paths. This program would have applicability to US and international commercial, research and government reactor and nuclear facilities. Additionally, this program would apply to any complex facility or system that requires protection from sabotage and uses a fault-tree program. The goal of the program would be to reduce costs associated with target set development and maintenance while providing a more accurate and insightful product for use in developing a facility's protective strategy.

Chapter 2

Program Description

The primary purpose of the program is to guide users to use information that is already available as a part of their licensing basis to populate target set data within a database to allow easy editing, sorting and grouping. The program would be a tool to be used in the development of target sets. The program will populate target set data originally from PRA software, such as SAPHIRE and CAFTA cut set data sheets. Additional information will need to be entered manually from other data sources (e.g. safe shutdown list) either for each individual component or by a grouped set of components. By using results and analyses from previously reviewed and verified safety analyses to form the target sets, the most accurate and thorough representation of the reactor systems can be used to inform the protective strategy. After the population of several different component parameters (component type, location, system, etc…), sorting and grouping of the target set components would be accomplished by several standard and user-defined options. The program will have the ability to mark some target elements (through the sorting and filtering options) as unavailable, to represent systems, trains or equipment in maintenance, outage, or under special circumstance, and the updated target sets that result from the change. The program would have several standard and custom user generated reports for printing or exportation. The program is intended as a unique tool to use in the development and continued maintenance of target sets.

Target Set Development Process

Outlined in RG 5.81, the target set development process seeks to provide steps for the identification and development of target sets: 1. Establish Target Set Analysis Team, 2. Determine Objectives, 3. Identify Target Elements, 4. Generate Target Sets, and 5. Screen for Achievable Targets.

Step 1 of the target set analysis (TSA) process is to form a team of individuals knowledgeable in: reactor engineering, plant systems and design, plant operations, structural design, PRA, physical security, cyber security, and maintenance. Team

expertise in these areas would provide the individual knowledge and experience to inform the development of target sets.

Step 2 of the TSA is to determine the objective of the analysis. For a nuclear power plant, prevention of significant core damage or spent fuel sabotage are the primary objectives. Lesser objectives could include redundant safety system availability, or mitigating and containment system availability (though not required for TSA).

Step 3 of the TSA process is identification of target elements. Target elements can be determined from examination of existing safety-related equipment lists and system descriptions. Equipment in the PRA would also likely be included as target elements. The goal of target element identification is to include in the TSA those SSCs that have a safety basis or purpose to the plant. The inclusion in target sets of non-safety related SSCs provides a greater safety defense-in-depth against adversary attack.

Step 4 of the TSA process is target set generation, the identification of equipment combinations that lead to core damage. A PRA could provide many of the equipment combinations required for target sets, but additional SSCs, operator actions, and combinations would be required beyond the PRA to accomplish this step.

Step 5 of the TSA is to screen the target sets for achievable targets. Some targets may be beyond the capabilities of the adversary, and thus need not be included for consideration in target sets. The characteristics of the adversary are found in RG 5.69.

The intention of the proposed computer program would be to assist in steps 3 and 4 by using PRA to populate the target elements and SSC combinations in target sets. Consistent with step 3 and 4, additional information from many additional sources is required to be entered by the user to complete the target sets. The computer program would provide a large basis via the importation of PRA data, and flexible framework to continue development of target sets with the inclusion of other user-entered data such as: equipment types, locations, systems, flood, fire and cyber-attack susceptibility, and additional SSCs not found in the PRA. The computer program would provide the proper functionality and reporting options required by target set development and maintenance and not offered in other existing programs.

Program Method of Use

The program is designed to be used within the TSA framework given in RG 5.81. Documentation that accompanies the program would provide a step-by-step process on the use of the program to develop and update target sets. The process for the creation of new target sets in the program is shown below:

1. Acquire Basis Documents
2. Import cut sets from PRA data file
3. Complete target element and target set data
4. Add or delete target elements and target sets
5. Group/mask target elements
6. Create challenge scenarios
7. Review of target set development
8. Report target set insights

The attributes of each step will be described in the following sections, and examples are given in Chapter 4 of this document.

Program Architecture

The program will be a database with a graphical user interface. The program will be password protected with encrypted data files for additional security, and will be designed to be used on a stand-alone machine or network in accordance with regulations on the protection of Safeguards Information and National Security Information. The program will have the ability to have several user profiles that access only the program data permitted to each user (data sharing between profiles will be non-simultaneous, and will be allowed though mutual authentication with the ability to revoke). By default, user profiles will be fully accessible only by the owner of the user profile and the program administrator. The program will log all access, files exported or printed, and changes for lengths of time determined by the administrator. The program will use temporary files

while open, and auto-save to the original files at predesignated points or at user request (to prevent corruption of the saved data should a fault or error occur).

The program will have two "frames." The "build frame" is where the user will build and modify the target sets and target elements (target sets are comprised of target elements). The "challenge frame" is where the user can build scenarios that challenge the plant. In the "challenge frame," no permanent editing or changes to the target sets or target elements will be possible, but challenge scenarios could be designed and saved, and would automatically update when the data is edited and saved in the "build frame." The system administrator or data owner will decide if users will have access to the "build frame," "challenge frame," or both.

Target Set Basis Documents

Though the program is built around using cut sets from a PRA program, additional information is required to populate the information fields in the data files and add target elements and sets that are not represented in the site's PRA. The program would provide specific guidance to documents and tables that should be included in the development of target sets. RG 5.81 provides guidance on the types of documents and tables that the NRC Staff would expect to be reviewed and used in the development of target sets (this information is not given here as some is deemed Official Use Only – Security Related Information). To facilitate the use of these documents, the program would provide a Bibliography Table feature that would allow the entry of document names, tables, and figures that possess the information referenced for the creation of target sets. Additionally, under each bibliographic entry, a separate field would be available to enter what information was excluded and an explanation to the omission. This function exists to provide transparency and traceability to the target set development process, so the disposition of systems, structures, and components deemed important in the facility safety analysis can be determined for the development of target sets.

Importing PRA Files

In the "build frame," the program will give the option to import a document of PRA cut sets in either the SAPHIRE or CAFTA format, as these are the codes primarily used in the commercial nuclear industry. The capability will exist to add additional PRA formats at a later time to encompass other risk assessment software. After the user selects the PRA program file for import, the program will automatically begin populating target set and target element data files in the database with each cut set and cut set component. Each cut set, upon transformation to a target set, would have a unique identification number assigned. Each target element derived from cut sets would be automatically assigned a unique ID number and name (derived from cut set component name). Duplicate cut sets will be ignored, and only unique cut sets will be captured as target sets. Duplicate target element entries will also be ignored except for logging their associated cut sets. The result of importing the PRA cut sets is to capture those relationships and form preliminary target sets.

The program will also have the capability to update with a new import of a PRA cut set document in the same way the initial data import function occurred, by checking and ignoring duplicates. In this way, updates to a site's PRA could be reflected within the site's target sets via an automatic process.

Target Set and Target Element Data Files

As the result of importing data from a PRA cut set data file, the program will have initial target set and target element data files populated. The target set data files will have: their identifying ID #, and the full set of target elements imported from the PRA cut set data file. The target elements will have: their identifying ID #; their identifying name; and the full list of target set ID#s to which that target element belongs. The target element and target set "ID#s" are unique identifiers assigned by the program upon creation of the data file.

In the "build frame," if no PRA cut set data file is imported, or there are additional target sets or target elements to add, the user can create a new target element

and enter all values manually. The user can then form target sets from the existing target elements.

Target element data files would contain the information fields listed in Table 1, column 1 and the target set data files would contain the information fields listed in Table 1, column 2. From the PRA import step, those fields that are underlined in Table 1 would be filled automatically. The remaining fields require that the user enter the data.

In the "build frame," the target elements can be displayed in the "Element Build List" and the target sets in the "Set Build List." The "Build Lists" could be filtered, sorted, and searched. The lists will have columns for attributes of target elements and target sets, and will be edited individually or in user selected groups. In this way, the data associated with many target elements and target sets will be able to be populated in a fast and efficient manner. The standard column headers for the target element and target set lists are located in **bold** in Table 1 column 1 and column 2 (respectively).

Table 1: Data File Information Fields

Target Element Data file	Target Set Data File
ID#	**ID#**
IDName	
Name	
Type	**# Elements**
Location	**# Locations**
Modes	**Modes**
Train	**Train(s)**
System	Systems
Cyber?	**Cyber?**
Flood?	**Flood?**
Fire?	**Fire?**
Operator?	**Operator?**
Target Sets	

Descriptions of the data file fields are:

- "IDName" field would be automatically be derived during import from cut set files, entered by the user, or edited by the user.
- "Type" field would be used to classify the type target element equipment, component or action with a standard library of terms (pipe, valve, switchgear, cable, etc…) or the option for user-defined terms. This information would be useful to users to understand what type of component is represented (as it may not be obvious given the name of the target element). The types listed will be links to the "Element Build List" with the list filtered to only those elements of the type selected.
- "# Elements" field would compile the number of target elements that comprise the target set. This information would be useful in sorting and filtering target sets. Providing the target sets with the fewest targets may provide a useful insight for the protective strategy.
- "Location" field would be user defined, but would identify the component location (room) within the site. The "# Locations" field would display the compiled number of distinct locations of target elements from that target set. Providing the target sets with the fewest locations may provide a useful insight for the protective strategy. The locations listed will be links to the "Element Build List" with the list filtered to only those elements contained within the location selected.
- "Mode" and "Modes" fields would list the modes of reactor operation that the target element and target set are applicable to. Target sets are required to represent all modes of operation. A specific reactor's modes of operation are defined in a site's Technical Specifications. Generic modes of operation, numbered 1-7 are as follows: Power Operation, Startup, Hot Standby, Cold Standby, Shutdown, Refueling, and Reduced Inventory Conditions. (RG 5.81)

- “Train” field would list the designated train that the target element belongs to. The “Train(s)” field would display the compiled trains associated with that target set. This information would be useful to understand the target sets when trains are taken out of service for maintenance. The trains listed will be links to the “Element Build List” with the list filtered to only those elements contained within the train selected.
- “System” field would list the associated system that the target element belongs to. The “Systems” field would display the compiled systems associated with that target set. This information would be useful to understand the target sets when systems are taken out of service for maintenance. The systems listed will be links to the “Element Build List” with the list filtered to only those elements contained within the system selected.
- The “Cyber?” field would indicate “Yes” or “No” if the target element is susceptible to a cyber-attack (consistent with the guidance in NRC RG 5.71, “Cyber Security Programs for Nuclear Facilities”). The “Cyber?” field for the target set data field would compile and display the fraction of target elements that are susceptible to a cyber-attack.
- The “Flood?” field would indicate “Yes” or “No” if the target element is susceptible to damage from flooding. The “Flood?” field for the target set data field would compile and display the fraction of target elements that are susceptible to flooding.
- The “Fire?” field would indicate “Yes” or “No” if the target element is susceptible to damage from fire. The “fire?” field for the target set data field would compile and display the fraction of target elements that are susceptible to fire.
- The “Operator?” field would indicate “Yes” or “No” if the target element or target set requires an operator action outside the main control room for its

success or “No”. For target sets, the “Operator?” field would sum the required operator actions of the target set.

- The “Target Set” field for the target element data file would list every target set ID# (as links to the target set data files) that the target element is contained within. The target sets listed would be links to the data file of the selected target set.

The program will have the capability of adding user-created and defined fields for the target elements and target set data files. These custom fields could also be added to the “Element Build List” and “Set Build List” for custom user-defined parameters for sorting.

The program will have a copy/paste window for target sets and target elements. Copied target sets and elements that are then pasted would have placeholder names and new ID#s, so that expansion of the target sets and target elements can occur based on selected existing data. For example, if a target set contained 5 elements, and the user wanted to make a new target set with 4 elements being the same and one new element, then the original set could be copied, the 5 elements would remain in the new target set while in the copy/paste window. The undesired element would then be removed, and a new target element would then be added. The target element list would then not be updated with the new 5^{th} element until the copied target set was “published,” and the copy/paste window exited.

The “build frame” would have standard reporting and printing options, using the “Element Build List” and “Set Build List” to filter, sort, and search those target elements and target sets for reports and printing. The intention of the “build frame” printing would be for target set development and maintenance purposes.

Challenge Frame

The “challenge frame” of the program is where the useful insights should be determined to inform the protective strategy. The intention of separating the “build

frame" from the "challenge frame" is multifaceted. First, the "challenge frame" would not allow users to edit the base data of the program. This would provide a safe space for users to design different scenarios of equipment availability without the worry of compromising the base data. Second, it provides for information compartmentalization. It may be that the users that build the target sets do not need to know the details on the Design Basis Threat and other threat characteristics that are used to challenge a plant. Third, the "challenge window" will have functionality that would impede the target set development. In the "challenge frame," filtering, grouping, and masking (replacing values with a placeholder) of elements could be saved. In the "build frame," filtering, sorting, and grouping would be for the session only, and also could be reset by the user during a session.

The "challenge frame" will have the ability for the user to filter, sort and mask data in order to derive useful conclusions from the data. The "Element Build List" and "Set Build List" are replaced with the "Target Element List" and the "Target Set List" and retain the bold columns from Table 20 (in the Appendix) as well as the capacity for custom user generated fields. The "Target Element List" and the "Target Set List" could be filtered and sorted, and the results saved so different scenarios could be modeled. In this way, the target sets could easily model scenarios like: having a train out of service; reactor in cold stand-by mode; refueling outage; or other planned maintenance. Target elements could also be masked to simplify the target sets. For example, all target elements in the control room could be masked as "control room" to act as a single target. The mask on the target elements would possess a data file like the target elements and target sets, and would display the same information as target elements with the addition of a list of all target elements it masks.

The "challenge frame" will have standard and custom user-generated reporting and printing options. The standard reports would detail information such as: the smallest target sets; the target sets with the fewest locations; the target sets with the largest cyber vulnerability (highest % of target elements that have cyber vulnerability); the target sets with the largest flood vulnerability; the target sets with the largest fire vulnerability; and

the target sets that rely on operator action outside the main control room. The user could also use the "Target Element List" and the "Target Set List" to develop and save custom reporting options.

Validation and Review

Initial validation of the computer code would be accomplished through the use of a prepared standard cutset data file and instructions for the user. The user would complete the example to test all of the code components, and the resulting target sets could then be compared against published results. The validation materials would include documentation on variations in the results, and likely sources for deviation from the correct results.

User, peer, and regulatory review of the target sets would be possible through the previously described reporting options (of individual or groups of target elements and target sets, or of all target set data). Review of the documents and comments contained within the program's Bibliographic Table would provide the basis for inclusion or exclusion of SSCs, which could then be traced to the target elements and target sets.

Chapter 3

Method of Demonstration

To illustrate the benefits of a program as described above, a small demonstration of the method can be performed without the large scope of producing the actual computer code program. To demonstrate the methods of the program, a PRA is required. For greater clarity, a PRA is constructed with simplified reactor systems and system interdependencies.

Nuclear Power Facility Model

For the reactor model, a Pressurized Power Reactor (PWR) is selected as they are the most numerous commercial reactor design used today. The design is roughly based on the Westinghouse Electric Company (WEC) four-loop PWR, however, the design is simplified such that creation of target sets does not approach a realistic representation of any former, current or future commercial nuclear reactor, nor would the information be useful to an adversary, and thus does not constitute information that should be withheld from public viewing. The model reactor is named the Simplified Generic Nuclear Plant (SGNP).

The SGNP reactor model is simplified from the Westinghouse four-coolant loop PWR to a two loop PWR with two safety trains. Using the system descriptions and diagrams in the WEC document, "The Westinghouse Pressurized Water Reactor Nuclear Power Plant," a piping and instrumentation diagram (P&ID) was created to represent the reactor facility. This P&ID can be found in the Appendix as Figure 2 and shows the primary coolant systems: the reactor coolant system (RCS), main steam supply system (MSSS), the emergency feedwater system (EFW), the high head safety injection (HHSI) system, and the residual heat removal (RHR) system.

The location of equipment is only specified to the building as a simplification from individually locked rooms on separate levels of a building. It is assumed that each building is separated by a locked flood and fire barrier.

Using the system descriptions, system interdependencies are determined and captured in Table 2. Basic representations of the support systems are modeled for the SGNP.

Table 2: System Interdependencies

System	Dependent Upon			
	EDGs	CCW	Service Water	Circulating Water
RCS	x	x		
RHR	x	x		
HHSI	x	x		
EDGs			x	
CCW	x		x	
EFW	x		x	
Service Water				x
Condensers				x

The primary coolant systems rely on the emergency diesel generators (EDGs), the component cooling water (CCW) system, the service water system, and the circulating water system. The system dependencies are simplified for ease of use (to one or two items), as actual nuclear power facilities have much greater redundancies and interdependent relationships between systems.

The chemical and volume control system (CVCS), which provides boration and can partially contribute makeup water, is not included in the model. Though the pressurizer is included in the P&ID, the pressurizer and the associated pressure operated relief valve are not modeled for reactor coolant inventory modeling simplification. As the CVCS cannot contribute water to the reactor coolant system at a rate to meet safety requirements for a LOCA, boration was not considered, and the pressurizer was not considered, the CVCS is determined to be unnecessary to model.

The power systems modeled are the EDGs, the switchyard, and offsite power. These components are selected to simplify target locations and electrical system

component and to demonstrate some simple system dependencies and redundancies for the electrical systems. Offsite power and EDGs are the primary load bearing safety electrical systems, and both route through the common switchyard. Switchgear, class 1E batteries, and non-safety electrical systems were not modeled, and this assumption does not pose any negative impact on the model. These components are omitted from the model as their locations are numerous and they also support separate trains and systems, which would complicate the reactor model.

The reactor protection system (RPS) (plant safety computer), instrumentation and control systems, and reactor reactivity systems (control rods and boration) are not modeled, but a successful control rod insertion is assumed when needed (consistent with reactivity control requirements). Though the RPS would likely be the primary target for a cyber-attack, plant instrumentation and control systems are too numerous to model for this example. It is assumed that a reactor trip initiates automatically or manually and successfully signals equipment to actuate.

Operator actions are not modeled for the PRA, but the possibility of operator action was left as an option with the manually controlled steam line A and B condenser and atmospheric dump valves.

Other plant systems that are not modeled, but were assumed to have no negative effects on plant performance were: containment isolation valves, heating ventilations and cooling systems (HVAC), containment spray systems, check valves, and the spent fuel pool and associated systems. Containment isolation, HVAC, and containment spray systems are omitted as these systems are typically excluded from target set analysis, and thus would provide little benefit for this demonstration. Check valves are excluded for simplicity of the model design. The spent fuel pool is not considered as the complexities of the reactor systems provide a better example for the demonstration of the program methods.

The reactor modeled is assumed to be at full power operation, with no equipment out of service. Though other reactor modes can rely on fewer pieces of equipment to

cool the reactor, full-power operation is chosen as it challenges more systems of the plant for the demonstration.

PRA Model of the SGNP

From the Figure 2 P&ID found in the appendix, system dependencies in Table 2, and system descriptions found in WEC documentation, the initiating events, event trees and fault trees for the PRA are formed for the SGNP using the SAPHIRE 7 PRA code.

Five initiating events are explored for the SGNP: steam line break in loop A (SL-A-Break), steam line break in loop B (SL-B-Break), RPS trip (RPS-TRIP), small break loss of coolant accident (SBLOCA) in the RCS (reactor coolant system) (RCS-SBLOCA), and large break loss of coolant accident (LBLOCA) in the RCS (RCS-LBLOCA). These initiating events represent common challenges to the reactor operation that pose significant challenges.

The SL-A-Break and SL-B-Break initiating events are similar but occur in opposite secondary cooling loops between the steam generators and turbines. These initiating events challenge the plant by the loss of secondary coolant loop inventory, and thus there is greater reliance on the opposing secondary cooling loop or shutdown and cooling systems.

The RPS-TRIP event represented the actuation of shutdown systems of the reactor. The RPS-TRIP initiating event challenges the ability to remove heat from the primary coolant loop through the use the secondary coolant systems, and not through the injection of cool water from the safety injection systems. The RPS-TRIP event was assumed to be bounding for LOOP, turbine trip, and reactor coolant pump trip, as they would result in a RPS-initiated trip. LOOP and loss of steam loop functionality are found within the fault trees of the events of the RPS-TRIP initiating event.

The RCS-SBLOCA initiating event challenges the plant to cool the reactor with at least one safety injection system. The RCS-LBLOCA initiating event challenges the plant to cool the reactor with the minimum of at least one accumulator and one high-head safety injection system. The LOCA initiating events are standard events that challenge

the plant to cool the reactor by keeping enough cool water to flow through the reactor by the use of the safety injection and RHR systems.

For each initiating event, event trees were created that represented the major coolant systems required to function in response to each initiating event. The results of reactor "OK" status and core damage "CD" are determined by the event trees. The "OK" status denotes a safe final reactor conditions, and the "CD" status indicates the failure of safety systems that result in core damage. Figure 3 through Figure 7 (in the appendix) show the event trees modeled for the SGNP.

The SGNP event tree models are simplified by having only two possibilities: "Actuates" and "Fails." "Actuates" is taken to mean that the action / component / system occurs/operates as desired and at a sufficient level. "Fails" is taken to mean that the action / component / system does not meet the required level of action by either inaction, undesired action, or insufficient action.

Failure of the events in the event trees are determined by their associated fault trees. Figure 8 through Figure 23 (in the appendix) illustrate the fault trees for the SGNP. The fault trees differ from most internal event PRAs as they consider the failure of passive components (pipes and tanks), and not just the failure of active components (valves, pumps, etc…). Each fault tree was formed from understanding the SSCs of each system, and the systems they rely upon. The success criteria for the PRA was the successful cooling of the reactor core to cold standby (through Mode 4 to achieve Mode 5, Shutdown), when the RHR system is required to cool the reactor, due to low temperature and pressure. As the RHR system would be required to run for decay heat removal, this success criteria would challenge the major cooling systems of the reactor facility.

The failure combinations given by the fault trees and events in the event trees give the cut sets for the SGNP. For the purposes of this demonstration failure probabilities were not considered, so what remains are all possible failure paths to core damage for the SGNP, 169,115 different cut sets, with the largest cut sets having 10 different components. As this number of cut sets is unwieldy, ten cut sets were selected to use for

demonstration, six with RPS trip as the initiating event, two with a steam line break in loop A as the initiating event, and two with a LBLOCA as the initiating event. These ten cut sets are shown in Figure 1, in the report format from the SAPHIRE 7 PRA program.

As a note: the model of the reactor and systems in the PRA applies only to the simulated reactor facility and do not approach the complexity and redundancy of an actual nuclear reactor design. The descriptions provided for the cut sets apply to the model only, and are not intended to provide an account of actual reactor system, component, or procedure performance or capabilities.

END STATE CUT SETS REPORT

Project: SGNP Case : Current

Analysis: RANDOM Units: Per Year

End State Cut Set # Events Count Inputs

CD 7 2 RPS-TRIP, CCW-COMP-FAIL

14 3 RCS-LBLOCA, ACC-PIPE-INJ-LINE-A, ACC-PIPE-INJ-LINE-B

30 3 RCS-LBLOCA, HHSI-A-PUMP-UNIT-FAIL, HHSI-B-PUMP-UNIT-FAIL

201 3 RPS-TRIP, RHR-A-HX-UNIT-FAIL, RHR-B-HX-UNIT-FAIL

710 4 RPS-TRIP, EDG-A-UNIT-FAILS, EDG-B-UNIT-FAILS, LOOP

928 4 SL-A-BREAK, CCW-COMP-FAIL, COND-B-FAIL, EFW-A-MP-FAIL

1360 5 RPS-TRIP, FW-A-MP-FAIL, FW-B-MP-FAIL, VT2A-Fail, VT2B-Fail

3062 RPS-TRIP, COND-A-FAIL, COND-B-FAIL, EFW-A-MP-FAIL, EFW-A-SP-FAIL, VT2B-Fail

3666 6 RPS-TRIP, EFW-A-MP-FAIL, EFW-A-SP-FAIL, FW-A-MP-FAIL, FW-B-MP-FAIL, VT2B-FAIL

9757 6 SL-A-BREAK, SWITCHYARD-FAIL, VE2A-FAIL, VE3A-FAIL, VS2A-FAIL, VS2B-FAIL

2014/08/02 Page # 19:01:01

Model Rev. ----/--/--

Figure 1: Selected PRA Cut Sets

Cut set 7 consists of a trip of the reactor protection system to shut down the reactor and the failure of the CCW system. This cut set led to core damage as upon RPS trip, safety systems are required to bring the reactor to a shutdown state. The component cooling water system provides the cooling to systems required to control the reactor. Without the proper cooling, these systems fail, stopping the cooling systems to the reactor, and leading to core damage.

Cut set 14 consists of a large break in the reactor coolant system, and failures of both of the accumulator injections lines. Upon a large break loss of coolant accident, additional water inventory is required to be added to the reactor coolant system to cool the reactor. This coolant is injected into the cold leg of the RCS through the accumulator injection lines. If the accumulator injection lines fail, there is no other method of providing additional coolant into the reactor vessel, and thus leads to core damage.

Cut set 30 consists of a large break in the reactor coolant system and failures of both high head safety injection pumps. As a large break loss of coolant accident results in a large amount of coolant inventory being relocated to the floor of the containment building during full-power operation, a large volume of coolant is required to replace it in a short time span. As such, the injection of at least one accumulator and one high head safety injection pump is required to provide the coolant inventory until the reactor cools enough for the residual heat removal system to take over the coolant inventory circulatory function. The loss of both high head safety injection pumps prevents the required water inventory from entering the reactor core, and thus leads to core damage.

Cut set 201 consists of a trip of the reactor protection system to shut down the reactor and failures of both residual heat removal heat exchangers. Upon RPS trip, control rods insert and reduce the reactor reactivity and cooling systems reduce the reactor coolant temperature. When the reactor coolant temperature is low enough, long-term cooling is facilitated by the residual heat removal systems, of which at least one is required. In this cut set, the loss of both RHR heat exchanges leads to no heat removal from the reactor coolant system and thus core damage.

Cut set 710 consists of a trip of the reactor protection system to shut down the reactor, loss of both emergency diesel generators, and a loss of offsite power. In order for safety systems to bring the reactor to shut down and continue removal of decay heat, electrical power is required to run instrumentation and control equipment, (most) valves, and pumps. The loss of offsite power means no electricity is reaching the site to power equipment, and thus the use of on-site emergency diesel generators is required to provide power to plant equipment. The loss of offsite power and the emergency diesel generators leads to core damage as there is no electricity to monitor the reactor or systems or to run any equipment to cool the reactor.

Cut set 928 consists of a break in the steam or feedwater line of loop A, loss of component cooling water, loss of condenser B, and loss of motor-driven emergency feedwater pump A. For the model, the reactor can safely reach shutdown with one operational steam line without the use of emergency equipment. In this cutset, steam line A experiences a break, but makeup water cannot be added to steam loop A as the motor driven pump of the emergency feedwater system has failed (and the steam driven pump is unavailable in a steam line break in the same train). Steam loop B loses cooling function as condenser B fails. Steam is then dumped to the atmosphere in steam loop B to cool the reactor by way of a natural convective current within the RCS. The loss of component cooling water incapacitates the residual heat removal system, meaning when the reactor coolant cools below the capabilities of steam loop B, the natural convection within the reactor coolant system slows and stops and leads to core damage.

Cut set 1360 consists of a trip of the reactor protection system to shut down the reactor, loss of feedwater pumps A and B, and failure of valves VT2A and VT2B for steam dump to the atmosphere. Upon reactor trip, the turbines are tripped as well, removing their heat removal function. The loss of feedwater pumps A and B removes the ability to dump steam to condensers to remove heat. The failure (closing) of valves VT2A and VT2B closes the pathway for the steam dump to the atmosphere. With the steam/feedwater loops unable to remove heat with the condensers or through steam dump, no heat is removed from the reactor coolant system, resulting in core damage.

Cut set 3062 consists of a trip of the reactor protection system to shut down the reactor, loss of condensers A and B, loss of motor driven emergency feedwater pump A, loss of steam driven emergency feedwater pump A, and failure of valve VT2B for steam dump to the atmosphere. Upon reactor trip, the turbines are tripped as well, removing their heat removal function. The failure of the condensers to function requires that heat be removed from the core via dumping steam to the atmosphere. Failure of both the motor-driven and steam-driven emergency feedwater pumps in loop A prevents any makeup water being added to the loop and the loss of heat removal functions of that loop. The failure (closing) of valve VT2B closes the pathway for the steam dump to the atmosphere for loop B. The loss of makeup water for steam dump in loop A, and closing of the pathway for steam dump in loop B results in no heat removal functions large enough to cool the reactor core, and thus core damage.

Cut set 3666 consists of a trip of the reactor protection system to shut down the reactor, loss of motor driven emergency feedwater pump A, loss of steam-driven emergency feedwater pump A, loss of feedwater pumps A and B, and failure of valve VT2B for steam dump to the atmosphere. Upon reactor trip, the turbines are tripped as well, removing their heat removal function. The failure of both feedwater pumps removes any ability to cool the turbine/feedwater loop with the condensers. The loss of both the motor-driven and steam-driven emergency feedwater pumps in loop A prevents any makeup water being added to the loop and the loss of heat removal functions of that loop. The failure (closing) of valve VT2B closes the pathway for the steam dump to the atmosphere for loop B. The loss of makeup water for steam dump in loop A, and no pathway for steam dump in loop B results in no heat removal functions large enough to cool the reactor core, and thus core damage.

Cut set 9757 consists of a break in the steam or feedwater line of loop A, failure of the switchyard, and the failure of valves VE2A, VE3A, VS2A, and VS2B. This cutset demonstrates a partial success to cool the reactor. In this cutset, steam line A experiences a break, but due to failure of the switchyard, turbine B trips as well, removing that heat removal option. Though valves VE2A and VE3A fail, the motor operated emergency

feedwater pump functions through operational valve VE1A, cooling the reactor coolant to the point where the RHR system can take over cooling functions. This cutset leads to core damage due to the failure of valves VS2A and VS2B, which prevent the RHR system from providing a circulating current and cooling to the reactor coolant system.

Chapter 4

Program Demonstration

The resulting cut sets from the PRA represent the failure combinations due to random failures of equipment considered in the PRA. The program uploads this data from the PRA to use as a starting point for the development of target sets. The addition of data from other sources populates data fields that allow for the efficient sorting and grouping of target elements and target sets.

Build Frame

Figure 1 is the cut set data file received from the SAPHIRE PRA model of the SGNP. The program imports this SAPHIRE PRA cut sets, and populates data files for the target sets and target elements. For example, Table 3 and Table 4are examples of what the resulting data files would look like for a target element and a target set after importing cut set 928 from Figure 1.

Table 3: Target Element #7.02 Data File after import

Target Element Data file	
Attribute	Value
ID#	7.02
IDName	CCW-COMP-FAIL
Name	
Type	
Location	
Modes	
Train	
System	
Cyber?	
Flood?	
Fire?	
Operator?	
Target Sets	7, 928

** Data File Parameters are described after Table 1*

Table 4: Target Set #928 Data File after import

Target Set Data File	
Attribute	Value
ID#	928
# Elements	4
# Locations	
Modes	
Train(s)	
Systems	
Cyber?	
Flood?	
Fire?	
Operator?	
Elements:	7.02, 928.01, 928.02, 928.03

* *Data File Parameters are described after Table 1*

Table 19**Error! Reference source not found.** (in the appendix) shows the "Element Build List" after importing from the PRA data file. The occupied fields are those that would be filled automatically by the program upon PRA data file import. The empty fields need to be filled by the user.

The program takes the cutset data from the PRA to create most of the failure combinations found in the target sets. It is up to the user to add to or remove from the imported data to complete the target sets. After importing data from the PRA data file, the remaining information is entered manually due to the non-standard nature of the documents, figures, and tables that should be used to complete the data entry for the target elements and target sets. The additional information is required to be entered to provide the level of detail necessary to determine the insights desired of the target set development process. This additional information is required for target set development if a user has the program or not, but the program has means to expedite and replicate the

data entry, and update with new data when plant changes occur. In this way, the entry of this data needs to occur once, and then be maintained for the life of the design.

The program provides a means to catalog and comment upon the documents required to provide the additional information beyond what is found in the PRA. Table 5 lists the bibliographic entries for the source documents used to fill in the remaining information fields for the SGNP target elements and target sets. The documents listed in Table 5 are some of the dozens that would need to be consulted to complete target sets.

Site PRAs would document different failure combinations that lead to different undesirable consequences (e.g. core damage and/or radionuclide release) and most of the safety related SSCs. Documentation related to the development of the PRAs would outline system dependencies, success criteria, and criteria for component inclusion in the PRA.

The site Safe Shutdown list would document those SSCs required to affect and maintain reactor shutdown consistent with 10 CFR Part 50. Class 1E equipment is defined as safety-related electrical equipment, consistent with The Institute of Electrical and Electronics Engineers (IEEE) Standard IEEE 323-1974, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations." Seismic Category I SSCs are to be designed to withstand seismic events consistent with RG 1.29, "Seismic Design Classification." P&IDs illustrate system design and connections in a graphical manner. Review of P&IDs and system walk downs may reveal equipment or structures omitted from PRA activities. System Description documents would outline and detail required and expected operating conditions of systems and equipment performance. ite procedures and training manuals would provide details on those operator actions accounted for in the site safety analysis. Further understanding of operator actions would be required for target set development. The Cyber Security Plan and Critical Digital Asset (CDA) List would detail the analyses conducted to determine CDAs, and provide additional information on cyber security vulnerabilities not considered in the PRA.

.

Table 5: SGNP Bibliographic Table

Document	Omission from target sets
SGNP Level 1 PRA 5/3/14	
SGNP Level 1 PRA development report rev. 5	
Safe Shut Down List rev. 45	
Vital Equipment List rev. 11	Containment venting and filtering systems do not meet the definition of TS equipment
Class 1E electrical power systems	Containment venting and filtering systems do not meet the definition of TS equipment
Seismic Category I SSCs	Containment venting and filtering systems do not meet the definition of TS equipment
P&ID RCS	
RCS System Description and Requirements	
P&ID MSSS	
MSSS System Description and Requirements	
P&ID EFW	
EFW System Description and Requirements	
P&ID RHR	
RHR System Description and Requirements	
P&ID SIS	
SIS System Description and Requirements	
P&ID CCW	
CCW System Description and Requirements	
Site Procedures - Reactor Operator Actions	Procedures for containment venting and filtering systems do not meet the definition of TS equipment
Site Training Manual - Reactor Operator	Training for containment venting and filtering systems do not meet the definition of TS equipment
SGNP Cyber Security Plan	
SGNP Critical Digital Asset List	CDAs that relate to containment venting and filtering systems do not meet the definition of TS equipment

* SIS: Safety Injection System

Table 5 shows documents with SSCs omitted from target sets. The definition of target set is more restrictive than safety-related or vital equipment, as it does not include the functions to mitigate or prevent any offsite releases after core damage or spent fuel sabotage. Due to this difference, some systems and components would be expected on safety-related and vital equipment lists and not in the target sets. Other omissions from the target sets from safety-related equipment lists would be documented in a similar manner to provide traceability on the inclusion and exclusion of equipment.

Using the documents in Table 5, we fill in the empty information fields in the Target Element and Target Set Data Files. Easy updating of data would be accomplished with the "Element Build List" through group selection and updating on the table. Table 6 and Table 7 show examples of data files after populating the information fields for target element 7.02 and target set 928.

The population of data files with the new information provides the ability to sort and group target elements and target sets for more data entry. Once all fields have been completed, the user can then identify start to develop insights.

Table 6: Target Element #7.02 Data File with Complete Information Fields

Target Element Data file	
Attribute	Value
ID#	7.02
IDName	CCW-COMP-FAIL
Name	Comp. Cool Water
Type	Cool Sys.
Location	AUX
Modes	1,2,3,4,5,6
Train	
System	CCW
Cyber?	Y
Flood?	N
Fire?	Y
Operator?	N
Target Sets	7, 928

Table 7: Target Set #928 Data File with Complete Information Fields

Target Set Data File	
Attribute	Value
ID#	928
# Elements	4
# Locations	3
Modes	MSSS A
Train(s)	MSSS B
Systems	CCW, MSSS A, MSSSB, EFW A
Cyber?	0.5
Flood?	0.25
Fire?	1
Operator?	0
Elements:	7.02, 928.01, 928.02, 928.03

After populating the information fields we find the complete "Set Build List" for the "build frame" in Table 8.

Table 8: Set Build List in with Complete Information Fields

ID#	# elements	# location	Modes	Train(s)	Cyber?	Flood?	Fire?	Operator?
7	2	2	1,2,3,4		1	0.5	1	0
14	3	1	1,2,3,4,5,6	A, B	0.33	0	0.33	0
30	3	2	1,2,3,4	A, B	0.66	0.66	1	0
201	3	1	1,2,3,4	A, B	0.33	0.33	1	0
710	4	2	1,2,3,4		1	1	1	0
928	4	3	1,2,3,4	A, B	0.5	0.25	1	0
1360	5	1	1,2,3,4	A, B	1	1	1	2
3062	6	2	1,2,3,4	A, B	0.83	0.83	1	1
3666	6	2	1,2,3,4	A, B	1	1	1	1
9757	6	4	1,2,3,4	A, B	0.83	0.83	1	0

Table 8 shows several insights at this point. Every target set with 3+ targets has a reduction in locations to fewer than the number of targets. Most target sets apply to

conditions at power, and only one applies to shut down conditions. Most target sets would be affected if a steam or safety train would be taken out of service. There exists a possibility of whole target sets being susceptible to cyber-attack. Several target sets are susceptible to flooding conditions. Almost all target sets are very susceptible to fire. Cyber-attack, flooding and fire susceptibility are indicated by the fractional number of elements in the target set that are susceptible to those types of attacks. Three target sets have operator actions outside the main control room associated with them. Insights like these should be examined in the "challenge frame" as the target sets are not yet fully developed.

The updated and complete "Element Build List" for the "Build Frame" is shown in Table 20 (in the appendix). Some information fields in Table 20 remain empty as location or train designations may not apply, for example: the RPS-TRIP target element could be accomplished in many different locations by many different methods (Operator-initiated in the main control room (MCR), remote shutdown workstation (RSWS), through manipulation of a sensor, through automatic initiation by the RPS after an adversary attack on plant safety systems occurs, or through onsite or offsite adversary action) and thus location information is inapplicable. Similarly, the LOOP target element can be accomplished by an offsite adversary in locations not within the jurisdiction of the site security force, and thus location information is inapplicable. Information on target element "train" would primarily serve a purpose in the "challenge frame" to update target sets when trains are taken out of service for maintenance. Many systems, structures and components would not belong to a specific train.

The PRA provides an excellent starting point for target sets, but the differences between PRA and target sets necessitates a review of system documentation to verify that the components imported from the PRA are appropriate for target sets, and to add target sets for components not found in the PRA. RG 5.81 provides guidance on the use of PRA, additional documents, and clarification on some of the subtleties between PRA and target sets.

The creation of new data files is easiest when the PRA data has been fully uploaded and information fields have been completed, as the program can copy existing target elements for the purposes of creating new ones. For example, to represent a design change at the SGNP of adding a valve to RHR loop A, before the RHR heat exchanger, we pick to copy target element 9757.04, RHR A injection line valve, an element of similar function and purpose. Table 9 shows the data file for target element 9757.04.

Table 9: Target Element #9757.04 Data File

Target Element Data file	
Attribute	Value
ID#	9757.04
IDName	VS2A-FAIL
Name	Rx Trip
Type	RHR A Inj line Valve
Location	AUX
Modes	1,2,3,4,5,6
Train	A
System	RHR A
Cyber?	Y
Flood?	Y
Fire?	Y
Operator?	N
Target Sets	9757

Upon choosing to copy target element 9757.04, a window would open with the fields shown in Table 10.

The new target element is automatically assigned a new ID#, and the remaining fields are "grayed." The "grayed" text can be overwritten or removed, or if there is no change, the "grayed" text is what is written to the new data file.

Table 10: Copy of Target Element #9757.04 Data File

Target Element Data file COPY	
Attribute	Value
ID#	9757.06
IDName	VS2A-FAIL
Name	Rx Trip
Type	RHR A Inj line Valve
Location	AUX
Modes	1,2,3,4,5,6
Train	A
System	RHR A
Cyber?	Y
Flood?	Y
Fire?	Y
Operator?	N
Synonymous to:	

The last information field is where the user can enter a synonymous target element. The target element does not need to be the same type of component, but needs to be synonymous in the fault tree (the synonymous component is an "or" for the new component). For this example, we could enter the valve we originally picked, target element 9757.04, or we could pick another element. We pick the RHR A heat exchanger, target element 201.01, as the single failure of either would disable RHR system A.

Upon selection of a synonymous target element and acceptance of the copy command, the program would create the new target element data file, as well as new target set files containing the new target element. When the program understands that a target element is synonymous, it copies all target sets that the synonymous target element is in, and replaces the synonymous target element with the new one in the copied target sets. For example, if we choose the RHR A heat exchanger, target element 201.01, the existing target set of our selection looks like Table 11.

The program would take all target sets that target element 201.01 is in (in our selection, that is only 201), and copy them to the new file to create the new synonymous target set.

Table 11: Target Set #201 Data File

Target Set Data File	
Attribute	Value
ID#	201
# Elements	3
# Locations	1
Modes	1,2,3,4
Train(s)	A,B
Systems	RPS, RHR
Cyber?	0.33
Flood?	0.33
Fire?	1
Operator?	0
Elements:	7.01, 201.01, 201.02

Table 12 shows the new target set that is synonymous with Target Set 201 as the result of originally copying target element 201.01 and declaring the new target element synonymous with 201.01.

For the creation of new target elements (and thus target sets), the program would be uniquely designed to expand on the information already provided. The use of existing data allows the user to trace the basis for inclusion of new elements in the target sets, and allow ease of use in the maintenance of target sets as designs and procedures change on site.

The traceability of the target sets to existing safety analyses is important as there are systems, structures, and components not included in a PRA, that would need to be included in target sets. For example, SSCs that only passively fail under normal conditions are normally excluded from internal event PRAs, but as they could be targets

for an adversary, those SSCs need to be included in target sets. Examples of passive SSCs that could be targets of an adversary are: water tanks, building structures, and flood and fire barriers.

Table 12: Target Set #9758 Data File (synonymous to TS 201)

Target Set Data File	
Attribute	Value
ID#	9758
# Elements	3
# Locations	1
Modes	1,2,3,4
Train(s)	A,B
Systems	RPS, RHR
Cyber?	0.66
Flood?	0.66
Fire?	1
Operator?	0
Elements:	7.01, 201.02, 9757.06

Upon completion of target set development, the element build list and set build lists can be used to sort and filter target elements and target sets for report generation and printing. The primary purpose of these reporting options would be for target set development and review.

Challenge Frame

The "challenge frame" of the program would start with data compiled in the "build frame" and provide additional options for sorting, grouping and editing. For the challenge frame, the "Element Build List" and "Set Build List" would gain additional capabilities and become the "Target Element List" and the "Target Set List." The "challenge frame" would possess the capability to create and save different scenarios to replicate site conditions under which an adversary attack would be credible. The

"challenge frame" is intended for grouping target sets and elements to replicate adversary attack goals and capabilities.

Grouping target elements in the "challenge frame" is achieved by "masking." Masking begins similarly to making a new target element in the "build frame." Masking different target elements seeks to simplify the target sets to commonly defended locations containing many targets.

The main control room contains target elements for likely every target set, but it can be simplified to a single target. Similarly, most equipment in reactor containment is simplified to a single target, due to the multitude of ways an adversary could cause core damage upon access. For this example, we will simplify all target elements found in containment with a mask called "containment," as shown in the mask data file in Table 13.

Mask 1 would replace all target elements listed on its data file within their target sets. The answers for "Cyber?", "Flood?", "Fire?", and "Operator?" give a conservative response. If any element that is masked has a "Yes" answer, then the mask will too.

Table 13: Mask 1 Data File

Element Mask Data File	
Attribute	Value
ID#	M1
Name	Containment
Location	Containment
Modes	1,2,3,4,5,6
Train(s)	A, B
Cyber?	Y
Flood?	Y
Fire?	Y
Operator?	N
Elements:	14.01, 14.02, 14.03, 9757.02, 9757.03

Mask 1 shows a "No" for "Operator?" as all elements contained within the mask have a "No" for "Operator?" The "Target Set List" would reflect the changes to the target sets, as shown by the highlighted target sets in **Error! Not a valid bookmark self-reference.**.

Table 14: Target Set List with Mask 1 applied

ID#	# elements	# location	Modes	Train(s)	Cyber?	Flood?	Fire?	Operator?
7	2	2	1,2,3,4		1	0.5	1	0
14	1	1	1,2,3,4,5,6	A, B	1	1	1	0
30	3	2	1,2,3,4	A, B	0.66	0.66	1	0
201	3	1	1,2,3,4	A, B	0.33	0.33	1	0
710	4	2	1,2,3,4		1	1	1	0
928	4	3	1,2,3,4	A, B	0.5	0.25	1	0
1360	5	1	1,2,3,4	A, B	1	1	1	2
3062	6	2	1,2,3,4	A, B	0.83	0.83	1	1
3666	6	2	1,2,3,4	A, B	1	1	1	1
9757	5	4	1,2,3,4	A, B	0.8	0.8	1	0

The "Target Element List" would show Mask 1, the elements it replaced would not be shown unless the mask was removed. Masked target elements are not altered or removed, but they are taken out of individual consideration for target sets within that save file, and thus can be verified to still be represented within the target sets for review and audit purposes.

Masks could also be used to group collocated elements susceptible to a single action. If we assumed that the steam-powered and motor-powered emergency feedwater pumps were collocated such that both could be destroyed or made inoperable at the same time with the same action, we could mask the elements to have the target sets better represent the conditions of the SGNP.

Table 15 shows target set 3666 before masking target elements 928.03 and 3062.02, the EFW A motor-operated and steam-operated pumps, into mask 2 (shown in

Table 16). Mask 2 combines the EFW A pumps and provides an insight for the protective strategy (wherein redundant pieces of equipment are collocated thus rendering their safety system redundancy irrelevant to an adversary).

Table 15: Target Set #3666 Data File

Target Set Data File	
Attribute	Value
ID#	3666
# Elements	6
# Locations	2
Modes	1,2,3,4
Train(s)	1,2,3,4
Systems	RPS,EFW A, MSSS A, MSSS B, SD B
Cyber?	1
Flood?	1
Fire?	1
Operator?	1
Elements:	7.01, 928.03, 1360.01, 1360.02, 1360.04, 3062.02

Table 16: Mask 2 Data File

Element Mask Data File	
Attribute	Value
ID#	M2
Name	EFW A pumps
Location	EFW Bld A
Modes	1,2,3,4
Train(s)	A
Cyber?	Y
Flood?	Y
Fire?	Y
Operator?	N

Elements: 928.03, 3062.02

Table 17 shows target set 3666 with the mask applied, reducing the number of targets by one.

Table 17: Target Set 3666 with Mask 2 applied

Target Set Data File	
Attribute	Value
ID#	3666
# Elements	5
# Locations	2
Modes	1,2,3,4
Train(s)	1,2,3,4
Systems	RPS,EFW A, MSSS A, MSSS B, SD B
Cyber?	1
Flood?	1
Fire?	1
Operator?	1
Elements:	7.01, 1360.01, 1360.02, 1360.04, M2

Masks added to the target sets will systematically reduce the number of targets and target sets, and although individual mask creation takes effort, the change takes effect through hundreds or thousands of target sets. Representing these insights in a consistent, traceable, and automated manner allows the target sets to reflect site conditions and adversary tactics for a more robust product to inform the protective strategy.

For the purposes of creating challenge scenarios, target elements can be selected as "out" to represent their unavailable, out of service, or destroyed state. Target elements can be marked as "out" in either the "Target Element List" or in the individual target element data files. The change would be reflected in the appropriate target sets. For example, if we choose target element 928.03, the EFW A motor-operated pump, to be out

of service, we can see that the highlighted target sets in Table 18 are changed as a result of this equipment unavailability.

Table 18: Target Set List with element 928.03 unavailable

ID#	# elements	# location	Modes	Train(s)	Cyber?	Flood?	Fire?	Operator?
7	2	2	1,2,3,4		1	0.5	1	0
14	3	1	1,2,3,4,5,6	A, B	0.33	0	0.33	0
30	3	2	1,2,3,4	A, B	0.66	0.66	1	0
201	3	1	1,2,3,4	A, B	0.33	0.33	1	0
710	4	2	1,2,3,4		1	1	1	0
928	3	2	1,2,3,4	A, B	0.33	0	1	0
1360	5	1	1,2,3,4	A, B	1	1	1	2
3062	5	2	1,2,3,4	A, B	0.8	0.8	1	1
3666	5	2	1,2,3,4	A, B	1	1	1	1
9757	6	4	1,2,3,4	A, B	0.83	0.83	1	0

The selecting of equipment as "out" may be saved under different scenarios files in the "challenge frame." The possibility of different save files allows for the automatic updating of many different scenarios when changes are made to the target sets.

After masking, the target element list and target set list can be sorted and filtered to show the updated qualities of the target sets desired. The sorts and filters could be saved to file, so when the target sets are updated, the insight sought would be updated as well and reflect the changes in the design. Reports could be generated from the target sets, with options to print full lists of target elements and their associated parameters. Reporting options could be saved so they are updated upon updates to the target sets.

Chapter 5

Conclusion

The results of target set development are insights to inform the site protective strategy. Using the program described, insights are easily determined for those target sets that: have the greatest flood/fire/cyber susceptibility, fewest target elements or target locations, have the greatest reliance on operator actions, are most affected by equipment maintenance and unavailability, have elements that are not contained within a vital or protected area, and are applicable to reactor modes of operations. The highlighting of the most vulnerable target sets allows informed decisions to update and improve the site protective strategy. The ability of the program to update target sets to plant configuration and design changes allows the security program to update protective measures closely in line with changes to plant safety systems and procedures.

Though the concept of target sets has been in practice since the early 1990s, the maturation of the tool and guidance has been slow. As a tool to inform a protective strategy, target sets wield great strength and flexibility, but currently are onerous and imprecise to develop and maintain. The creation of a computer program to guide, expedite and automate target set development and maintenance would affect greater security at US commercial reactor facilities, as well as any other facility or system that put the program into effect, while reducing overall costs.

Bibliography

[1] B. Mrowca, S. Pope and C. Chwasz, "Nuclear Power Plant Security Assessment Format and Content Guide," Information Systems Laboratories, Rockville, MD, September 2009.
[2] Nuclear Energy Institute, NEI 03-11 [Rev. 1], "Guidance for the Preparation and Conduct of Force-on-Force Exercises," December 2005. (Security Related Information – Withheld under 10 CFR 2.390)
[3] G. B. Varnado and N. R. Ortiz, "Fault Tree Analysis for Vital Area Identification," US NRC, NUREG/CR-0809, SAND79-0946, June 1979.
[4] G. B. Varnado and D. W. Whitehead, "Vital Area Analysis for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants," Sandia National Laboratories, Albuquerque, NM, SAND2008-5644, September 2008.
[5] US NRC. NUREG-1178, "Vital Equipment/Area Guidelines study: Vital Area Committee," February 1988.
[6] US NRC, RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," September, 2007. (Safeguards Information).
[7] US NRC, RG 5.71, "Cyber Security Programs for Nuclear Facilities," January. 2010.
[8] US NRC, RG 5.81, "Target Set Identification and Development for Nuclear Power Reactors," November, 2010. (Official Use Only – Security Related Information).
[9] US NRC, Security Order EA-02-026, "Order for Interim Safeguards and Security Compensatory Measures," February 25, 2002.
[10] US NRC, Security Order EA-03-086, "Issuance Of Order Requiring Compliance With Revised Design Basis Threat For Operating Power Reactors," April 29, 2003.
[11] US NRC, Staff Requirements Memoranda 06-0204, "Proposed Rulemaking -- Security Assessment Requirements for New Nuclear Power Reactor Designs," April 24, 2007.
[12] US Code of Federal Regulations, Chapter 10, Part73, "Physical protection of plants and materials."
[13] Power Reactor Security Requirements, 74 Fed. Reg. 13960 (March 27, 2009) (to be codified as 10 CFR pt. 73.55).
[14] The Westinghouse Electric Company LLC, "The Westinghouse Pressurized Water Reactor Nuclear Power Plant," 2006.
[15] D. W. Whitehead, C. S. Potter and S. L. O'Connor, "Nuclear Power Plant Security Assessment Technical Manual." Sandia National Laboratories, Albuquerque, NM, SAND2007-5591, September 2007.

Appendix

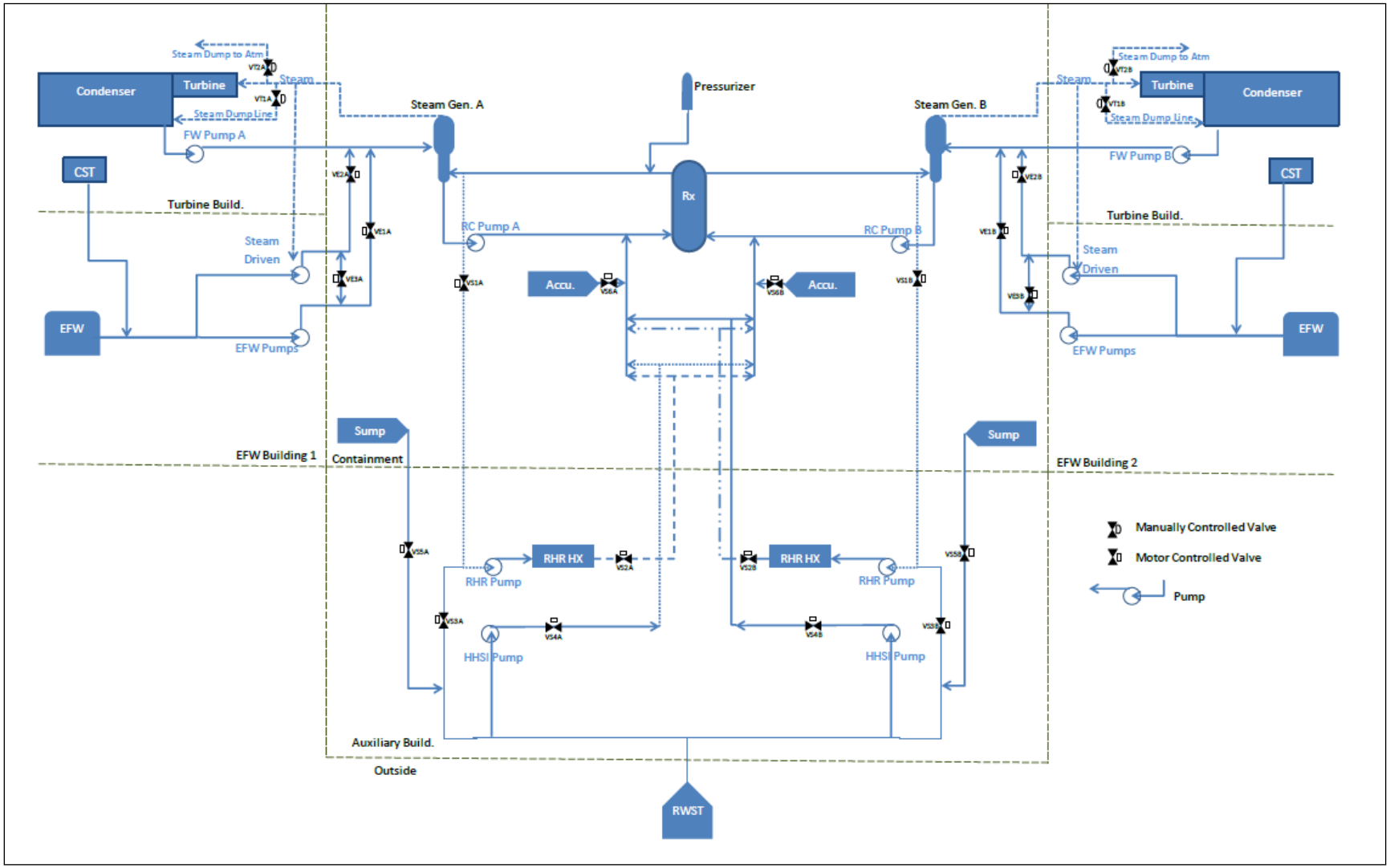


Figure 2: SGNP P&ID

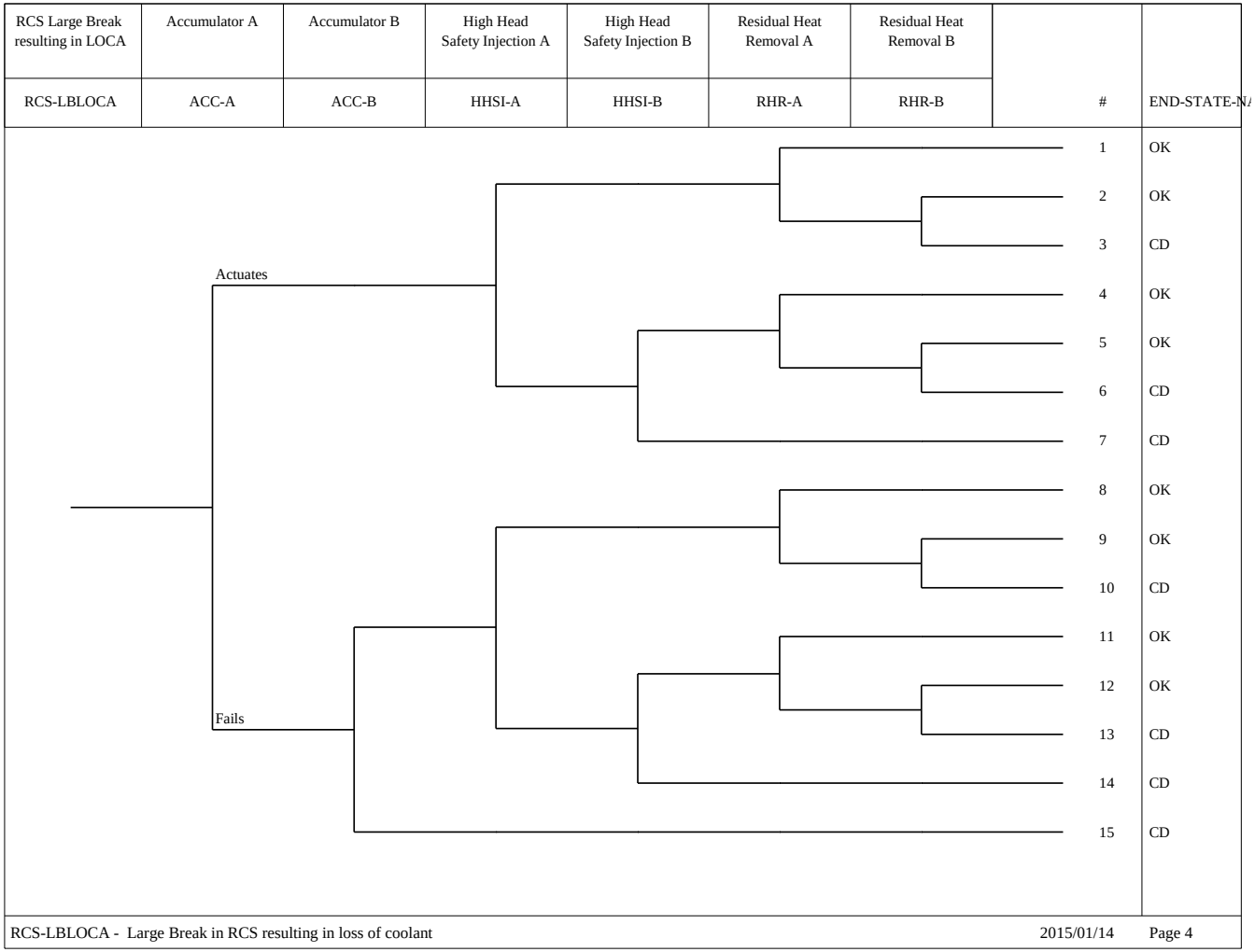


Figure 3: RCS-LBLOCA Event Tree

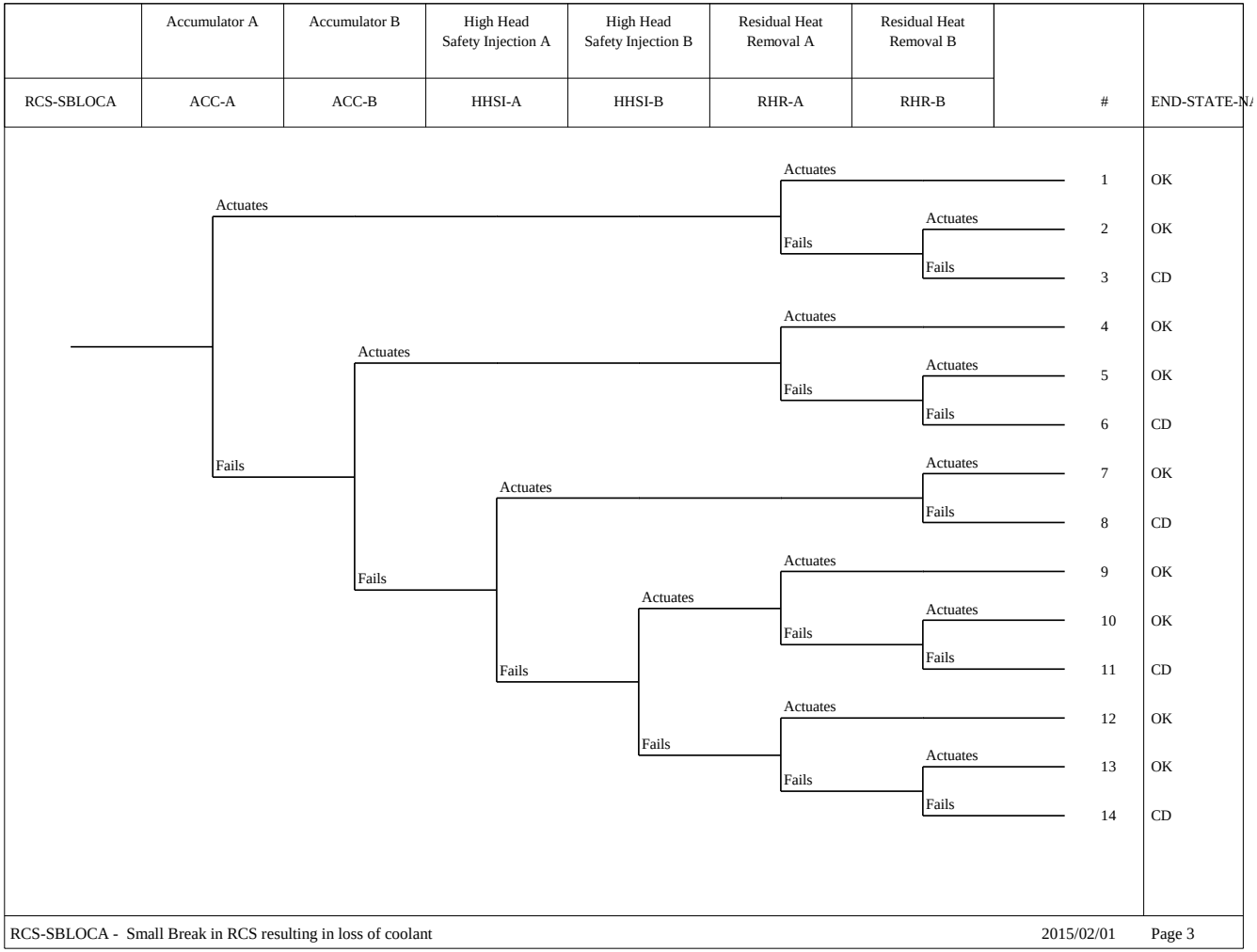


Figure 4: RCS-SBLOCA Event Tree

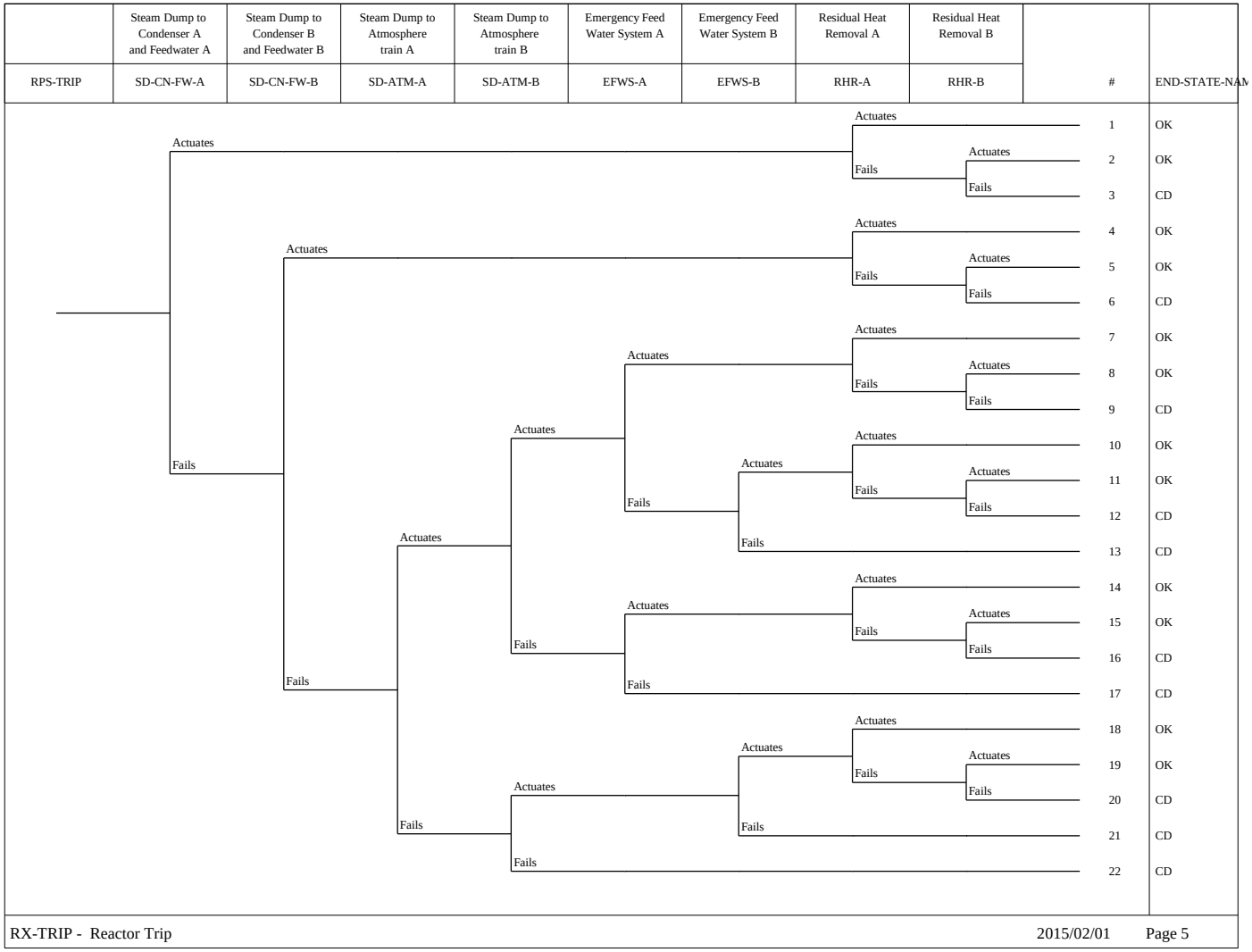


Figure 5: RX-TRIP Event Tree

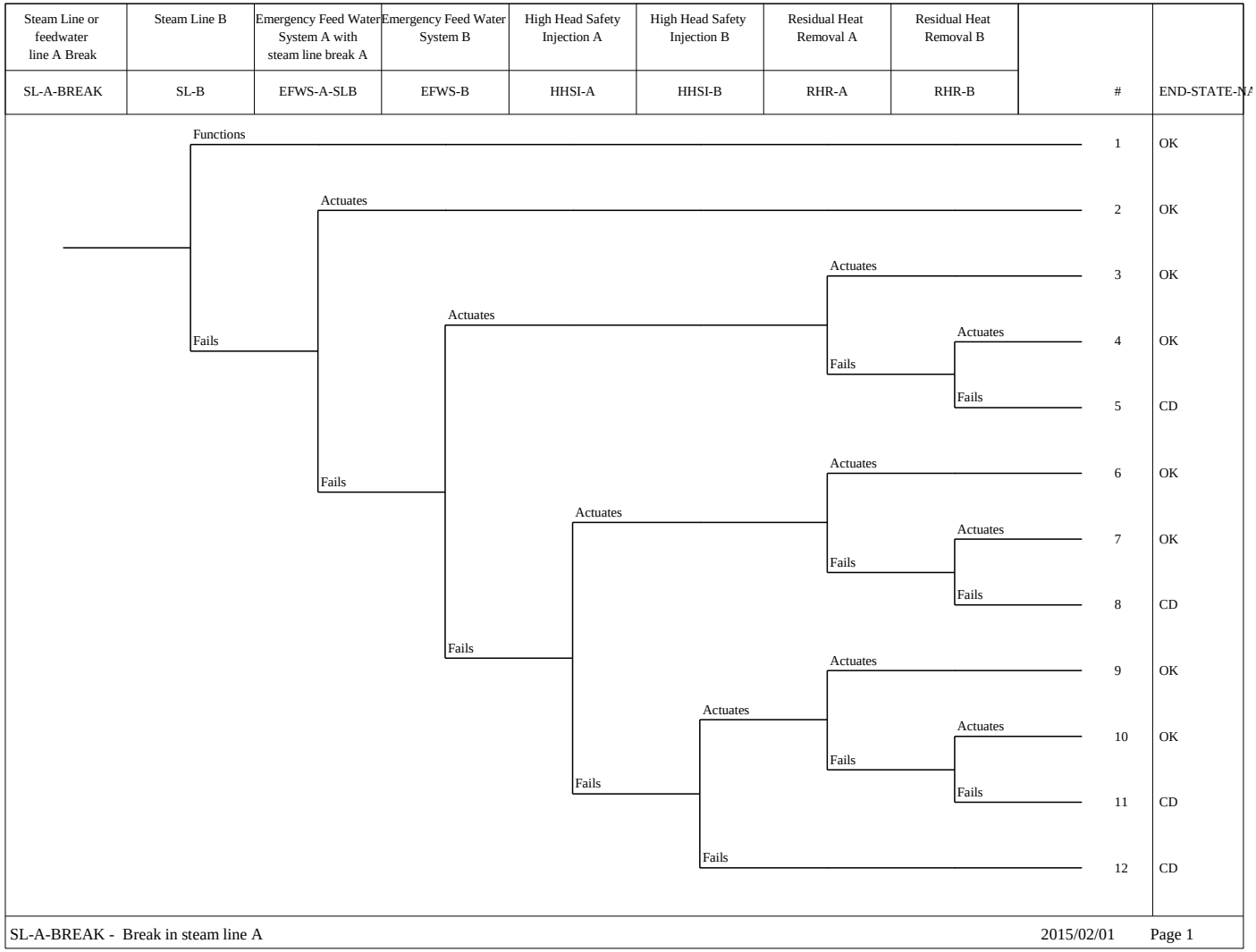


Figure 6: SL-A-BREAK Event Tree

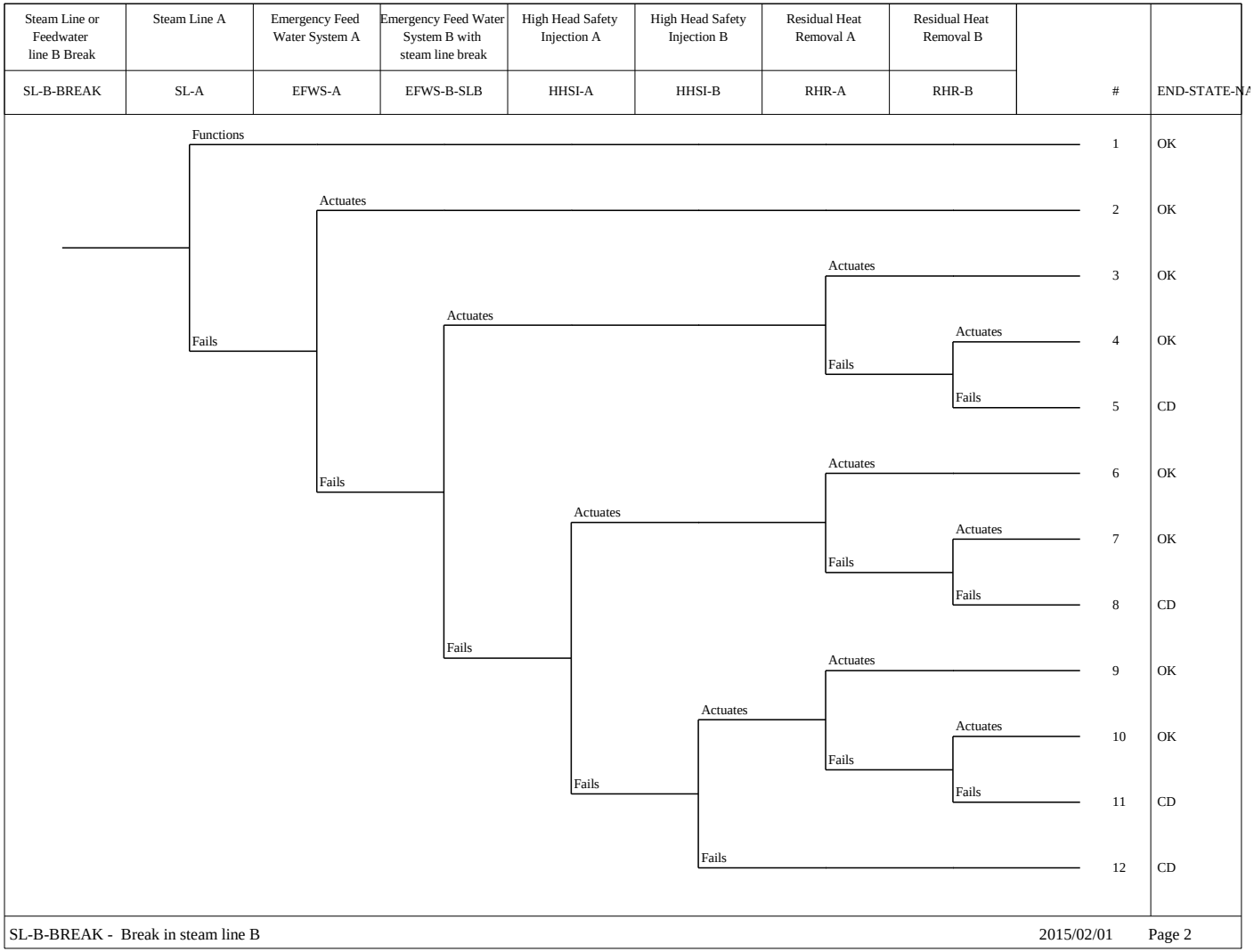


Figure 7: SL-B-BREAK Event Tree

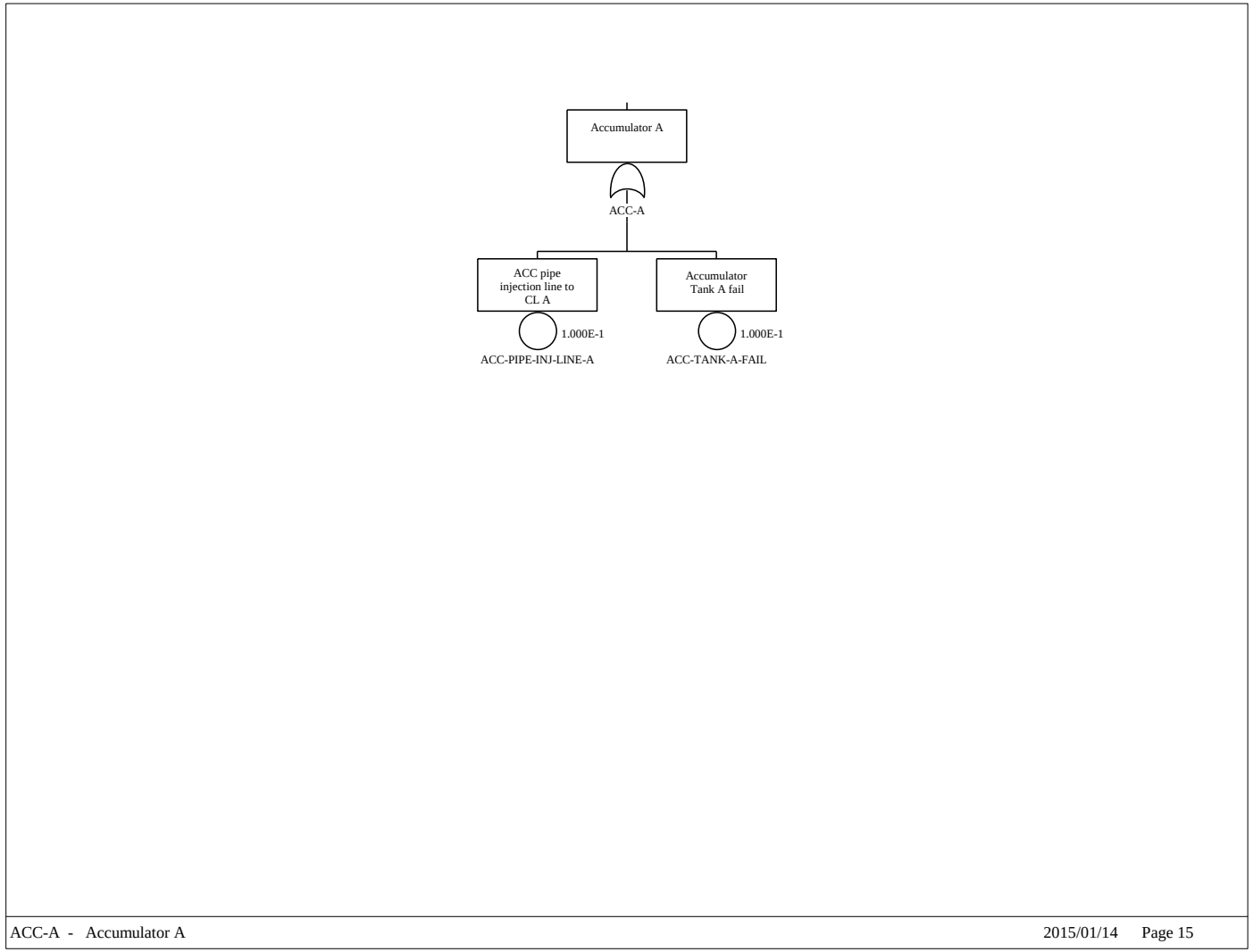


Figure 8: Acc-A Fault Tree

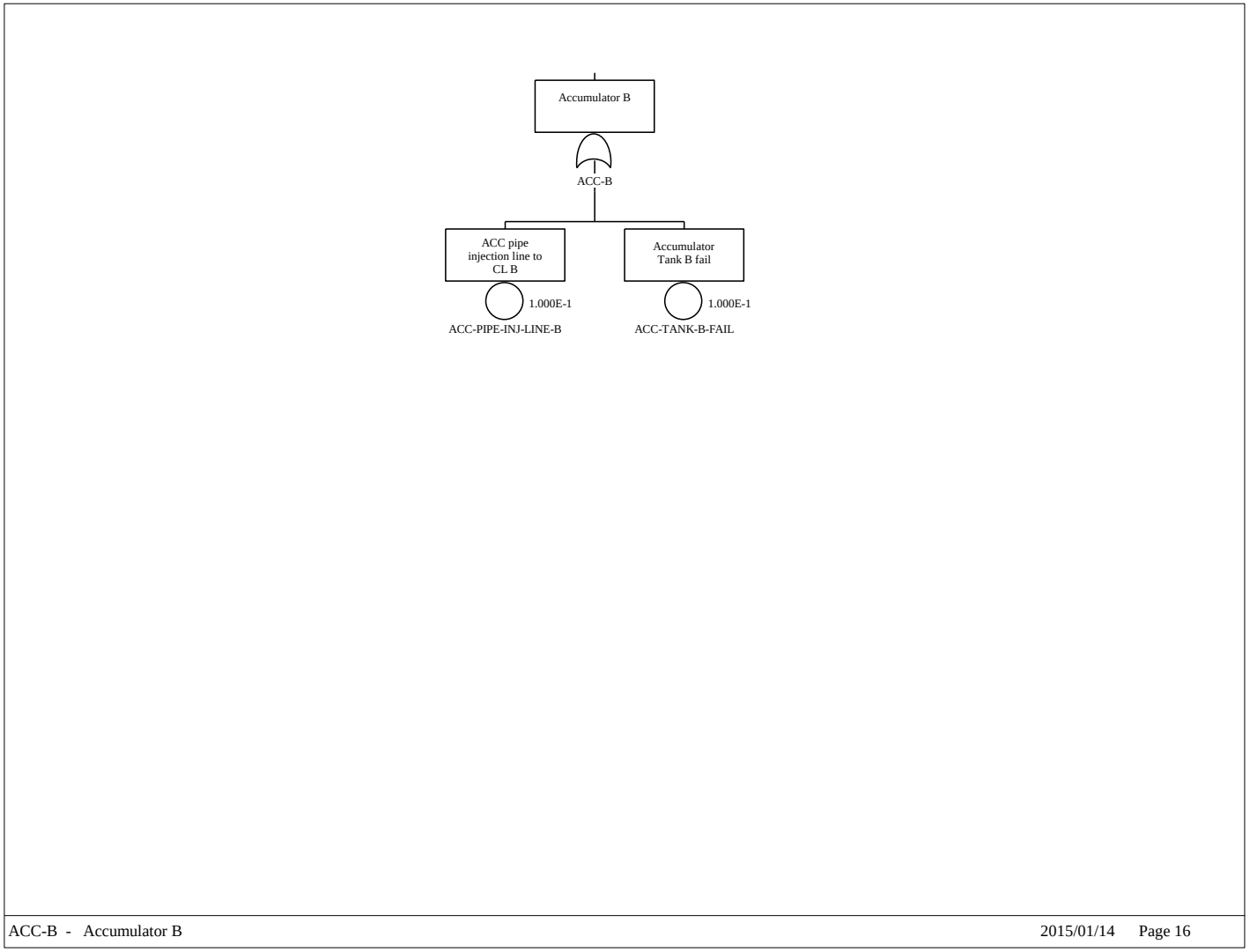
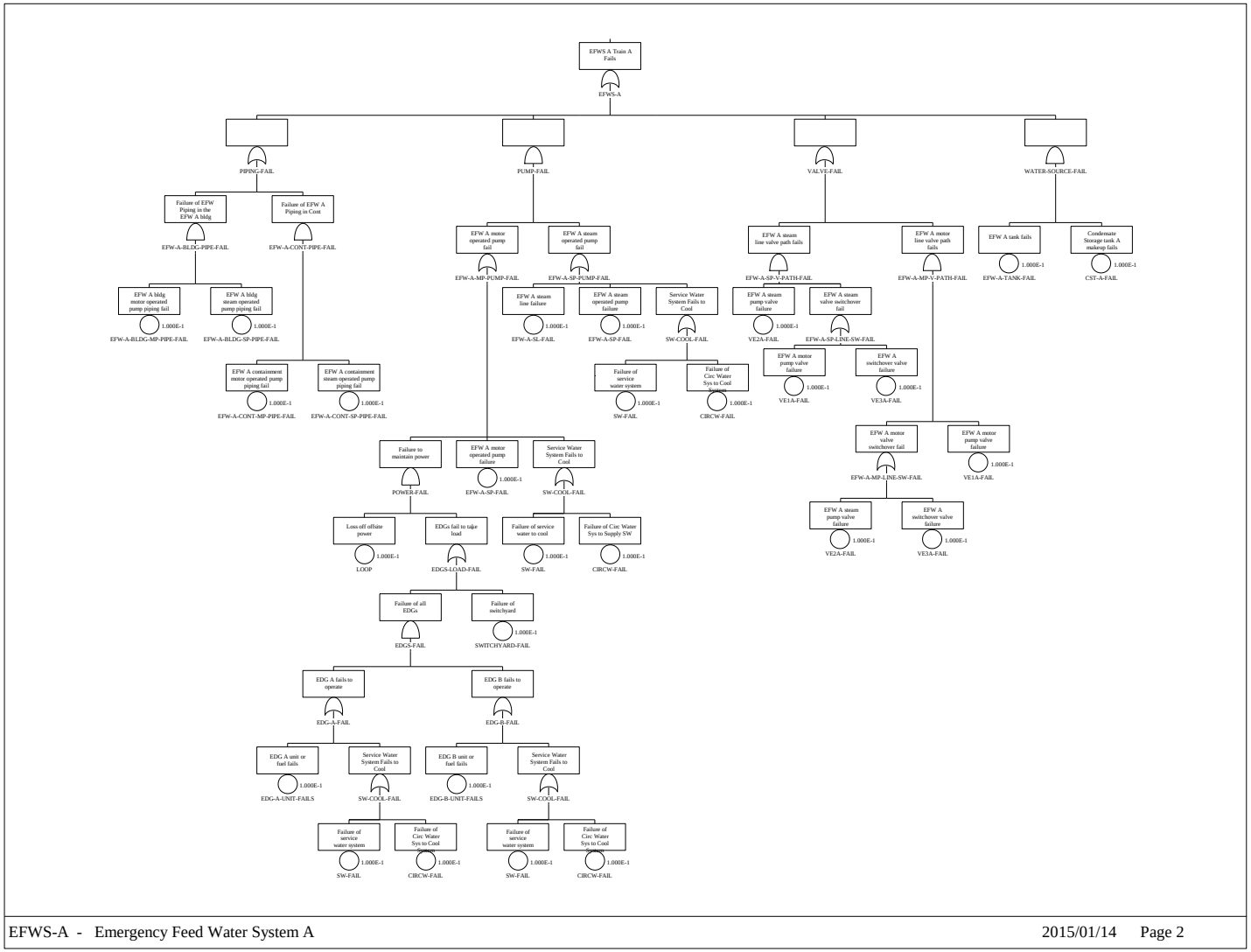


Figure 9: ACC-B Fault Tree



EFWS-A - Emergency Feed Water System A 2015/01/14 Page 2

Figure 10: EFWS-A Fault Tree

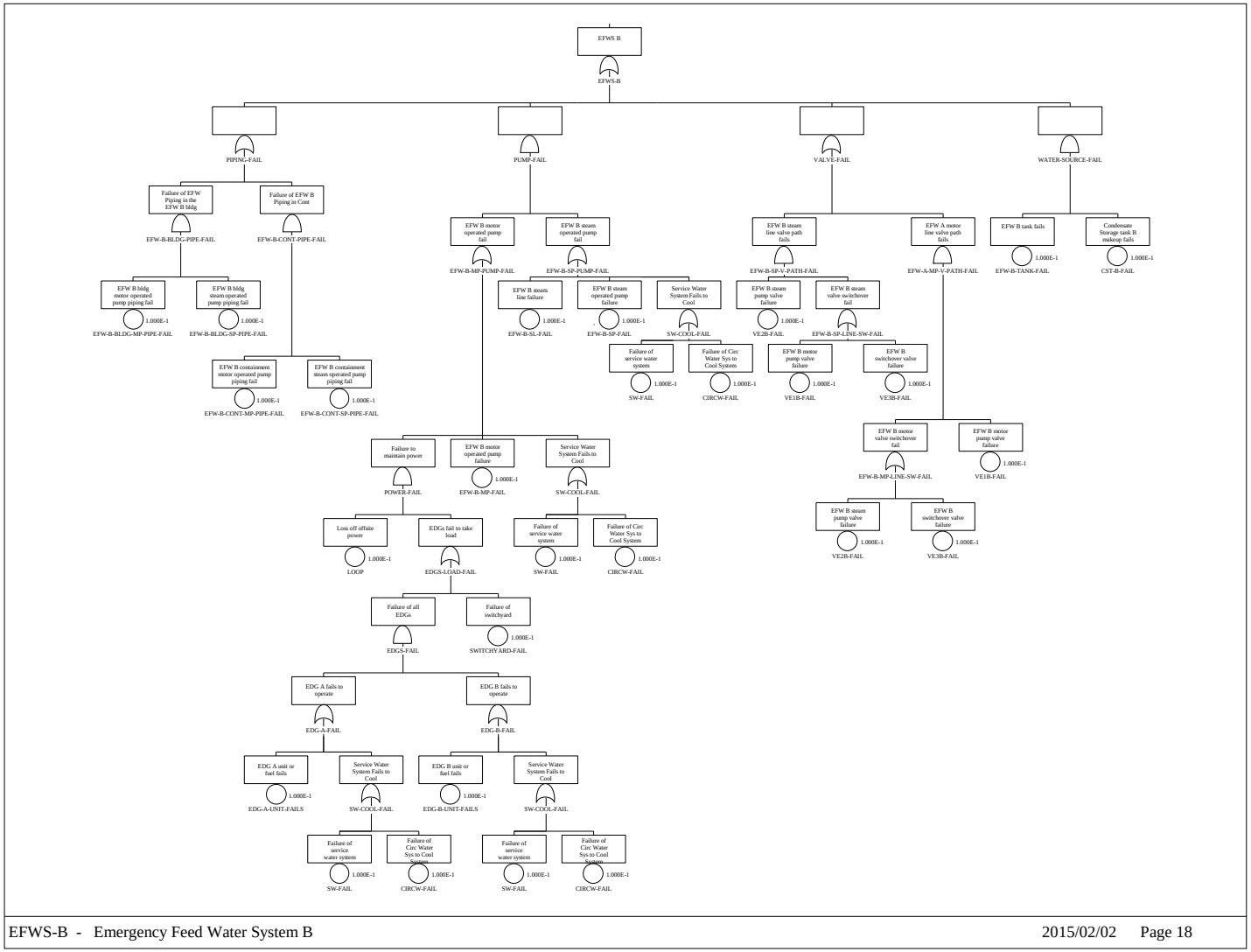


Figure 11: EFWS-B Fault Ttree

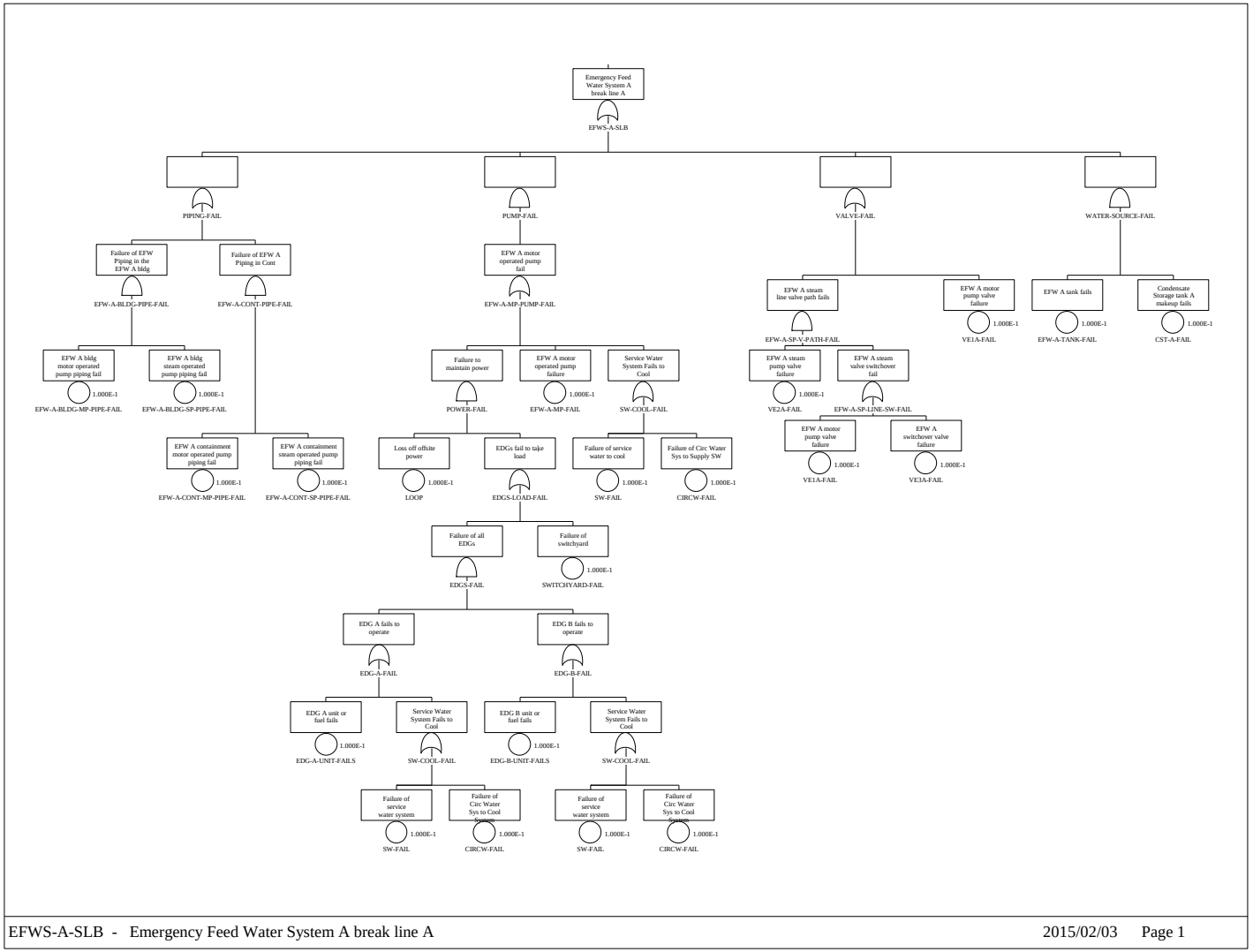
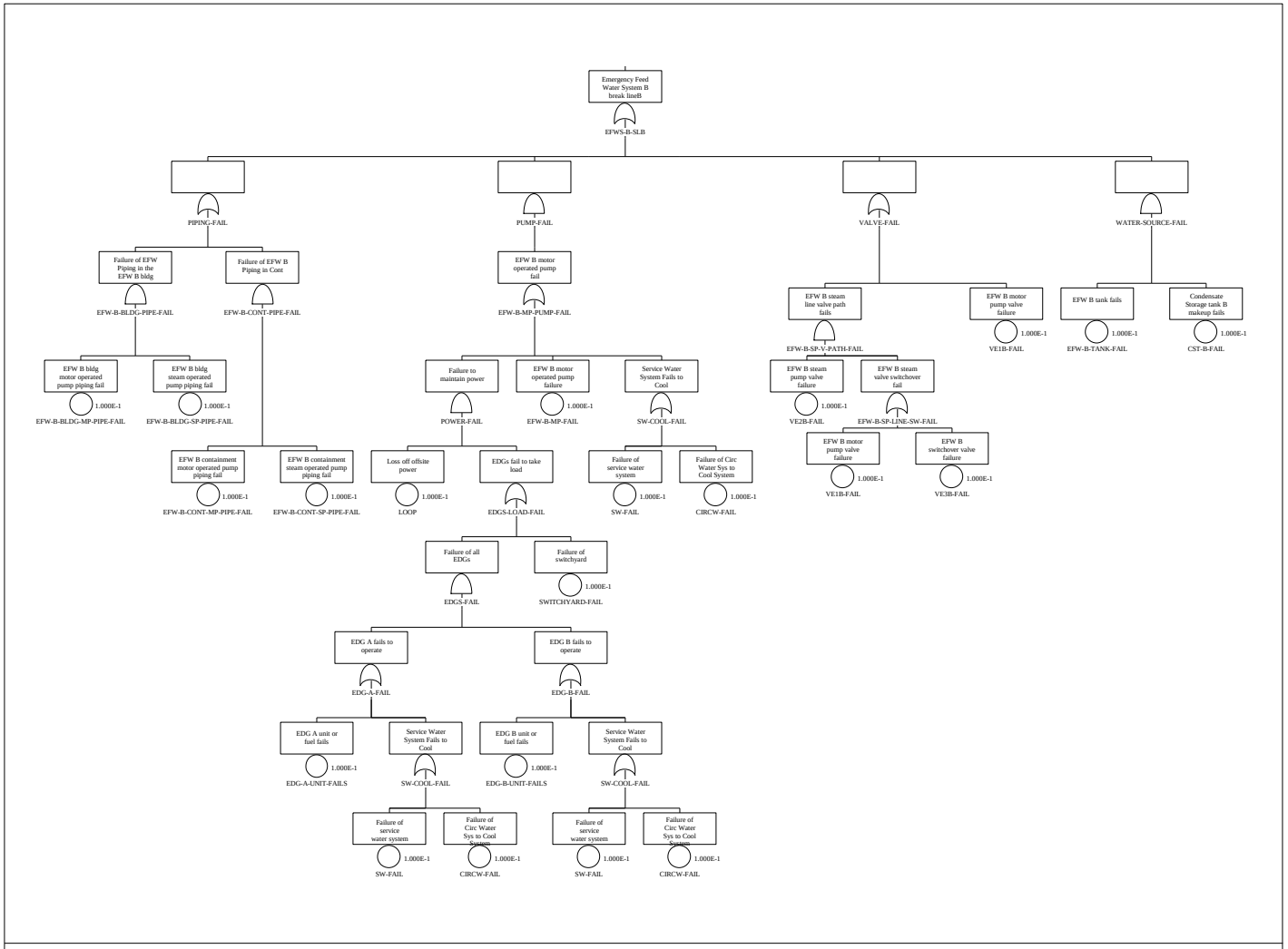


Figure 12: EFWS-A-SLB Fault Tree



EFWS-B-SLB - Emergency Feed Water System B break lineB 2015/02/02 Page 11

Figure 13: EFWS-B-SLB Fault Tree

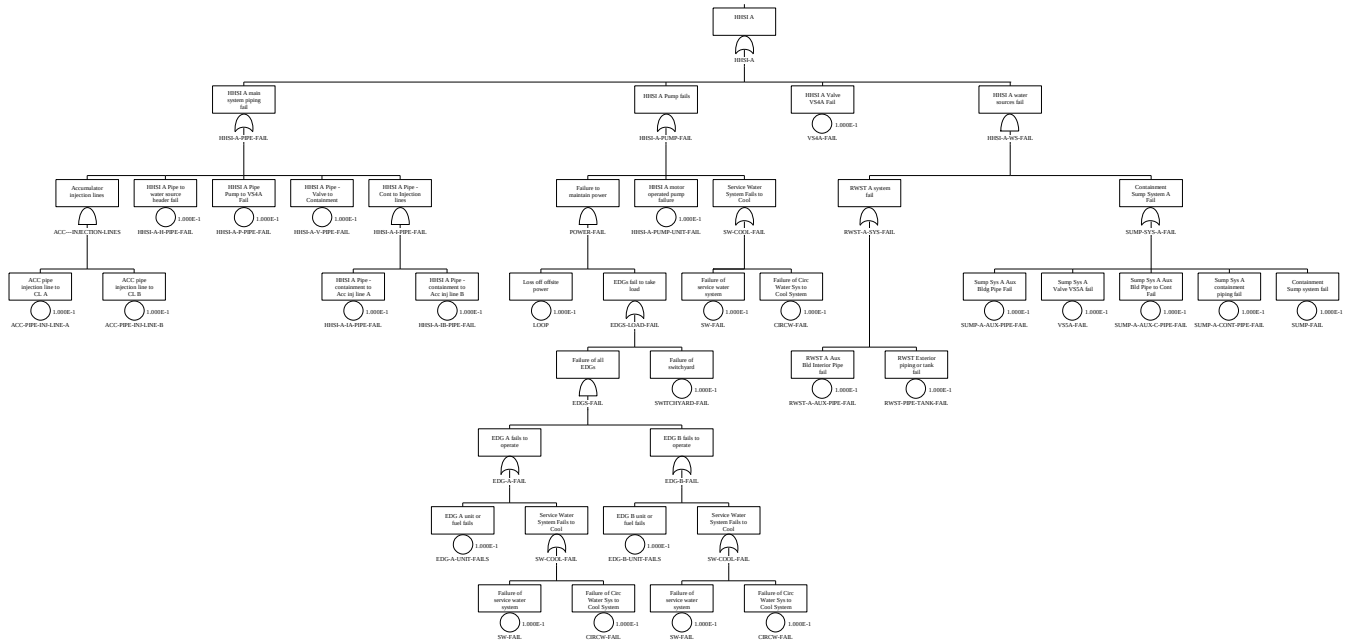


Figure 14: HHSI-A Fault Tree

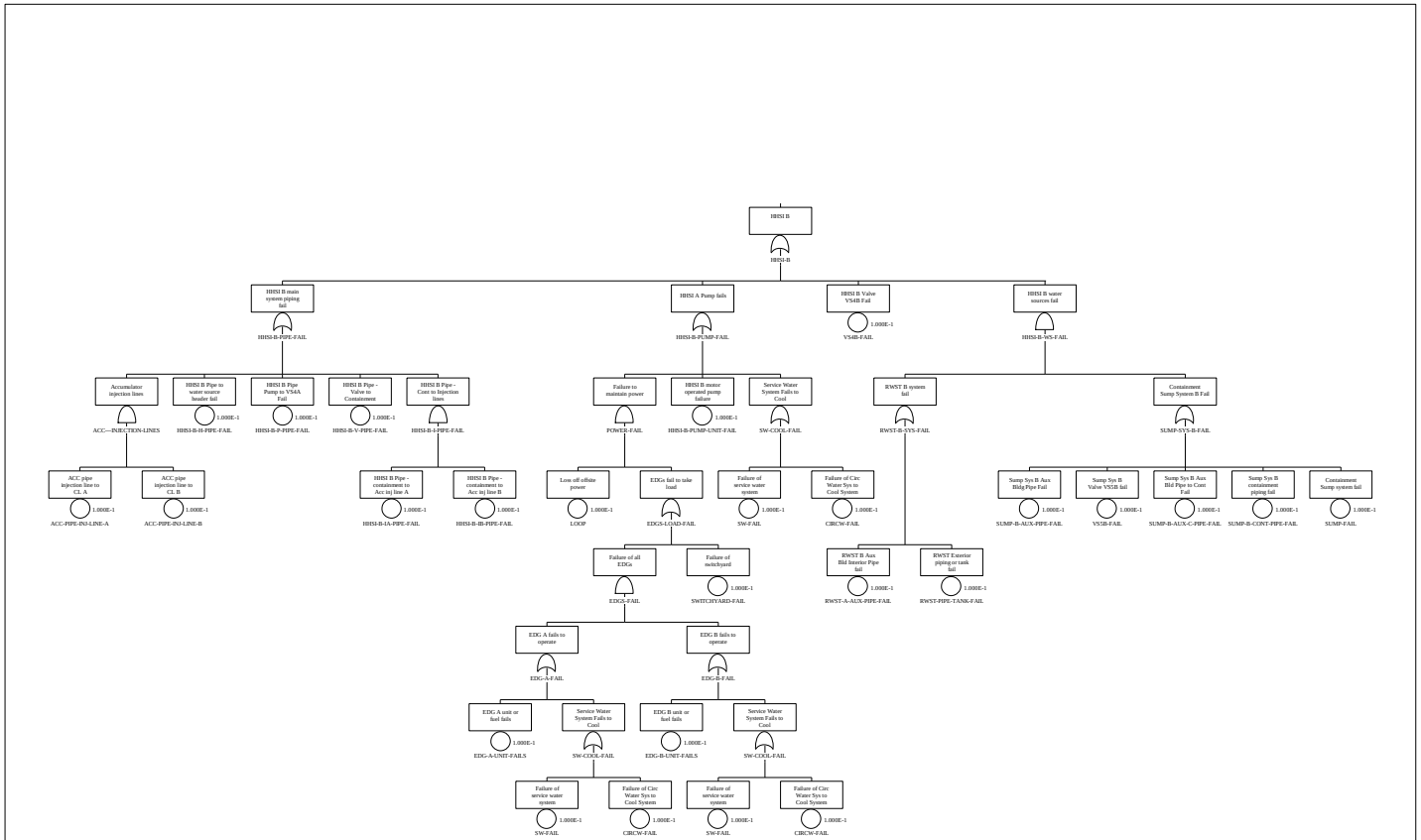
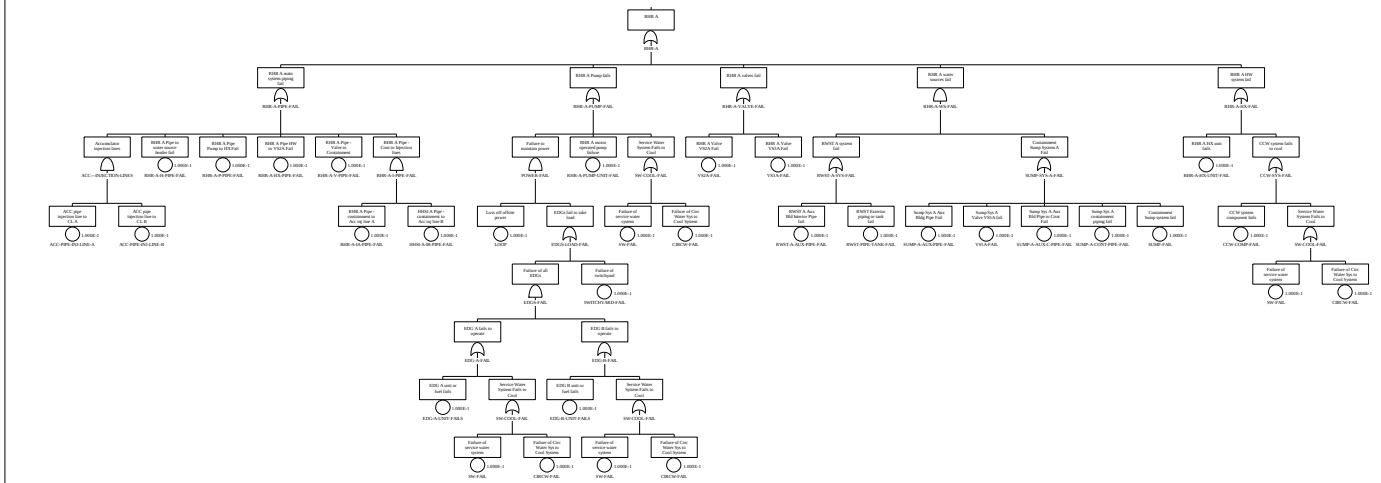
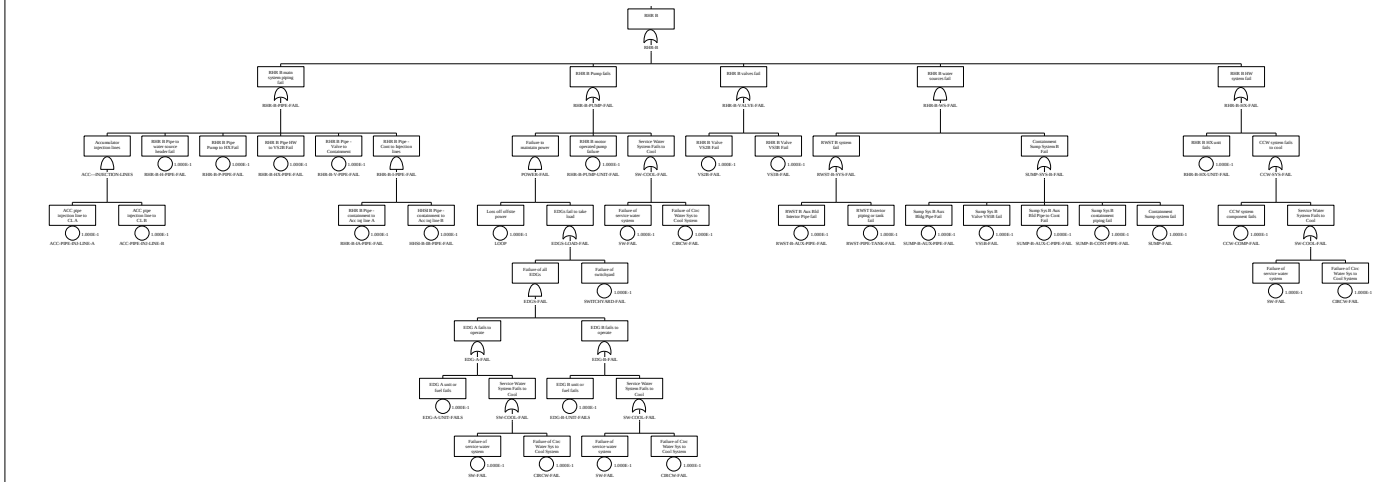


Figure 15: HHSI-B Fault Tree



RHR-A - Residual Heat Removal A 2015/01/14 Page 6

Figure 16: RHR-A Fault Tree



RHR-B - Residual Heat Removal 2015/01/14 Page 7

Figure 17: RHR-B Fault Tree

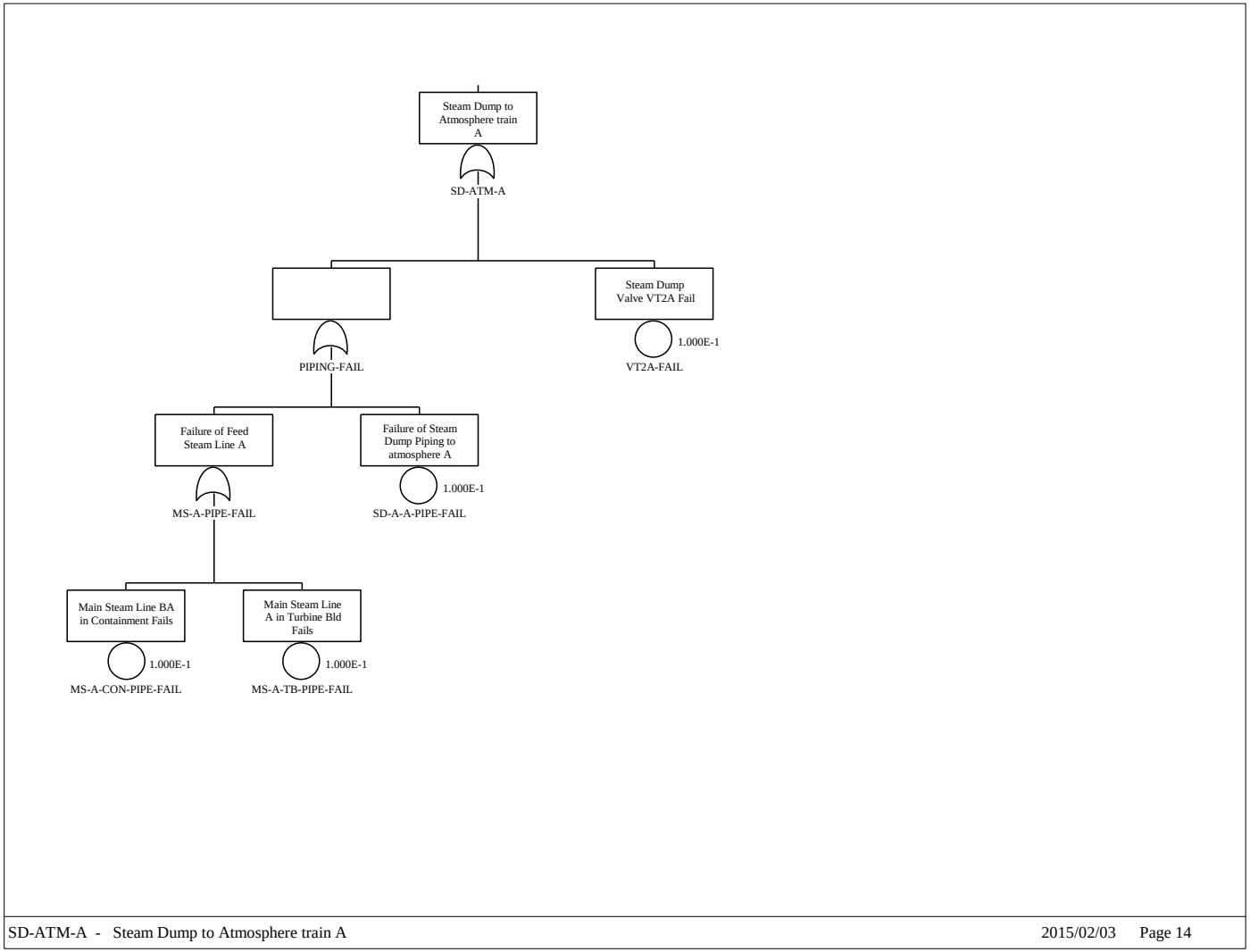


Figure 18: SD-ATM-A Fault Tree

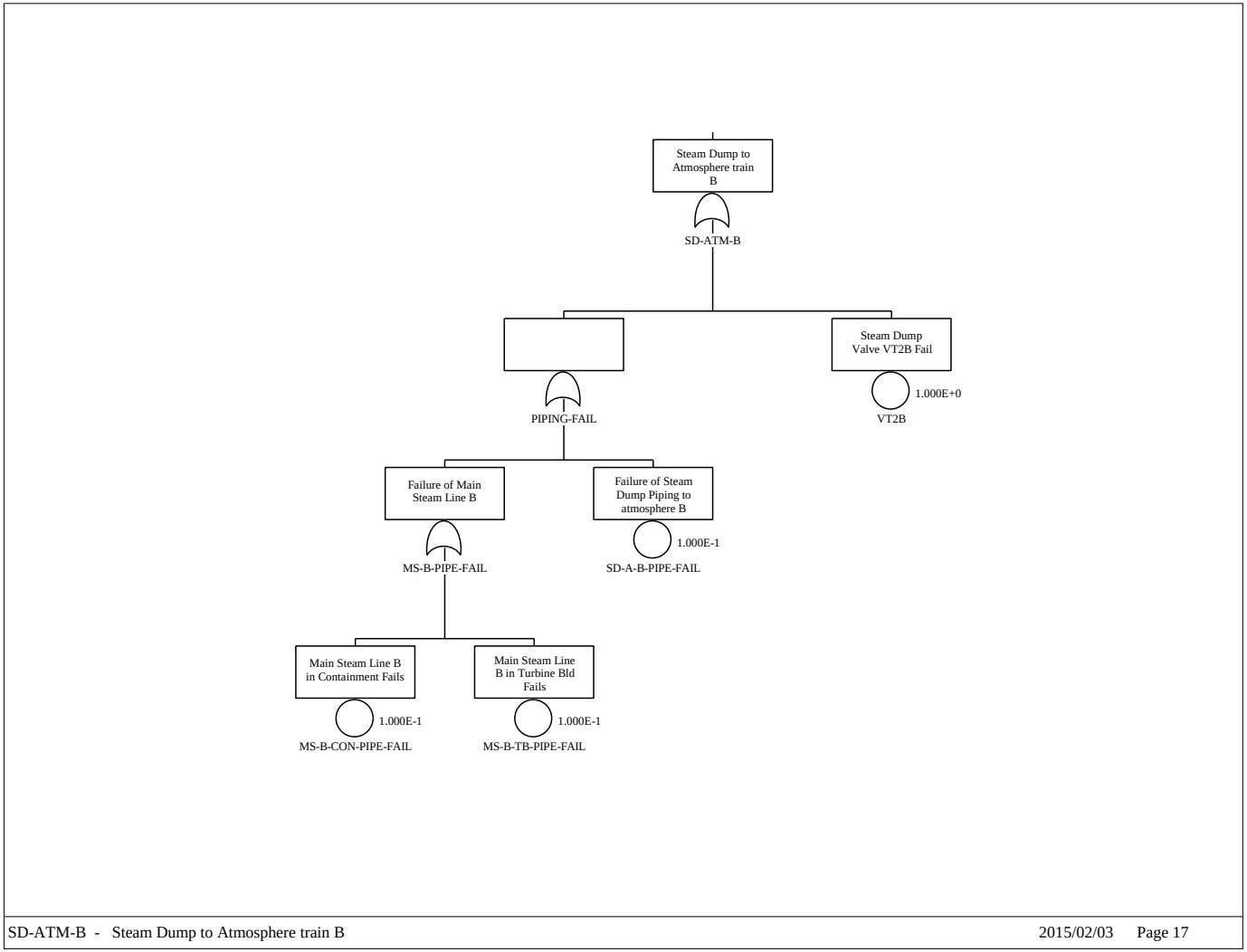


Figure 19: SD-ATM-B Fault Tree

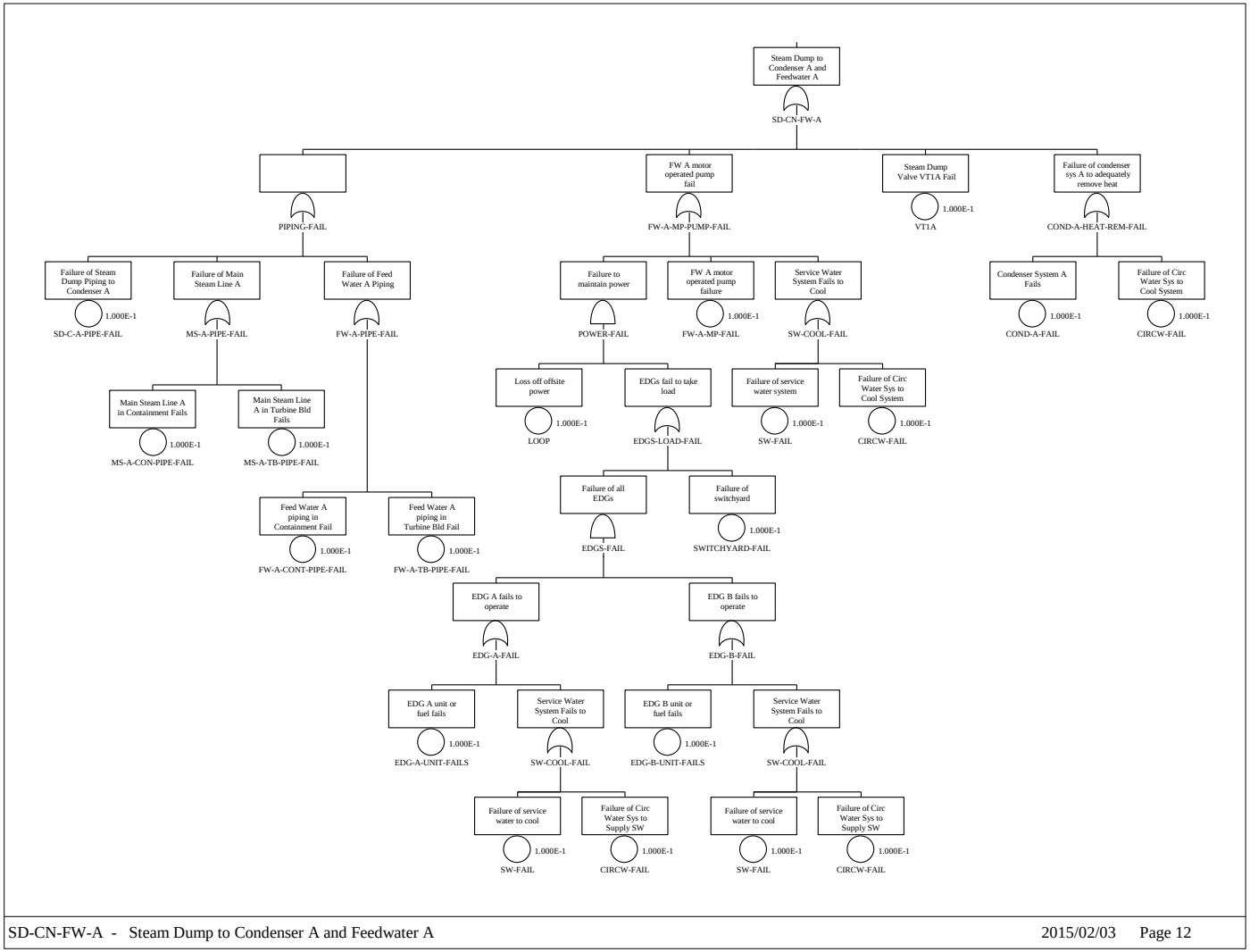


Figure 20: SD-CN-FW-A Fault Tree

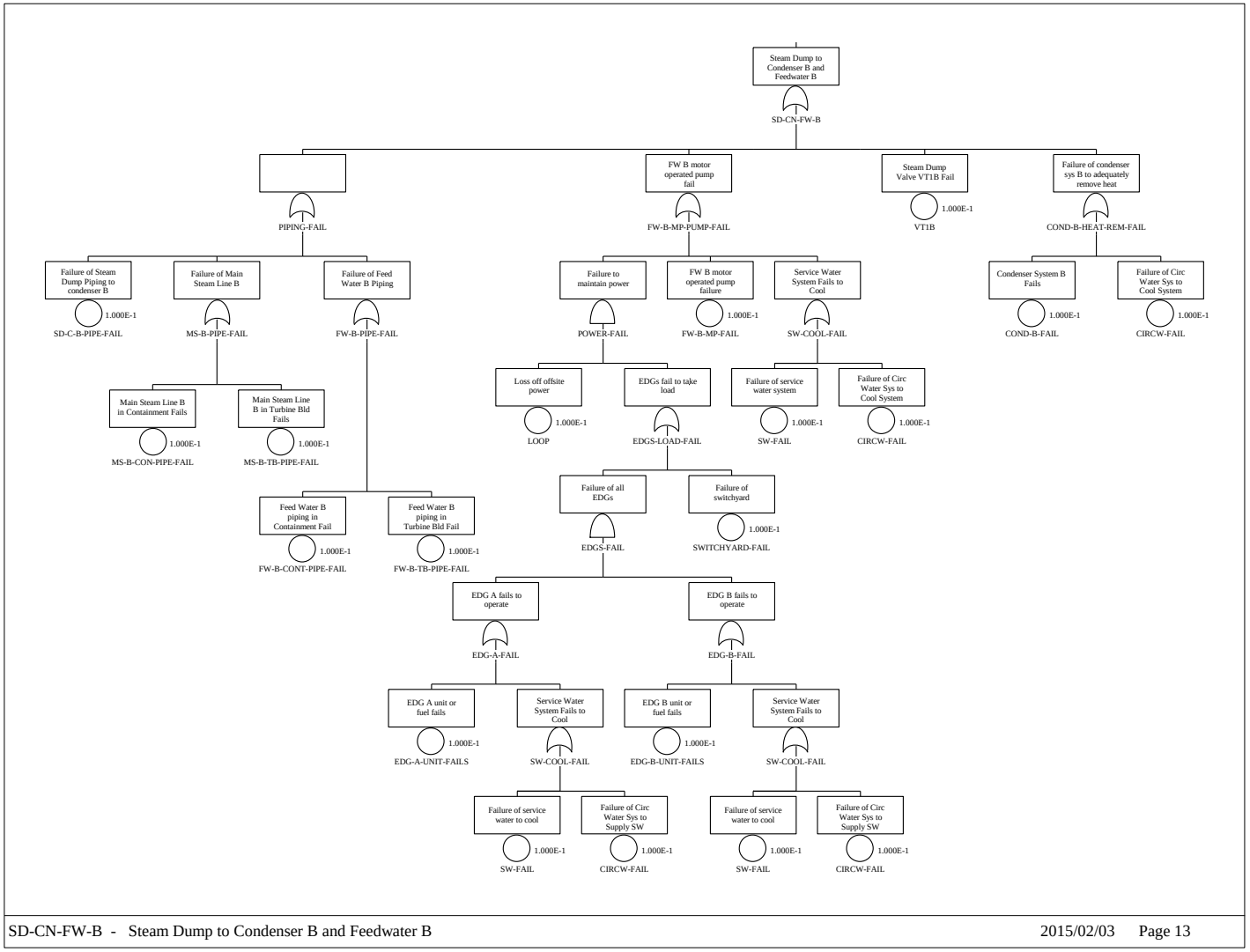


Figure 21: SD-CN-FW-B Fault Tree

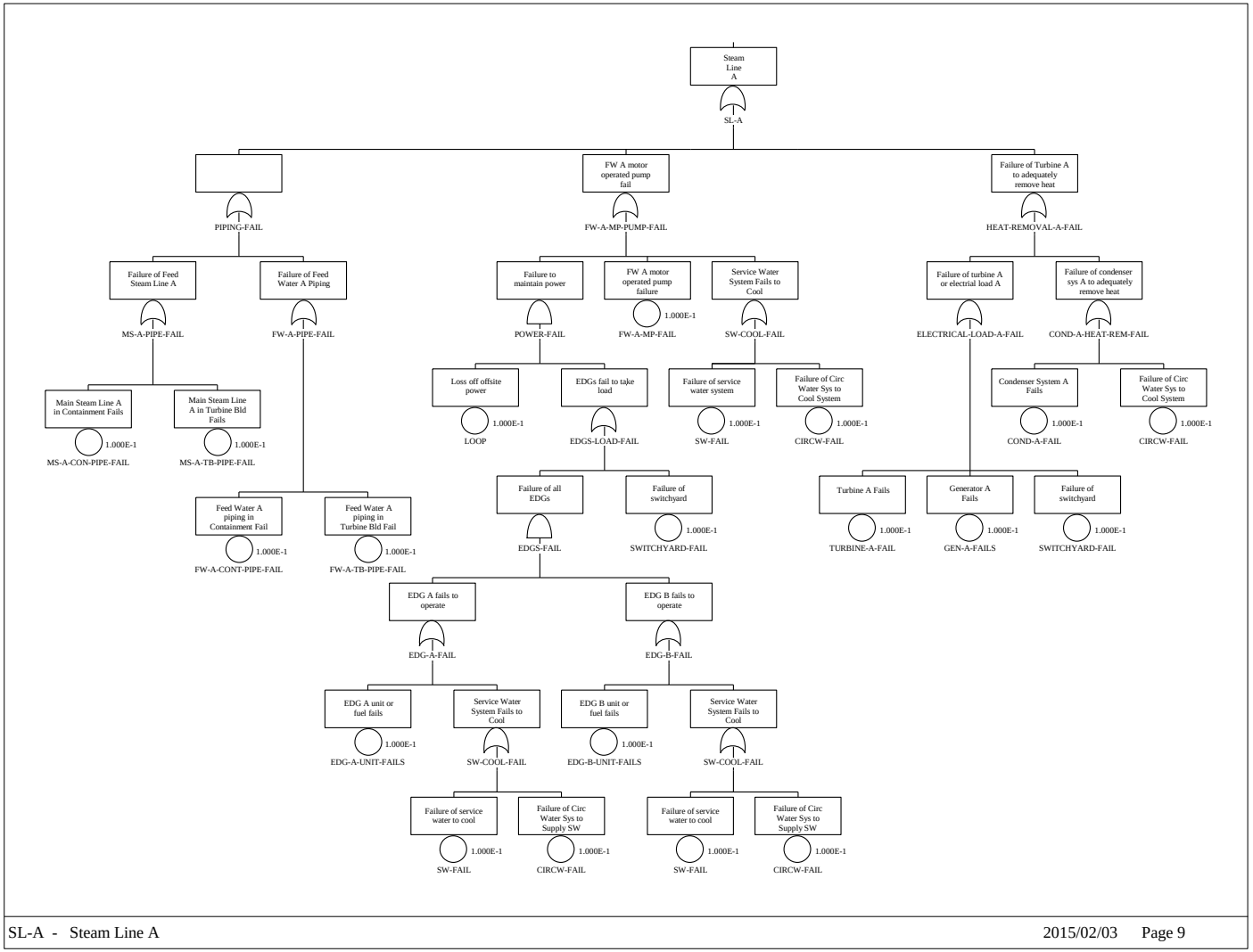


Figure 22: SL-A Fault Tree

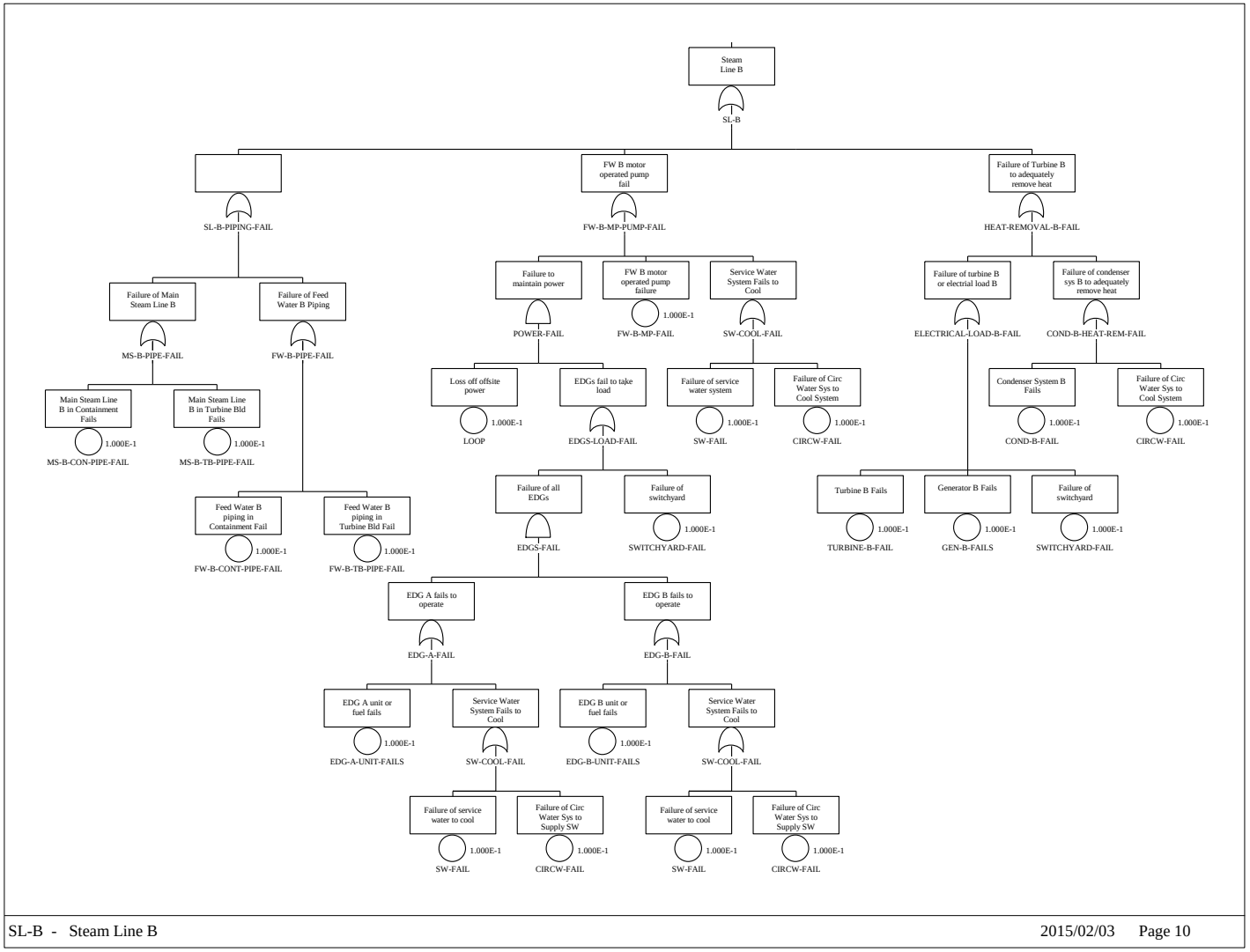


Figure 23: SL-B Fault Tree

Table 19: Element Build List after import from PRA data file

ID#	IDName	Name	Type	Location	Modes	Train	System	Cyber?	Flood?	Fire?	Operator?	Target Sets
7.01	RPS-TRIP											7, 201, 710, 1360, 3062, 3666
7.02	CCW-COMP-FAIL											7, 928
14.01	RCS-LBLOCA											14, 30
14.02	ACC-PIPE-INJ-LINE-A											14
14.03	ACC-PIPE-INJ-LINE-B											14
30.01	HHSI-A-PUMP-UNIT-FAIL											30
30.02	HHSI-B-PUMP-UNIT-FAIL											30
201.01	RHR-A-HX-UNIT-FAIL											201
201.02	RHR-B-HX-UNIT-FAIL											201
710.01	EDG-A-UNIT-FAILS											710
710.02	EDG-B-UNIT-FAILS											710
710.03	LOOP											710
928.01	SL-A-BREAK											928, 9757
928.02	COND-B-FAIL											928, 3062
928.03	EFW-A-MP-FAIL											928, 3062, 3666
1360.01	FW-A-MP-FAIL											1360, 3666
1360.02	FW-B-MP-FAIL											1360, 3666
1360.03	VT2A-FAIL											1360
1360.04	VT2B-FAIL											1360, 3062, 3666
3062.01	COND-A-FAIL											3062
3062.02	EFW-A-SP-FAIL											3062, 3666
9757.01	SWITCHYARD-FAIL											9757
9757.02	VE2A-FAIL											9757
9757.03	VE3A-FAIL											9757
9757.04	VS2A-FAIL											9757
9757.05	VS2B-FAIL											9757

Table 20: Element Build List with Complete Information Fields

ID#	IDName	Name	Type	Location	Modes	Train	System	Cyber?	Flood?	Fire?	Operator?	Target Sets
7.01	RPS-TRIP	Rx Trip	Rx trip		1,2,3,4		RPS	Y	Y	Y	N	7, 201, 710, 1360, 3062, 3666
7.02	CCW-COMP-FAIL	Comp. Cool Water	Cool Sys.	AUX	1,2,3,4,5,6		CCW	Y	N	Y	N	7, 928
14.01	RCS-LBLOCA	Large Break LOCA	LOCA	Cont.	1,2,3,4,5,6		RCS	N	N	Y	N	14, 30
14.02	ACC-PIPE-INJ-LINE-A	CL injection line A	Pipe	Cont.	1,2,3,4,5,6	A	SIS A	N	N	N	N	14
14.03	ACC-PIPE-INJ-LINE-B	CL injection line B	Pipe	Cont.	1,2,3,4,5,6	B	SIS B	N	N	N	N	14
30.01	HHSI-A-PUMP-UNIT-FAIL	High Pres Inj Pump A	Pump	AUX	1,2,3,4	A	SIS A	Y	Y	Y	N	30
30.02	HHSI-B-PUMP-UNIT-FAIL	High Pres Inj Pump B	Pump	AUX	1,2,3,4	B	SIS B	Y	Y	Y	N	30
201.01	RHR-A-HX-UNIT-FAIL	RHR Heat Exc. A	HX	AUX	1,2,3,4,5,6	A	RHR A	N	N	Y	N	201
201.02	RHR-B-HX-UNIT-FAIL	RHR Heat Exc. B	HX	AUX	1,2,3,4,5,6	B	RHR B	N	N	Y	N	201
710.01	EDG-A-UNIT-FAILS	EDG System A	EDG	EDG A	1,2,3,4,5,6		EDG A	Y	Y	Y	N	710
710.02	EDG-B-UNIT-FAILS	EDG System B	EDG	EDG B	1,2,3,4,5,6		EDG B	Y	Y	Y	N	710
710.03	LOOP	Loss of Offsite Power	IE		1,2,3,4,5,6		Power	Y	Y	Y	N	710
928.01	SL-A-BREAK	Steam/FW ln bk A	SL break	TB	1,2,3,4	A	MSSS A	N	N	Y	N	928, 9757
928.02	COND-B-FAIL	Condenser B	Condenser	TB	1,2,3,4	B	MSSS B	N	N	Y	N	928, 3062
928.03	EFW-A-MP-FAIL	EFW A motor pump	Pump	EFW A	1,2,3,4	A	EFW A	Y	Y	Y	N	928, 3062, 3666
1360.01	FW-A-MP-FAIL	FW A motor pump	Pump	TB	1,2,3,4	A	MSSS A	Y	Y	Y	N	1360, 3666
1360.02	FW-B-MP-FAIL	FW B motor pump	Pump	TB	1,2,3,4	B	MSSS B	Y	Y	Y	N	1360, 3666
1360.03	VT2A-FAIL	Steam-Atm valve A	Valve	TB	1,2,3,4	A	SD A	Y	Y	Y	Y	1360
1360.04	VT2B-FAIL	Steam-Cond valve A	Valve	TB	1,2,3,4	B	SD B	Y	Y	Y	Y	1360, 3062, 3666
3062.01	COND-A-FAIL	Condenser A	Condenser	TB	1,2,3,4	A	MSSS A	Y	Y	Y	N	3062
3062.02	EFW-A-SP-FAIL	EFW A steam pump	Pump	EFW Bld A	1,2,3,4	A	EFW A	Y	Y	Y	N	3062, 3666
9757.01	SWITCHYARD-FAIL	Unit Switchyard	Switchyard	Switchyard	1,2,3,4,5,6		Power	Y	Y	Y	N	9757
9757.02	VE2A-FAIL	EFW A SP valve	Valve	Cont.	1,2,3,4	A	EFW A	Y	Y	Y	N	9757
9757.03	VE3A-FAIL	EFW A transfer valve	Valve	Cont.	1,2,3,4	A	EFW A	Y	Y	Y	N	9757
9757.04	VS2A-FAIL	RHR A Inj line Valve	Valve	AUX	1,2,3,4,5,6	A	RHR A	Y	Y	Y	N	9757
9757.05	VS2B-FAIL	RHR B Inj line Valve	Valve	AUX	1,2,3,4,5,6	B	RHR B	Y	Y	Y	N	9757

Vita

Christopher Chwasz grew up in Oak Park, IL and attended Oak Park and River Forest High School where he developed an interest in the sciences. He attended the University of Michigan – Ann Arbor, and studied radiation detection under Dr. Zhong He. He received a Bachelor's of Science in Engineering with a concentration of Nuclear Engineering and Radiological Sciences in 2007. He accepted a position with Information Systems Laboratories in the Nuclear System Analysis division located in Rockville, MD. Christopher worked closely with the US Nuclear Regulatory Commission Office of Nuclear Security and Incident Response through 2012. He began his graduate studies at the University of Tennessee - Knoxville in 2011 in the Nuclear Engineering Department. He used experience gained working with the Nuclear Regulatory Commission to develop his Master of Science thesis under Dr. Steven Skutnik.