9-29-2015 12:00 AM

Design, Implementation, and Verification of a Reactor Protection System Using HFC6000

Michael V. Gverzdys, *The University of Western Ontario*

Supervisor: Jin Jiang, *The University of Western Ontario*

A thesis submitted in partial fulfillment of the requirements for the Master of Engineering Science degree in Electrical and Computer Engineering

DESIGN, IMPLEMENTATION, AND VERIFICATION OF A REACTOR PROTECTION SYSTEM FOR NUCLEAR POWER PLANT USING HFC6000

(Thesis format: Monograph)

by

Michael Victor Gverzdys

Graduate Program in Electrical and Computer Engineering

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Engineering Science

The School of Graduate and Postdoctoral Studies
The University of Western Ontario
London, Ontario, Canada

Abstract

Recently, a nuclear power plant physical simulator to support instrumentation and control (I&C) research has been constructed at the University of Western Ontario using industry-grade sensors and actuators. This platform, known as the Nuclear Power Control Test Facility (NPCTF), provides means to safely inject faults and examine their effects on the system. The NPCTF may be configured into a number of nuclear power plant (NPP) types, but focus has been placed on CANadian Deuterium Uranium (CANDU) type. In a CANDU based NPP, there are two independent and separated systems with decision-making units capable of actuating two shutdown systems. These units form the reactor protection system, and monitor critical system variables to ensure that they remain within safe operating limits.

For this work, in ongoing efforts to further improve the fidelity of the NPCTF, a dedicated reactor protection system has been realized. This system has been implemented through a United States Nuclear Regulatory Commision certified safety programmable logic controller (PLC), known as the HFC6000. This has been integrated with the NPCTF through a standard industrial interface, and performs monitoring functions and decision logic operations. The reactor protection system responds to contingencies by issuing trip signals to perform safety shutdown actions.

The designed system has undergone a full verification and validation (V&V) process. Nine CNSC design basis events have been considered under full-system testing, including the loss-of-coolant-accident and loss-of-reactor-control. The designed logic achieved a 100% success rate on 25 trials. Further, the implemented system produced no spurious trips during normal operations.

The relationship between CANDU type NPPs and the NPCTF has been established. The work has also concluded that the NPCTF is capable of replicating dynamic relationships among different variables in an NPP. Through V&V tests, , the designed logic, and implemented system using HFC6000 have been proven to be successful according to the safety system criteria from the Canadian Nuclear Safety Commission.

Key Words: Physical Simulation, Safety Systems, V&V, PLC, Shutdown Systems, Reactor Protection System

Acknowledgements

I wish to express sincere appreciation to my thesis supervisor, Dr. Jin Jiang. Without his guidance, expertise, patience, and dedication, this work would not have been possible. His leadership and inspiration have been essential in my studies. I would further like to thank Dr. Xinhong Huang for her support, friendship, and commitment to our research team.

Special thanks to HFControls for donation of their system. Sincere appreciation is given to Thom Shaefer, who gifted me countless hours of his time supporting this project. His humour and expertise shed light on my most frustrating hours.

I have deep gratitude to the UWO CIES team. Their endless support, both technical and non-technical, have been invaluable to me over the past two years. Elizabeth K.M. Tomaszewski, Devbratta Thakur, Syed A. Raza, and the entire team made my time during my master's work a deeply enjoyable and rewarding experience.

I could not have done this without those closest to me: my mother and father, Ingrid Thie and Sharunas Gverzdys, for their love, encouragement, and inexhaustible belief in me; Ariana and Marcus Gverzdys for celebrating my successes and relieving my disappointments in equal parts with humour; and Andrée Chartrand for her endless support, kindness, and grace. In particular, recognition is given to Tomas Gverzdys, who taught me to love science, pursue knowledge, and follow my dreams.

Above all, I am blessed to have worked with Drew J. Rankin. I would not have finished this work without his endless technical knowledge, mentorship, and friendship. He has inspired me in ways I cannot appropriately articulate.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

2oo3	2 out of 3
AECB	Atomic Energy Control Board
C-Link	Communication Link
CANDU	CANadian Deuterium Uranium
CCF	Common Cause Failure
CNSC	Canadian Nuclear Safety Commission
DCS	Distributed Control System
DPM	Dual Port Memory
EE	Equations Editor
EWS	Engineering Work Station
FMEA	Failure Mode Effect Analysis
HIL	Hardware In the Loop
HFC	HFC6000 Nuclear Safety PLC
HX	Heat eXchanger
I&C	Instrumentation and Control
ICL	Inter-Communication Link
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IRC	Inverse Response Characteristic
ISO	International Organization for Standardization
LOCA	Loss Of Coolant Accident
NPCTF	Nuclear Power Control Test Facility

NPEC	Nuclear Power Engineering Committee
NPP	Nuclear Power Plant
PDC	Programmable Digital Comparator
PES	Power Engineering Society
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
SDS1	Shutdown System 1
SDS2	Shutdown System 2
SPICE	Software Process Improvement and Capability dEtermination
SYS	HFC SYStems processor
USNRC	United States Nuclear Regulatory Commission
UWO	University of Western Ontario
V&V	Verification and Validation

Symbols and Nomenclature

$\boldsymbol{MR}$	Moderating Ratio
$\boldsymbol{\xi}$	Average Log Energy Decrement
$\boldsymbol{\sigma_s}$	Scattering Cross Section
$\boldsymbol{\sigma_a}$	Absorption Cross Section
$\boldsymbol{E_{high}}$	Initial Neutron Energy
$\boldsymbol{E_{low}}$	Required Neutron Energy
$\boldsymbol{N}$	Average Collisions Required
$\boldsymbol{P}$	Power of Reactor
$\boldsymbol{E_R}$	Energy Released in Fission
$\boldsymbol{N_d}$	Fissile Density Number
$\boldsymbol{\sigma_f}$	Atomic Cross Section
$\boldsymbol{\phi}$	Instantaneous Neutron Flux
$\boldsymbol{V}$	Volume of Reactor
$\boldsymbol{E_{incoming}}$	Neutron Energy before Collision
$\boldsymbol{E_{scattered}}$	Neutron Energy after Collision
$\boldsymbol{k_{ex}}$	Excess Multiplication Factor
$\boldsymbol{k_{eff}}$	Effective Multiplication Factor
$\boldsymbol{\rho}$	Reactivity
$\boldsymbol{A}$	Atomic Mass
C2	Heater Current
T2	Heater Outlet Temperature
L3	Pressurizer Water Level

L4	HX Tank Water Level
P1	Primary Loop Pressure
P2	HX Tank Pressure
F1	Primary Loop Flow Rate
CV	Control Valve
FV	Flow Valve

1 Introduction

Nuclear power plants (NPP) have a proven capability to produce reliable and clean power in large quantities. However, because both the energy density in the fuel in an NPP and its radioactive by-products, NPPs present an inherent risk in their operations. For these reasons the nuclear industry not only possesses a plethora of governing bodies and regulations, but treats safety as top priority during all phases of an NPP's lifespan. The ultimate foal of NPP safety is to prevent radiological releases [1]. Thus, safety continues to be an area of continual research and improvement within the industry.

A physical NPP simulator to support instrumentation and control (I&C) research has been developed in the Control and Instrumentation in Electrical Systems (CIES) group at the University of Western Ontario (UWO). This simulator, the Nuclear Power Control Test Facility (NPCTF), is capable of simulating a wide variety of faults safely and repeatedly [2]. The NPCTF therefore presents an ideal platform for prototype testing of a number of I&C apparatus, including verification and validation (V&V) of safety algorithms.

This thesis presents the development of a safety system for the NPCTF. This safety system is based on a Canadian Deuterium Uranium (CANDU) NPP. This chapter presents a brief introduction to NPPs, the relevant standards, and methods of testing, as well as outlining the objectives, contributions, and organization of the thesis.

1.1 NPP Basics

NPPs are similar in structure to all other type thermal generating stations [3]. The primary difference is the fuel choice: radioactive isotopes are 'burned', converting the mass deficiency of nuclear fission into energy [4]. The reactor and accompanying machinery handle

the maintenance, control, and extraction of energy from the ongoing critical nuclear reaction, while the remaining machinery follow generic thermal plant configurations.

As shown in Figure 1.1 [5], a CANDU NPP utilizes a two loop, two building design. The first building, aptly named ‘Reactor Building’, is vacuum sealed and houses the reactor, primary heat transport pumps, pressurizers (not shown) and steam generators. These three devices use heavy water (D_2O) as coolant for transporting heat from the reactor to the rest of systems and make up the ‘primary loop’.

The ‘second loop’ is mostly contained in the turbine building. Here, steam from the steam generators drives the turbines of generators. Multiple turbines are used for increased efficiency. Steam is condensed within a condenser and pumped (using auxiliary pumps) back into the steam generators.

The CANDU reactor uses natural uranium in its fission reaction [3]. The coolant is heated up to approximately 310^{o}C [3]. The coolant is kept in a liquid state by the pressurizer, which maintains pressures up to 11.05 MPa (g) [6]. The superheated, pressurized coolant is transported to the steam generator. There, the coolant passes through as many as 16,000 tubes, dissipating its heat and boiling the light water in the secondary loop. Afterwards, the coolant flows back into the reactor with flow maintained by the primary loop pump [6].

The secondary loop connects the two buildings. Light water steam from the steam generator runs through first high pressure then low pressure turbines. The turbines turn the rotor of the generator producing the end-product electric power. The steam collects and condensates in the condenser. The condenser utilizes an intake of cold water from an external

source, which in Canada is often a lake or sea [6]. The now liquid water is pumped back into the steam generator to begin a new cycle.

1.2 Safety Systems

Safety systems are utilized to prevent possible accidents. Principally, a safety system performs four major roles [7]:

1) Shutdown the reactor and maintain it in a safe shutdown condition
2) Remove decay heat from the fuel
3) Maintain a barrier to limit radioactive release to the public and plant personnel
4) Supply information necessary for the operator to monitor the status of the plant

Safety systems are divided into three groups based on the role that they perform: Shutdown systems (objective 1), post-shutdown systems (objective 2), and safety support systems (objectives 3 and 4).

The International Atomic Energy Agency (IAEA) [8] defines the reactor protection system (RPS) as the system responsible for maintaining a reactor within a safe operating region. It does this by producing a shutdown (called a 'trip') signal when one or more physical parameters enter an unacceptable range. This signal causes the shutdown systems to halt the reaction. CANDU plants possess two independent mechanisms for this; referred to as Shutdown System 1 (SDS1) and Shutdown System 2 (SDS2) [6].

.

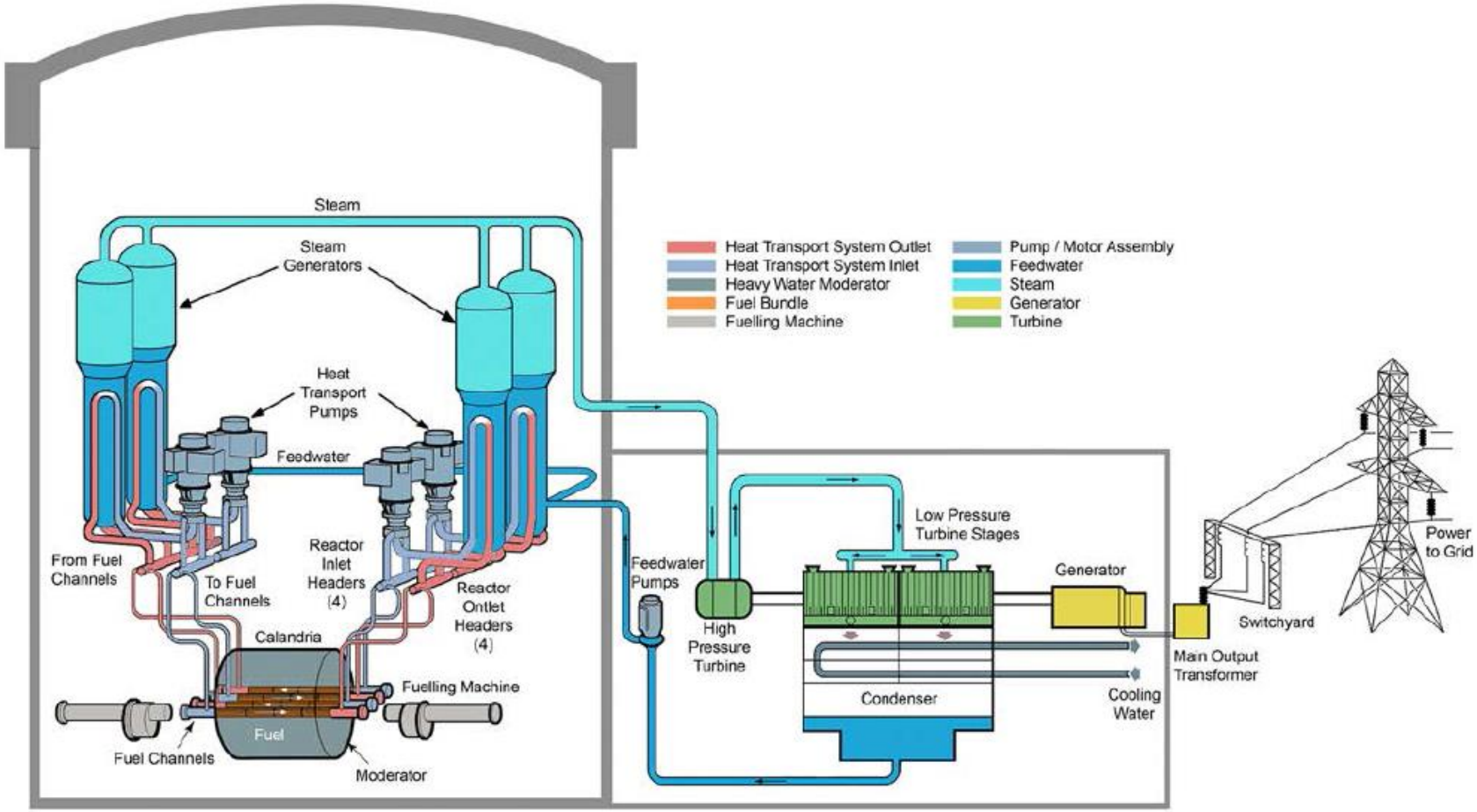

Figure 1.1: Configuration of a CANDU NPP

The portion of the RPS that makes the tripping decision is simply referred to as the 'electrical part of the RPS' [8]. The electrical part consists of two primary portions:

1) Analog Channels: These channels process mesasured crticial system variables and issue trip signals whenever some of these parameters exceed predetermined ranges
2) Logic Trains: These logical units receive information from the analog channels and determine through a voting scheme wheteher it is necessary to send a trip singal to the mechanical subsystem of the RPS that implement the actual shutdown actions.

In a CANDU NPP, this voting scheme is a two-out-of-three (2oo3) configuration such that two of the three channels must simultaneously signal unsafe conditions for a trip to occur [7]. This configuration requires two channels to falsely identify a problem simultaneously for a spurious trip to happen. 2oo3 thus allows each system to be pragmatically cautious while reducing the risk of spurious trip.

1.3 Nuclear Control and Safety Commissions

The international nuclear community cooperates globally through the IAEA, an autonomous organization established by the UN in 1957 [9]. The IAEA recommendations are meant to reflect the collective experience of the nuclear power community, though are not mandatory for IAEA member countries. Instead, IAEA members are free to adopt the standards by their discretion [10].

The IAEA has three stated missions [10]:

1) Assist its member states in the use of nuclear technology and science for peaceful purposes

2) Develop standards for nuclear safety and promote and achieve these standards in regards to human health and the environment
3) Verify through inspection that member states comply with the commitments under the Non-Proliferation Treaty

Another major engineering body, The Institute of Electrical and Electronics Engineers (IEEE), develops standards and methods for NPP's design and operations [11]. IEEE's main body for NPP technology is the Nuclear Power Engineering Committee (NPEC) of the IEEE Power and Energy Society (PES) [11]. NPEC protocol currently evaluates 29 categories of equipment before approving a design and validating its construction. These range from specific parts (#383 Cables, Splices and Connections) to capabilities of entire systems (#603 Safety Systems) [12], [13].

Potentially the most important identifier in the design of nuclear electrical systems is IEEE 1E designation, as adopted by the United States Nuclear Regulatory Commission (USNRC). 1E designates electrical systems related directly to safety [14]. The criteria for defining, designing, testing, monitoring, documenting, and more for 1E systems are outlined in the IEEE Standard 308 (2012) [14]. This standard is written and maintained by working group WG 4.1 – IEEE 308.

The International Electrotechnical Commission (IEC) is another major international body [15]. The IEC works closely with the International Organization for Standardization (ISO), the International Telecommunication Union, and the IEEE [15]. The IEEE and IEC signed a cooperation agreement in 2002 and since 2008 have performed joint technological development [16]. Guidelines relevant to nuclear engineering include IEC standards 62340,

61513, and 60880, which cover classification of common cause failures, safety instrumentation and control systems, and safety software respectively [17-19].

Standards are adopted or created at the discretion of an NPP's home country. The Canadian Nuclear Safety Commission (CNSC) (previously known as the Atomic Energy Control Board (AECB)) have ultimate authority in standards and licensing criteria utilized for Canada [20]. However, because Canada has signed into the IAEA, technical collaborations with inter-government organizations contribute to Canadian nuclear development [9]. The CNSC's credentials must be met or exceeded in all manners of design and operation before an NPP can be granted a license to operate in Canada [20]. This authority was installed to the CNSC by the Nuclear Safety and Control Act of 1997 [20]. Their standards are outlined in part by documents such as the SOR/2000-202 and AECB Requirements for Shutdown Systems R-8 policy statement [21], [22].

The CNSC does not specify technologies or methods; instead, CNSC's philosophy focuses on creating and enforcing high standards of performance and reliability [23]. The interpretation and burden of proof that these standards have been upheld is left to the licensee. In demonstrating their compliance, the licensee is free to choose whatever designs they deem appropriate [23].

1.3.1 Testing for Nuclear Applications

The high standards of nuclear commissions means certification requires significant time investment. This is especially true for computer based safety systems; systems whose failure rates are difficult to quantify through traditional methods [24]. The certification is difficult for several reasons: the volume of coding, manner by which tasks are carried out, verification once

on chip, means of failure, and more. This created an impact for the inclusion of digitally program devices into the industry [24].

One way by which this problem is relieved is through the use of simulators. Simulators aid in validation by demonstrating the capability of a system, digital or otherwise. Simulators are often able to simulate faults or other unusual circumstances, aiding in verification of safe system design and implementation. Simulators may be software, physical, or a combination of both.

1.3.2 Differences between Physical and Software Models

NPPs typically possess site-specific simulators for operator training. There are also private companies [25-27] capable of providing simulations for products seeking certification. These are software simulations however, and despite high accuracy models, are ultimately only models.

Software simulation requires the system to be tested to be physically connected to a simulator. The simulator interprets input signals, uses its model to change its internal states, and returns the appropriate response signals back to the system being tested.

Hardware-in-the-loop (HIL) consists of one or more physical components working in conjunction with software in order to provide a more accurate, model-free simulation of plant operations. Examples of physical components include mock steam generators, reactors, and more [28], [29]. Many of these undergo testing to ensure fidelity to the system that they are modeling. HIL testing is recommended by the IAEA and IEEE [30], [31]. HIL is particularly useful in safety-critical applications such as NPPs where it is not possible for on-line testing. HIL enables real-time simulation, thus permitting in-situ testing [28].

Physical simulators are an extension of HIL which minimize software components. Like HIL, they undergo testing to ensure fidelity. These provide online testing against real-world dynamics. The NPCTF is then, under this definition, a physical simulation of NPP for supporting I&C system studies.

The NPCTF presents a unique opportunity to test equipment process I&C. Because it uses low temperatures and pressures, one can simulate faults safely. Further, as fault insertion is designed into the mechanical structure and electrical control of the simulator, the faults inserted express a high degree of repeatability. The NPCTF is discussed in more detail in Section 3.1.

Such simulator is essential to evaluate logics and implementation issues associated with safety systems in an NPP. However, this has never been done before. The goal of this research is to investigate how a hardware ased simulator can be used to test safety systems and to validate & verify control logics.

1.4 Research Objectives and Scope

1.4.1 Objectives

The objectives for the current research are:

1. To design an RPS based on CANDU critical parameters' parallels to those on the NPCTF.
    - A comparison between CANDU safety logic and the operations of the NPCTF will be performed to ensure cross-compatibility

- An analysis of the NPCTF operating characteristics will be performed. This investigation will focus on each parameter's interaction with reactor power and the discovery of their normal operating ranges
- A complete safety logic scheme will be designed that monitors key system parameters under normal operations, while detecting faults and subsequently shutting down the NPCTF

2. To implement said aformentioned RPS using industrial grade safety PLC
    - The design will be coded into PLC logic such that it can be operated in real-time according to the requirements of that unit
    - The communication between the programed PLC unit and the NPCTF will be constructed as necessary for each system
    - Simulations will be performed to validate the logic and make necessary improvements
3. To validate the implemented design on the NPCTF
    - The implementation will be tested against design criteria determined during the initial stages
    - The fault injection capabilities of the NPCTF will be used to validate the designed RPS against CNSC standard design basis events as outlined in regulatory document R-8 [22].

1.4.2 Scope

Throughout this research, it is assumed that the validation of the NPCTF as a nuclear simulator is complete. The scope of this work will not include changes to the distributed control system or dynamics of the NPCTF. Instead, these are used under the assumption that they are

well performing and complete. The HFC6000, a certified nuclear safety PLC used for implementation, is likewise assumed to be correct in all aspects of its construction.

1.4.3 Solution Technique

To achieve these objectives, a number of steps must be taken. These steps are outlined in Figure 1.2. The work shall begin with a literature review of the relevant CANDU technologies and research. Following is a description of the NPCTF system. Once the system is described, the safety control algorithm design may begin. A Matlab simulation shall be created and continual improvements made on the design. Once simulation results are satisfactory, the implementation on HFC6000 may begin. The V&V process follows. This includes opportunities for improvement by retuning the algorithm. When all criteria have been achieved, the system will be fully realized.

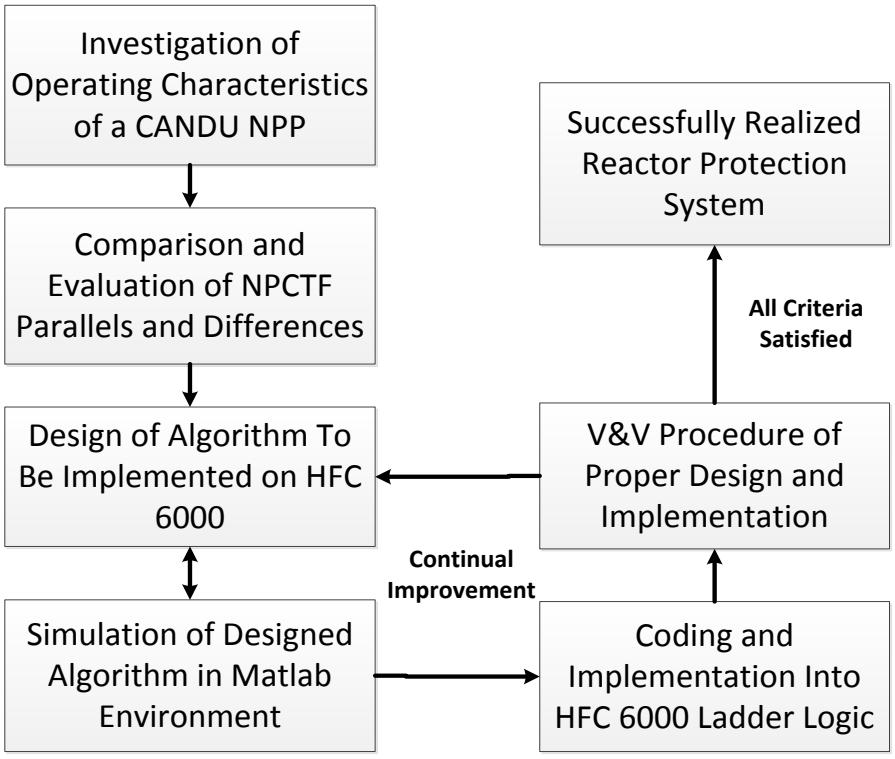

Figure 1.2: Thesis Workflow

1.5 Contributions of the Thesis

This thesis has made three major contributions:

1. The investigation of the NPCTF critical parameters is completed such that the relationships and dependence on the heater current are fully characterized
2. The cross comparison between NPCTF and CANDU operating signals and dynamics is performed to a degree capable of permitting the design of a RPS
3. An RPS is designed to operate on the NPCTF capable of achieving specified performance criteria: a perfect record in fault detection and no spurious trips during validation testing

1.6 Performance Criteria

The RPS must be capable of meeting design criteria. Thus, it is necessary that these criteria are specified such that they may be tested against. Though speed of the system is a performance measure of a RPS, this cannot be plausibly measured using the operations of the NPCTF. The RPS performs at rates too quick for the recording devices in question. However, given that the recording instruments operate at 1Hz, the performance criteria are therefore:

1. The system must be capable of detecting all faults inserted without exception. Specifically, these faults will be those outlined in CNSC regulatory document R-8
2. The system must not be the cause of spurious trips. The NPCTF, as the system under test, must be able to perform all permissible operations without interference from the RPS
3. All trips must occur within 1s. This will be measured by the NPCTF's internal log and defined as occurring from the recorded bypass to the recorded moment of complete cessation of heater operations

1.7 Organization of the Thesis

The thesis consists of six chapters including this Introduction. The second Chapter presents a literature review and essential background about CANDU reactors, nuclear safety, V&V methods, techniques for safety system design, and information about PLC including the HFC6000. The subsequent chapter contains an in-depth investigation of the NPCTF physical characteristics and operation. Chapter 4 is a detailed explanation of the safety system, including the method of designing set points, the functions of the software, and techniques used to verify its operation. Chapter 5 details the V&V process used: the reasoning behind the tests and the means to perform these tests. Here, the results of experiment trials are presented, analyzed, and discussed. Conclusions and future work are discussed in Chapter 6.

2 Literature Review

2.1 CANDU Reactor

2.1.1 Heavy Water Moderator

Certain design features of the CANDU reactor affect the design of relevant safety systems. The first is the CANDU choice of moderator: D_2O (AKA heavy water). Moderators are used to slow, through repeated collisions or 'scattering', the neutrons released from fission. This is done so that the neutrons are absorbed into other fissile atoms rather than passing through them at near-light speeds [32]. Heavy water possesses a large scattering cross-section, a small absorption cross-section, and large energy losses per collision [32]. Amongst moderators, heavy water possesses the best performance for the first two criteria and is surpassed by only light water in the third.

The average log energy decrement describes energy lost per collision. It is defined as [32]:

$$\xi = \ln \frac{E_{incoming}}{E_{scattered}} \tag{1}$$

where ξ is the average log energy decrement, and $E_{incoming}$ and $E_{scattered}$ are the energy levels of the neutron before and after collision. This value is almost entirely empirical as its value must be investigated through experimentation. However, a very rough estimation can be made as [32]:

$$\xi = 1 - \frac{(A-1)^2}{2A} \ln \frac{(A+1)}{(A-1)} \tag{2}$$

where *A* is the atomic mass. Using either observed or estimated values, it becomes possible to estimate the total number of particle collisions necessary to slow neutrons to appropriate velocities. Assuming each loss is near the average log energy decrement, the total number of collisions could therefore be calculated as [32]:

$$N = \ln \frac{E_{high}}{E_{low}} \Big/ \xi \tag{3}$$

where *N* is the expected number of collisions, and E_{high} and E_{low} are the starting and required energy levels. Ultimately, the fewer collisions needed to bring neutrons to appropriate velocities, the more easily the reaction will propagate.

The two other important factors are the scattering-cross-section and the absorption-cross-section [32]. A good moderator will have a much larger scattering than absorption cross section, such that neutrons are slowed down but not removed from the ongoing reaction.

Combining all three crucial characteristics is the moderating ratio, *MR* [32]:

$$MR = \xi \frac{\sigma_s}{\sigma_a} \tag{4}$$

where σ_s is the scattering cross section and σ_a is the absorption cross section. Observing the moderating ratio for commonly chosen moderators shows heavy water as the optimal choice.

Table 2.1: Effectiveness of Common Moderators.

Material	Ave. Log Energy Decrement	Necessary Collisions	Macro Slowing Power	Moderating Ratio
H_2O	0.927	19	1.425	62
D_2O	0.510	35	0.177	4830
He	0.427	42	9e-6	51
Be	0.207	86	0.154	126
B	0.171	105	0.092	0.00086
C	0.158	114	0.083	216

As mentioned in Section 1.1, CANDU NPPs use natural uranium as their fuel source. Natural uranium, being significantly more inert than the enriched uranium of light water reactors, forces improved moderator performance to maintain the ongoing reaction.

CANDU NPPs thus submerge and contain the reactor core in a vessel known as the calandria, as shown in Figure 1.1, and again in Figure 2.2. The calandria and primary loop are each filled with heavy water to act as the moderator and the coolant respectively. This maximizes the likelihood a released neutron will be slowed and return to the reaction. Heavy water thus allows CANDU NPPs to sustain a chain reaction without the need for enriched uranium.

2.1.2 Neutron Economy

The proportional growth and decay of the number of free neutrons is referred to as the ‘neutron economy’. Maintenance of the neutron economy is critical as the power of the reactor is directly proportional to the instantaneous neutron flux [33].

Explicitly, this is expressed as [33]:

$$P = E_R N_d \sigma_f \phi V \quad (5)$$

where P is the reactor power, E_R is energy released per fission (~200MeV), N_d is the fissile density number (~10^{24}/cm^3), σ_f is the cross-section of the atoms, Φ is the instantaneous neutron flux, and V is the reactor volume [33].

Released neutrons are divided into two categories based on their rate of release from their atom [33]. The first category, 'prompt' neutrons, come from atoms that decompose within 10^{-17}s after absorption of a neutron. 'Delayed' neutrons are those released from atoms that decompose more slowly. Delayed neutrons are often released in six distinct steps resulting from the incremental decay of U^{235} into Sr^{87} [33]. From the initial absorption, these delayed neutrons are released anywhere from 0.23s up to 55.72s. U^{235}, the fissile isotope used in CANDU, has a total delayed neutron fraction of 0.0065, or 0.65% [33].

This disparity demonstrates the importance of understanding the neutron economy when designing a reactor protection scheme. With most propagations taking less than 10^{-17}s, neutron economy can quickly advance to dangerous levels. Additionally, with some releases requiring nearly a minute, and many of the created radioactive by-products requiring much longer, reactors continue to produce heat long after being shut down.

Effective multiplication factor, k_{eff}, represents the ratio between the population of the current generation of free neutrons and the population of the next [33]. It thus follows that when k_{eff} is greater than one: the economy is growing, and when less than one: the economy is shrinking. The targeted value is one, referred to as 'unity', such that the reactor remains at steady state [33].

From k_{eff} the excess multiplication factor is defined as [33]:

$$k_{ex} = k_{eff} - 1 \tag{6}$$

where k_{ex} is the excess multiplication factor. From here, the 'reactivity', ρ, is defined as the ratio between the excess multiplication factor and the effective multiplication factor [33]:

$$\rho = \frac{k_{ex}}{k_{eff}} \tag{7}$$

such that increasing reactivity corresponds to positive values, and decreasing reactivity corresponds to negative values.

The most important factors effecting the reactivity are: fuel temperature, coolant temperature, coolant void, moderator temperature, reactor power, moderator poisons, and fission products [2]. However, long term considerations include depletion of fuel, active breeding, and accumulation of fission by-products (called reactor poisons) [33].

In a CANDU reactor, the reactivity in the core has to be under control at all times. Light water channels in the reactor may be filled to decrease reactivity, and boric acid in the moderator or cadmium control rods removed to increase reactivity [34]. These mechanisms are controlled by the reactor control system, ensuring that the reaction remains stable. When circumstance leads to the failure of these mechanisms, either due to their own loss of control or the presence of faults, it becomes the role of the RPS to intervene.

These details of reactor physics are presented to demonstrate the importance of the RPS. Two major issues arise from neutronic physics that the RPS must account for. First, the

ongoing decaying heat of delayed decompositions require sufficiently thorough and long lasting responses, and careful examination during start-up procedures.

Second, the exponential characteristic of the neutron economy necessitates rapid response as reactions may quickly 'run-away'. As a prompt neutron is released 10^{-17}s after initial absorption, generations of neutrons are released and absorbed rapidly. A positive value of ρ that persists for even short periods of time greatly effects the system, as reactor power, P, is directly proportional to the instaneous flux, Φ. This necessitates rapid action on behalf of the RPS, as the exponential growth ultimately implicates sudden and immense increases of reactor core temperature.

2.2 Reactor Protection Systems: Overview

All nuclear reactors possess the capability to release radiation, rupture to release superheated steam, and/or meltdown. While a reactor cannot explode in the manner of a nuclear warhead [35], the inherent risks of nuclear power generation demand that the RPS remain poised to place the reactor into a safe state at any moment. The two systems to perform this task are shutdown system 1 and 2, referred to as SDS1 and SDS2. These are controlled by monitoring safety systems. Safety systems are not involved in the control of the NPP. Instead, they monitor the critical parameters of the NPP, alert operators to dangerous conditions, and determine when an intervention is necessary. The logical configuration of an NPP is shown in Figure 2.1.

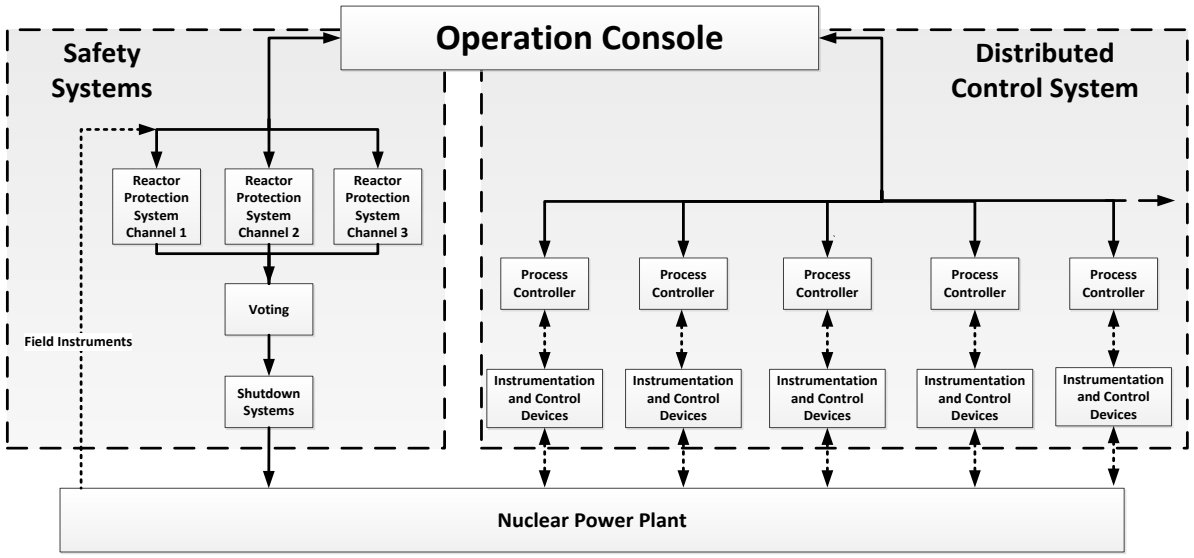

Figure 2.1: Safety Systems and Control Systems of a Nuclear Power Plant

2.2.1 Shutdown Systems 1 and 2

Each SDS is required by law to be independently capable of halting the nuclear reaction [36]. Also, their operation must not interfere with the capability of the other. The systems must individually achieve an unavailability $1/1000^{th}$ of a year annually. As such, their combined unavailability is one in a million, or 10^{-6} [22]. This allots just 8 hours annually per system, including maintenance, full system testing, or any off-line operations.

SDS1 is a group of 32 shutdown rods capable of immediately stopping the nuclear reaction through the absorption of neutrons [37]. Without these neutrons, the nuclear reaction fails to propagate and the reactor ceases to produce as much heat. These rods are a cadmium alloy, coated in stainless steel for strength [37]. When the cadmium atom absorbs a neutron it produces only a photon in response [38]. This photon may be absorbed but the reaction has ultimately been interrupted.

The cadmium rods are positioned above the reactor core, held by electromagnetic clutches or magnetically coiled springs [37]. This can be seen in Figure 2.2. Gravity and/or spring power rapidly forces the rods into the reactor core when released. All 32 rods are inserted within 2 seconds [38] and possess enough negative reactivity that even the two most effective rods may fail to insert with no consequence [33].

SDS2 is a liquid neutron absorber [37]. This is typically referred to as 'reactor poison' [37]. The reactor poison is considerably more destructive than the shutdown rods and its effects on the reactor core can only be undone through special means. The reactor poison is a gadolinium nitrate ($GdNO_3$) mixture which, like cadmium, acts as a neutron absorber [37].

The gadolinium nitrate is kept in tanks adjacent to the reactor [37] as shown in Figure 2.2. These are kept pressurized through the helium tanks shown directly above the $GdNO_3$ tanks. When necessary, SDS2 releases the normally open valves at the bottoms of the poison tanks. Under the pressure provided by the helium tank, reactor poison is injected into the moderator [37]. Theses valves are high reliability [22] and designed to be normally open (that is, spilling into the moderator) [37]. The safety system is thus actively keeping the poison out of the reactor. This is another fail-safe design such that the failure of the safety or shutdown system defaults to injecting poison into the reactor.

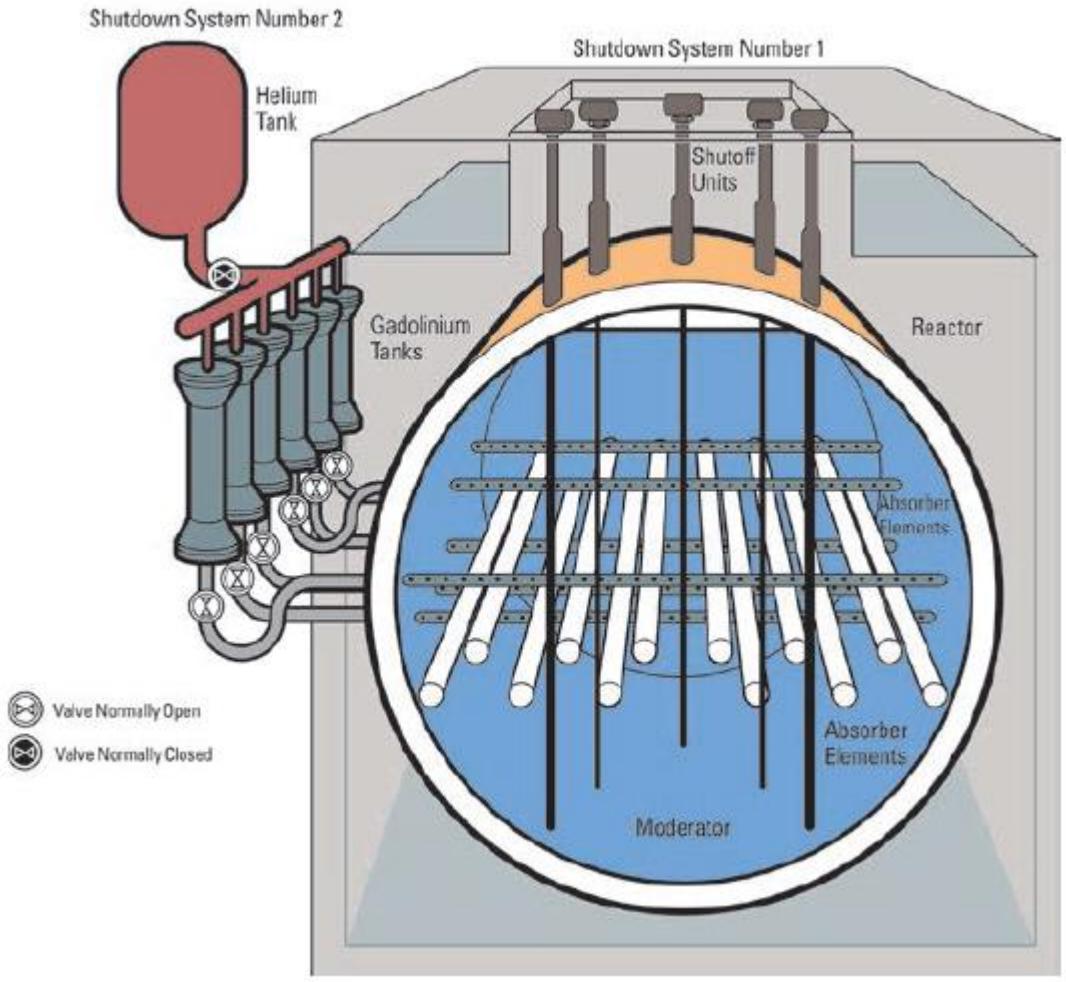

Figure 2.2: CANDU Shutdown Systems

The gadolinium rods of SDS1 are capable of being withdrawn from the reactor core via chains, while SDS2 must be laboriously cleaned from the moderator [37]. Because of this, the two systems are staggered in actuation. It is preferable SDS1 handles the shutdown individually as recovery is faster and less expensive. Thus, SDS1 typically posesses more conservative set points so it remains first to actuate [37]. Though both systems are available, SDS2 is utilized as a last resort.

2.2.2 Safety Systems

Safety systems are responsible for initializing the shutdown of the reactor (known as a 'trip') through the SDS [39]. CANDU utilizes at least three safety systems to control the two SDS. The safety systems initialize trips collectively by utilizing two-out-of-three (or 2oo3) voting logic, allowing each safety system to be prudently cautious without risking spurious trip.

The safety systems make judgements through monitoring of trip parameters [39]. Safety systems initialize trips when parameters reach their respective trip thresholds. Determining trip thresholds is discussed in section 2.4.

Safety systems have gone through four major generations [40]. The first generation utilized relay logic and operator interfaces consisting of mounted meters and lights in the control room. Operations were recorded with multipen trend recorders and operators controlled the plant through pushbuttons and hand switches.

The next generation began with the introduction of monitoring computers [40]. These computers did not change the NPP's circuitry or much of the interface, but allowed data manipulations, statistical checks, and comparisons to be generated. This information could be displayed to the operators [40]. The computers increased the capability to record plant operations and could more easily track trends. Subsequently, early warning logic was implemented to warn of impending trip conditions.

Programmable digital comparators (PDCs) were the first to replace analog devices [39]. Instrumentation remained analog and interfacing tools remained unchanged, but signal comparisons, decision making, and trip initiation was now digital [39]. This change was

conservative: neutronic trips did not migrate to digital for safety concerns [40]. However, PDC's made digital logic evaluation and process trips possible.

Now, fully computerized shutdown systems are possible. Instrumentation remains analog though monitoring, testing, logic, and display are fully digital [40]. CANDU safety systems utilize 15 computers between the two SDS, each with specialized tasks including monitoring parameters, tripping, display/testing, and monitoring the other computers [40].

Modern safety systems attempt to minimize unnecessary reliance on software. Failure of any aspect of the software must be fully understood with reliability measures (ex. error checking) included. Darlington, as an example, utilizes over two-thirds of its safety system's code to error check the implemented logic [39].

2.3 Design Methods of Reactor Protection Systems

A safety system is defined as the system responsible for autonomously initiating shutdown in an NPP [32]. Conversely, the SDS is the body of mechanisms that are responsible for carrying through with that task [40]. Thus, it is the safety system which holds the logic, processes the system parameters, and discerns if and when a trip is necessary.

The importance of this task begets a number of common design criteria. Other than the vigorous testing that must be performed during V&V, engineering principles are utilized to mitigate issues that arise due to environment and failures of foresight [41].

2.3.1 Key Monitoring Parameters

Safety systems typically refer to the choice of monitored system variables as the safety parameters. This term gets extended onto the variables themselves, such that critical variables

are likewise refered to as safety paratmers. CANDU safety algorithms often examine a similar set of parameters. These parameters are chosen due to their proven capability of detecting faults or abnormalities in the CANDU design [37]. Common parameters for SDS1 are listed in Table 2.2 along with which conditions abnormalities in those parameters could indicate [37].

Table 2.2: Common CANDU Safety Parameters.

Tripping Signal	Common Cause
Neutron Flux Level – High	Reactor power level too high
Neutron Rate Log	Power change too quick, unstable reactor
Steam Generator Level – Low	Loss of heat sink
Feed water Line Pressure – Low	Loss of heat sink
Pressurizer Level – Low	Loss of coolant
Primary Line Pressure – High	Reactor power too high for eat sink
Primary Line Pressure – Low	Poor coolant flow
Primary Line Flow – Low	Poor coolant flow
Reactor Building Pressure – High	Containment break
Moderator Level – Low	Reactor instability
Moderator Temperature – High	Cooling issue. Reactor power level too high
Manual Trip	Discretion of operating crew

When designing the NPCTF's safety algorithm, these parameters were mirrored in order to retain the CANDU parallel. Referencing Figure 3.1 in section 3.1, the equivalents in the NPCTF for the parameters in Table 2.2 are shown in Table 2.3.

Table 2.3: NPCTF Equivalent Signals.

CANDU Critical Signal	NPCTF Equivalent
High Neutron Power	None
High Rate of Rise of Neutron Power	None
High Coolant Pressure	Primary Loop Pressure (P1)
Low Coolant Pressure	Primary Loop Pressure (P1)
High Building Pressure	None
Low Steam Generator Level	HX Tank Level (L4)
Low Pressurizer Level	Pressurizer Level (L3)
High Moderator Temperature	Heater Outlet Temperature (T2)
Low Coolant Flow	Primary Water Flow (F1)
Low Steam Generator Pressure	HX Tank Pressure (P2)
Manual Shutdown	Manual Release Button

Because the nuclear reactor is simulated by a heater on the NPCTF, a number of CANDU parameters relating to neutron flux and the reactor building possess no NPCTF equivalent. However, the NPCTF still possesses equivalents for 8 of the 11 shutdown signals. This will be discussed in greater detail in section 3.1.

Because the redundant safety systems must still be diverse; safety systems monitor different sets of parameters, though there exists some overlap between them. An example set of parameters commonly used for SDS2 are listed in Table 2.4, along with failures they could indicate [37].

Table 2.4: Common CANDU Safety Parameters.

Signal	Common Cause
Neutron Power – High	Reactor power level too high
Neutron Rate Log – High	Power change too quick, unstable reactor
Primary Line Pressure – High	Loss of flow, heat sink failure
Primary Line Pressure – Low	Leak in primary
Reactor Building Pressure – High	Steam line break
Steam Generator Level – Low	Steam/feed water line breaks
Pressurizer Level – Low	Leak in primary line
Pressure Differential in Primary – Low	Flow blockage/failure
Steam Generator Pressure – Low	Steam line break

These signals are equally valid in designing the safety algorithms to protect the plant. However, because it is preferable to initiate the destructive SDS2 after SDS1, the set points for initiating a trip through SDS2 are slightly less stringent [37]. Regardless, the redundancy introduced by diverse the SDS and their respective logic increases overall system reliability. The same principle used in the utilization of triplicated (or more) safety systems [42].

2.3.2 Redundancy

A common CANDU safety design is two-out-of-three (2oo3) triplicated logic. This requires two of the three safety functions to call for a trip before one can occur [42]. This methodology possesses a number of operating benefits [42]:

- Allows a single system to be tested while the other two systems remain redundant and in operation
- Should a system fail it automatically votes to 'trip'; neither compromising safety nor resulting in a spurious trip
- Allows operators to view read-outs from each safety system, clearly showing when one system possesses an anomalous reading
- Permits the tightest possible parameter bounds without excessive risk of initiating spurious trip

Triplication is not applied only to safety systems. Many sensors and other instrumentation devices make use of triplicated redundancies in order to minimize errors [35]. These redundancies may even take place at the circuit level, where primary and secondary calculations are performed on separate processors [43]. If the calculations by two processors do not match, chip error protocol is utilized. If the error continues, the device recognizes a malfunction and performs predetermined actions [43].

Darlington's redundant safety systems are fully computerized [39]. Darlington's safety system possesses three groups of computers, each monitored separately by independent watchdog devices [9]. The redundancy of three groups prevents errors while the independent watchdogs ensure errors that do occur are immediately recognized [39]. Additionally, of the

12,000 words that make up the trip software, over 8,000 (2/3 of the total) are used purely for self and cross checking the results of any calculation [39].

2.3.3 Diversity of Design

Common cause failures (CCFs) are antagonistic to redundancies [17]. CCFs are events that result in failures across several systems [17]. Because CCFs by definition affect multiple systems, they render redundancy frivolous [17]. A simple example is a power surge that results in a measurement error by each system. CCFs are a principle concern to safety design because they represent a possibility that all safety systems could fail from a single, unexpected source [17].

Because CCFs cannot be predicted, the best protective measure is diversity of design [17]. Diversity is systematically approached so that redundant or complementary systems have as little in common with one another as is practically possible [17]. Theoretically, diverse systems accomplishing their tasks with differing tools, methodologies, and equipment may cause more total failures, but these failures will be from different causes and happen at different times [17].

Diversity is a standardized IAEA concept. Many safety standards include diversity as a necessary aspect of safety critical systems [19], [44]. In particular, the IEC 60880, 62340, 61508-2 (parts 2, 3, and 7) as well as the IAEA NS-G-1.1 and 1.3 form part of the international community's criteria on diversity in NPPs [45], [46].

The aforementioned standards possess requirements in the application of diversity as well as minimum standards in quantized measures of the principle. Some, but not all of these standards contain further requirements stating which systems must have diversity, the types of

redundancy that apply, and recommendations on assessment [45], [46]. Detailed techniques in the evaluation of the systems is discussed in NUREG-7007, a referenced but non-standardized approach to diversity evaluation [47].

In general, diversity is realized from seven applicable vantages [47]:

1) Design: Methodology in approaching a task or problem
2) Equipment Manufacturer: To insure another company's CCFs don't enter the NPP
3) Logic Processing Equipment: To account for the inherent weaknesses of all types
4) Function: The means by which tasks are carried out
5) Life-Cycle: Stresses or environmental factors common between systems
6) Signal: In line, instrument, and when applicable: the signals themselves
7) Logic: The implemented software and machine reasoning, be it µP based, ladder, or otherwise

Evaluation of diversity in redundant systems has several options. The most used methodology is NUREG-A as found within the NUREG-7007 [47]. Other methods include check-list based, RBD (or MM) based, graph-model based, and those which derive from probabilistic metrics [49].

An important concept in these methods is the difference between inherent and intentional diversity [49]. Intentional diversity is using the same technology or methodology in a different way for the explicit introduction of diversity. Contrarily, inherent diversity is completely different technologies or approaches to a problem, which would be naturally diverse [49].

When choosing between separate options, the IAEA insists the selection of the most diverse designs [48]. However, the IAEA recognizes that other factors (such as complexity, cost, and maintenance) may be considered.

2.4 CANDU Shutdown Logic

As discussed, the CANDU shutdown logic is divided between conditional and absolute trips. Conditional trips are armed when reactor power is at greater than 2% of maximum [37]. At low reactor power, the conditional trip parameters are not critical to safety. Absolute trips remain armed at all times. The general logical structure of CANDU shutdown logic is shown in Figure 2.3 [37].

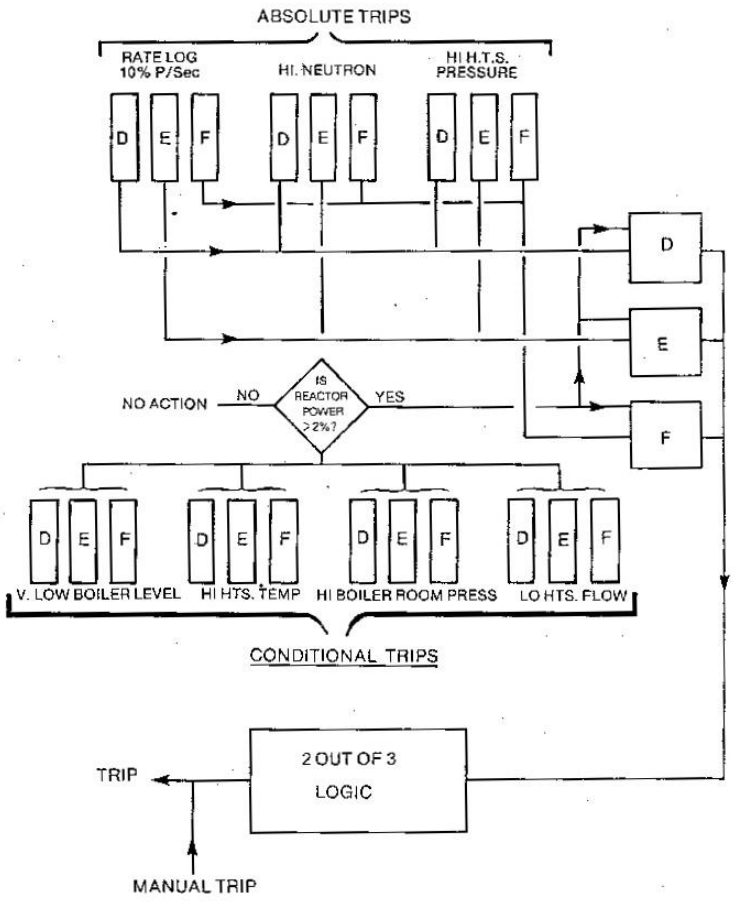

Figure 2.3: CANDU Shutdown Logic

Presented in Figure 2.3 are 7 of the shutdown thresholds. Each SDS utilizes three separate and independent channels (marked D, E, and F for SDS1, and G, H, and I for SDS2). The triplicated measurements work with 2oo3 logic, requiring two channels to exceed setpoints before a trip is initiated and reducing the possibility of spurious trip. These channels are exclusive to the safety systems [37].

Trip thresholds are separated for SDS1 and SDS2, with SDS2 designed to operat at higher setpoints [37]. However, these thresholds are designed in 'fail-safe' such that they are actively preventing the SDS from acting. Upon loss of signal from the safety systems, the SDS will activate to halt the reaction [37].

2.5 Trip Set-point Determination

The safety system, using the critical operating parameters, monitors the system for if and when breaches of predefined thresholds occur [1]. These thresholds are chosen such that even in worst case scenarios the SDS remain capable of reversing the supercriticality of the reactor core. An improperly placed threshold may result in system damage, release of radiation, or worse [50].

Threshold determination fundamentally begins from the understanding that an NPP may produce undesired effects [51]. All of these effects may be grouped together under the term 'damage'. The point at which a system parameter results in damage is referred to as the 'safety limit'. Thus, safety limits should never be met or breached in order to prevent the occurrence of damage [51].

As shown in Figure 2.4 [52], a safety margin is the breadth given to a safety limit even in the worst case scenario. For a rising fault (i.e. one by which the parameter causes damage

through a very high value), the safety margin is maintained by an ‘acceptance criterion’ at its base [52]. The acceptance criterion is the designed maximum value of the parameter. The RPS is therefore designed to prevent the parameter from ever breaching the acceptance criterion. If a parameter is halted before reaching its acceptance criterion, the safety margin is said to be ‘preserved’ [52].

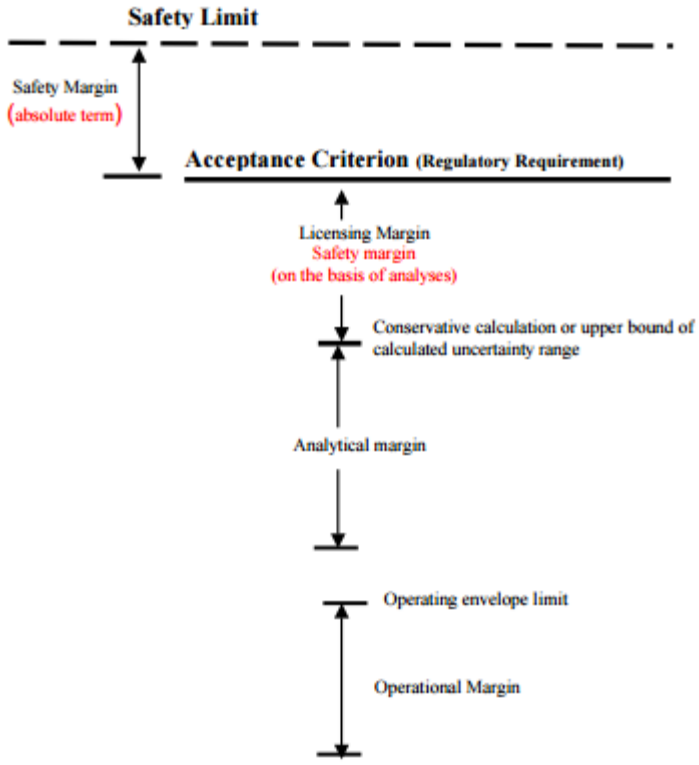

Figure 2.4: Definition of Margins in a Nuclear Power Plant.

Preservation of the safety margin requires the reactor to shut down well before the acceptance criteria is met. The parameter value at which action is taken is referred to as either the tripping set point or the tripping threshold. The tripping set point (labelled as the ‘operating envelope limit’), the safety limit, and acceptance criterion additionally utilize significant uncertainties are shown in Figure 2.4. Uncertainties originate from many sources, as discussed in the next subsection.

The decision behind the tripping threshold is mostly determined through the simulation of a worst-case-scenario. This scenario is a ‘design basis event’ [53]. Several design basis events must be utilized in each safety system design. The most infamous of these is the large loss-of-coolant-accident (LOCA).

The design basis LOCA is a complete shearing of the coolant inlet pipe immediately before the reactor. This results in coolant being rapidly drained from the calandria, a massive pressure loss, and consequent overheating of the reactor [53]. The large LOCA as a design basis event requires the swiftest response, theoretically resulting in the most conservative tripping set points [53].

Using the design basis event, engineers rely on modelling and simulation to evaluate the tripping set point. These are heavy calculations that rely on high accuracy modelling and thorough understanding of uncertainties. Uncertainty plays such a large role in the calculation of tripping set points that the IAEA publishes recommendations on uncertainty investigations. Historically, uncertainty is treated as pessimistically as possible in order to maximize safety [52].

2.5.1 Uncertainty Measurements and Calculations

Tripping set point determination continue to be an area of improvement and research in nuclear design. New methodologies have been proposed, tending to focus on the improvement of modelling and computations [54-56].

The unique aspects of new methodologies tend to be the means by which uncertainties are handled in simulation. Design basis events of simultaneous multiple failures, compounded with new theories of material, equipment, and operator failure began to drive conservative

estimates to below normal operating envelopes. As such, new statistical approaches, such as 'best-estimate' became necessary.

The CNSC accepts best-estimate evaluations that utilize reasonable approximations of operating conditions. Best-estimate embeds uncertainties into measurements and simulations and presents statistical ranges of outcomes. Best-estimate methods now make up the general methodology of tripping threshold determination in Canadian CANDU [57], [23]. The CNSC's best-estimate methodology is discussed in section 2.5.

Notably, best-estimate is very similar to the USNRC proposed methodology: Code Scaling, Applicability, and Uncertainty (CSAU) evaluation. Proposed in NUREG/CR-5249, CSAU uses statistical modelling of uncertainties [58]. Uncertainties are carried through the simulation of the design basis event, remaining a statistical distribution of possible outcomes.

One other notable methodology of uncertainty estimation is the 'partially-conservative' methodology [59]. The partially conservative methodology is a mathematically simplified means to evaluate the uncertainty of the NPP measurements and models. Often, the partially-conservative approach requires only a single calculation to be made for uncertainty. In an example given [59], this methodology produced similar results to a much more complex best-estimate evaluation. However, this methodology is not always applicable. A complete analysis through best-estimate is subsequently required in scenarios when this methodology cannot be utilized.

2.5.2 Methodologies without Design Basis Events

The design basis event is the most prevalent means of set point determination. By protecting against the worst-case scenarios, less severe events are assumed to be protected

against. This approach is taken as an NPP has too many fault and damage scenarios to simulate and evaluate exhaustively.

However, the IAEA recognizes that the safety margin may not be possible to calculate in some scenarios [52]. This obstacle can be circumvented by the demonstration that these incalculable situations are less severe (and thus under the umbrella) of the design basis events. These scenarios must still be evaluated to demonstrate that their presence will not increase the risk or consequences of other events. This may be done qualitatively if quantitative arguments are impossible [52].

There are also probabilistic safety targets. These complement deterministic analysis with technical judgement and experience [52]. These are utilized when safety margins cannot be explicitly determined and must be evaluated statistically. Probabilistic-safety-margins thus replace traditional safety margins, defined as the breadth maintained between the safety target and acceptance criterion.

There have been investigations to evaluate 'worst-than-reasonably-imaginable' scenarios [60]. These 'Beyond Design Basis Events' follow the same principles as the design basis event, but place the NPP in a worse scenario that can be reasonably encountered. These assume faster temperature increases, instantaneous coolant losses, and other conditions that are not perceivably possible. This methodology seeks to protect NPPs from events not yet encountered or imagined [60].

Vigorous statistical analysis of tripping set point determination may be done using extreme value statistics and Monte Carlo simulation [61], [62]. Because these rely on statistical analysis, they utilize CNSC adopted ISA '95/95' principle: the 95^{th} percentile worst case with

95% confidence [63]. These methodologies are computationally heavy but intrinsically generate confidence levels in set points they determine.

2.6 Best Estimate and Uncertainty Analysis

Canadian CANDU traditionally utilized the Limiting Operating Envelope (LOE) methodology [23]. This was a conservative approach that focused on worst case scenarios. The base assumption is that every key parameter is simultaneously operating at their worst case value for the event, even when this is not possible. A number of deterministic assumptions are also utilized [23]. These include simultaneous power losses, total failure of an SDS, partial failure of the other, and more. The LOE method thus builds an envelope of safe operations for the key parameters.

Recently, CANDU plants in Canada have moved towards the Best-Estimate and Uncertainty Analysis (BE+UA) methodology [23]. This has a number of benefits including

- More realistic predictions of plant behaviour, increasing confidence in predictions
- Resolve many outstanding safety questions by verifying their benignity
- Utilizes a more narrow range on parameters used in code validation
- Realistic plant behaviours breed familiarity for operators in diagnosing events
- Makes use of past analysis results, permitting incrementally improved analysis
- Potential to relax certain operating parameters

The BE+UA code requires sufficient certification and demonstration of prudence in order to be accepted by the CNSC. The methodology works with a number of generalized steps [23]:

(1) Identification of the facility, event of interest, and acceptance criteria

All relevant traits of the facility, including its operating state, the performance of its equipment, and location must be specified. The analyzed event must be completely identified. This includes postulated initiating event, sequence of assumed failures, and actions of operators. At this point, the acceptance criteria must also be stated with justification. It must be demonstrated to the CNSC that all threats posed have been covered. Validated models must be available to facilitate the BE+UA method for the selected criteria.

(2) Important phenomena and key parameters

Important phenomena must be identified and adequately modeled by computer codes. The parameters are ranked according to importance to the event. Uncertainty and sensitivity must be considered when ranking parameters [37].

High ranking parameters may use statistical uncertainties as they propagate through the code, or may use conservative values including the 95/95 principle [37]. Medium parameters are to be placed at their conservative values and low ranking parameters may be handled in any method.

(3) Analytical tools

The analytical codes used must satisfy the CNSC's criteria by demonstration of adequate modeling of important systems, phenomena and equipment. Code must demonstrate accurate and stable algorithms and verified interfaces for data transfer. Scaling must documented and verified. Outputs of all sections of code that are either acceptance parameters or the input of another code must include their bias and variance at the 95 percent confidence level [37].

(4) Deterministic assumptions

Deterministic assumptions introduce a measure of conservatism by postulating multiple failures and worst case scenarios. Deterministic assumptions are to be included and documented. Examples include LOCAs at worst case locations rather than most likely, crediting only one SDS with proper functioning, partial failure of shut-off rods, etc [37].

(5) Analysis input parameters

For every analysis, each relevant design and modeling parameter must be discovered. The size of the sampling set required to achieve the pre-determined confidence levels on the parameter characteristics (standard deviation, type of distribution, etc.) must be determined and realized. Equipment testing frequency must be decided to capture trends, covariances, and operational data, especially the effects of ageing [37].

If operational data is to be pooled, it must be demonstrated that the other unit, even if it is from the same facility, must be free from systematic differences. This includes design, equipment, and operating procedures. Only information gathered from the same operating state being analyzed is applicable [37].

(6) Quantification of uncertainties

There are three major sources of parameter uncertainties:

- Operational uncertainty results from variability, trends, measurement errors, instrument drift, etc.
- Design uncertainty results from allowances, fabrications tolerances, measurement errors, test and calibration accuracy, etc.

- Modeling uncertainties come from scaling effects, unmodeled processes, simplifications, nodaliztion effects, numerical solution schemes, etc.

Uncertainties must be characterized quantitatively with conservative envelopes. Distributions must be fully realized and integrated into parameter ranking and uncertainty assessment [37].

(7) Integrated uncertainty assessment

The uncertainty of output parameters of interest must be generated. Extremely low probability values must be included. The CNSC requires 95/95 conformance with acceptance criteria. At this stage, confirmation of parameter ranking should be performed. Sensitivity studies must now be performed to ensure all parameter behaviours have been identified [37].

(8) Expert judgement

Expert judgement should be minimized as much as practical. CNSC has established rules for the use of expert judgement. These rules address the identification of areas where expert opinions are logical and needed, the qualifications of experts, integration of judgements, references of supporting information, and documentation of recommendations made. Posteriori confirmation of judgement must be made when possible [37].

(9) Validation of the analysis

Sufficient demonstration must be performed to verify that non-characterized operating states are bounded by the analysis. If operating states cannot be verified to be covered by analysis, new analysis must be performed. Operations and procedures that have been covered by the analysis must be documented such that unusual operations (e.g. deliberate operation

changes due to impairment of equipment) may only persist for a limited time. Longer unusual operations (e.g. repairs) must be analyzed separately [37].

Adequate procedures for monitoring and updating plant parameter behaviours must be created. Compliance with analysis assumptions should continue to be verified through statistical observance. A ‘shelf life’ of the model should be created using these statistical observances [37].

(10) Non-typical plant states

As BE+UA focuses on most likely states and conditions, additional assessments must be performed. Operating procedures such as reactor upsets, equipment failures, operation with defective fuel, fueling operations, start-up/shutdown, etc. must also be performed, or verified to be enveloped by previous analysis [37].

2.7 Testing and V&V Methods

It is essential that all aspects of nuclear safety systems achieve high reliability standards. To measure their compliance it thus becomes necessary to quantize reliability. Traditionally, this was done by investigating lifetimes, probability of breakdowns, or likelihoods of events that would lead to device malfunction. A system’s reliability must be quantized before certification may be achieved.

Digital systems and software, such as those of computer based shutdown systems, present inherent difficulties in the certification. Traditional failure-rate calculations cannot be applied to non-physical systems as their failure methods are often not related to aging and wear [24].

However, there are analysis criteria and tools designed specifically for hardware and software of nuclear safety systems. It is always first essential to divide software programs into categories based upon their degree of criticality to safety. Standardized methods include STUK's safety classes of Finland and the IEC's Safety Integrity Level [64], [65]. The safety criticality determines the required reliability and necessary testing.

Once reliability requirements are found, the IEC recommends the Process Assessment Standard 15504, referred to as 'SPICE' [66]. Used mostly in the prequalification phase, SPICE assesses the capability level of each sub-process of the software [24]. SPICE follows a Preliminary Hazard Analysis (PHA) which defines user requirements for the application [66]. After PHA, there is a Failure Mode Effect Analysis (FMEA) which traces accidents back to their possible causes. This determines the most critical tests and evaluations, which SPICE then investigates.

2.7.1 Canadian Requirements

Canadian requirements for safety systems are summarized in CNSC R-8 document [6]. Canadian safety philosophy focuses on high performance requirements rather than specific methodologies [23]. The R-8 performance requirements focus on the effectiveness of the shutdown systems, but do have some requirements for the safety logic.

The R-8 contains 15 design basis events. Each design basis event must be readily identifiable through at least two different parameters [22]. The system must be able to operate autonomously, and must perform in a manner such that all requirements of the SDS are met. Further, the system must be self-diagnosing, notifying control room operators of any failures that might interfere with its function [22].

Canadian law dictates safety systems must adhere to the requirements for diversity and separation [22]. There must be redundant channels which are independent and physically separate. Like with SDS, the multiple, redundant safety systems must not be dependent upon one another in any way, and their functioning or malfunctioning must not interfere with the effectiveness of other safety systems [22].

2.7.2 Verification and Validation

V&V is a standardized concept in nuclear systems [45]. V&V provides a systematic means to determine the proper design and implementation of the system. It is divided into:

Verification: The system, as it has been designed, has been successfully realized and performs without error.

Validation: The design fulfills all user requirements, with capability demonstrated.

The V&V process is meant to provide substantial evidence that not only has 'the work been done right', but also that 'the right work has been done'. USNRC guidelines for software V&V are outlined in NUREG-0800 [41]. This focuses on clear outlining of requirements, objectives of testing, design best practises, and testing methods.

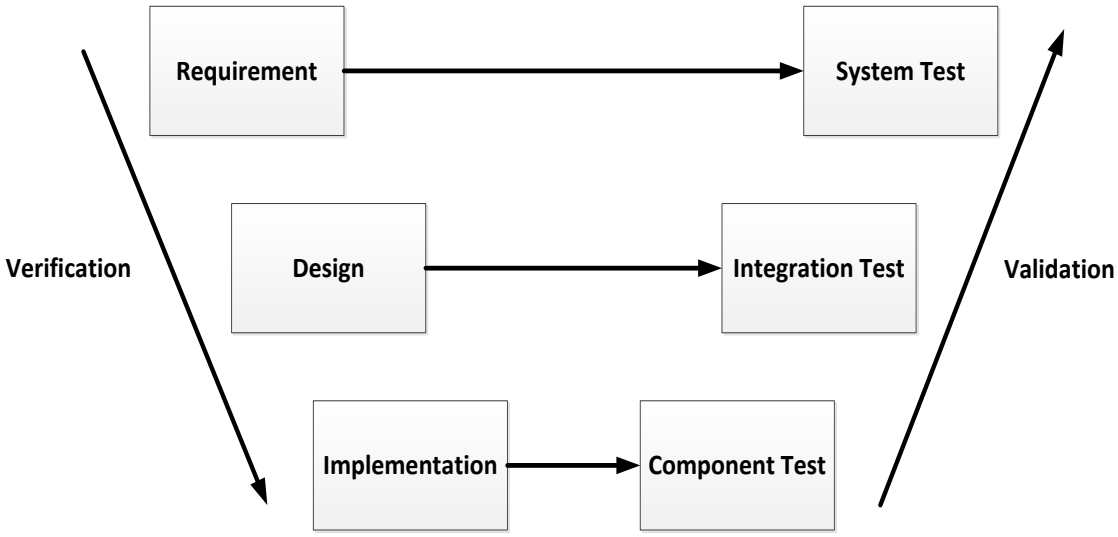

Figure 2.5: Simplified V&V Diagram

The V&V process for digital systems can be summarized with the 'V-diagram', as simplified in Figure 2.5. Each task on the left is related to tests on the right. Systematic testing ensures both the implementation and the design have been performed correctly.

Following Figure 2.5, the end requirements are specified first. These are the final criteria by against which the system will be held accountable. The design is then built off of these requirements. Implementation of the design is then performed and the system is thus realized.

Component testing then follows to ensure that the implementation has been performed to standard. Once each component is verified, integration tests confirm the design has been successfully realized. Finally, system tests examine whether the initial requirements, those created in the first task, have been fulfilled.

Physical models, such as HIL systems or the NPCTF, aid the V&V process as testing platforms. Being capable of testing components, their implementation, and their overall success on a physical process demonstrate design capability. As the NPCTF uses its physical dynamics, rather than modelling, less compatibility alterations need to be made, making it an ideal V&V platform for safety systems.

2.7.3 IEEE Std. 1012

IEEE Standard 1012 is the 'IEEE Standard for System and Software Verification and Validation' [31]. IEEE 1012 aids in:

a) Creation of requirements for software, and
b) Determining software conformity to said requirements

IEEE 1012 encompasses all aspects of the software including interaction with hardware and system requirements. Further, it outlines lifetime requirements for development, maintenance, and reuse [31]. It contains risk/hazard analysis outlines and determinants for integrity level (not to be confused nuclear safety integrity levels (SIL)) [31].

The IEEE 1012's V&V effort requires documentation of objectives and methods used to satisfy them [31]. Each desired integrity level performs the same primary activities. At each objective, there are five to fifteen subtasks. Quantity of subtasks performed corresponds to the desired integrity level [31]. These primary steps and their descriptions are in Table 2.5.

Table 2.5: IEEE Std. 1012 Process Steps.

Task	V&V Activity	Description
1	Software Concept	Describing the specific solution, avoiding false assumptions, specifying system requirements in hardware, software, and HMI
2	Software Requirements	Specifies performance, interface, data definitions, human factors, installation and acceptance, operation and maintenance
3	Software Design	Uses task 2 to create a detailed design for each software component. Ensures design is correct, accurate, and complete.
4	Software Construction	Design is transformed into code, structures, and machine executables. Verifies this transformation is correct and complete.
5	Integration Test	Each component (unit or module) is incrementally integrated. Assure system requirements allocated to software are valid.
6	Qualification Test	Assure the integrated software product satisfies its requirements.
7	Software Acceptance	Assure software satisfies acceptance criteria. Opportunity to allow customer to accept the produce.
8	Installation and Checkout	Tested in target environment.
9	Software Operation	Evaluates impact of changes in operating environment. Assesses system changes and operating procedures.
10	Software Maintenance	Changed in response to need for system maintenance. Includes modifications, migration, and retirement.
11	Software Disposal	Supervises deactivation or disassembly of software product. Ensures elements are properly stored or destroyed as required.

Subtasks relate to traceability, criticality, and hazard, security, and risk analysis [43]. Each subtask in the standard further includes specific means of analysis.

2.8 Safety PLC

Programmable Logic Controllers (PLC) were first created in the 1970s during manufacturing's conversion from mechanical to digital systems. PLC make use of relay style logic for simplicity but possess computational abilities. This allows complex commands, diagnostics, and other functions [67].

PLC are mechanically simple, possessing only four major components: Power Supply, CPU, I/O, and Indicator LEDs [67]. PLC maintain a simple: take inputs, process information, set outputs functioning. This is summarized in Figure 2.6. The IEC standardizes PLC in the IEC 61131 [68]. Part 3 of the standard covers the standardized programming languages. These are: sequential function charts, instruction lists, structured text, ladder diagrams, and function block diagram [69]. These languages are interchangeable when the logic is consistent.

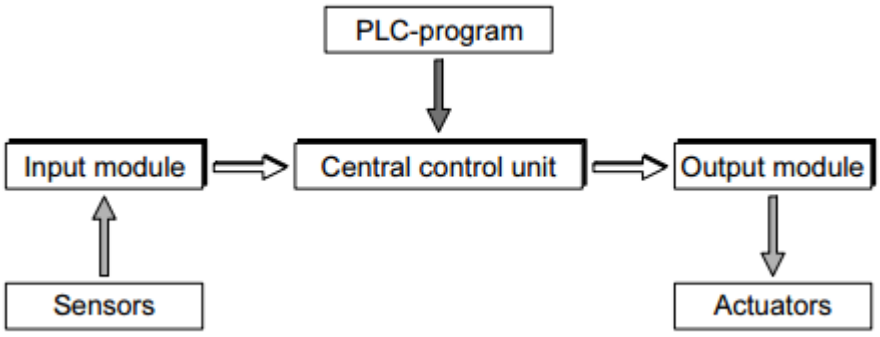

Figure 2.6: CANDU Shutdown Systems Control

PLC is steadily being accepted into nuclear industries. PLC are replacing relay based systems due to superior usability, reliability, and availability [70]. The latter two aspects make PLC particularly attractive for safety applications. The USNRC defines these terms as [70]:

Availability: The fraction of time that the system is actually capable of performing its mission.

Reliability: The probability that a device will function without failure over a specified time period or amount of usage.

The separation between PLC units for safety opposed to other plant operations is defined under a single principle: Safety PLC include two processors working in parallel,

running diverse logic for the same operations, continually cross-checking values against one another. The advantage in this is threefold: First, all calculations are double checked, so that there is mathematical redundancy as well as physical; second, diverse logic prevents CCFs that could occur through incorrect or incomplete logic; and third, two processor units allows one of the units to take over should a failure occur.

Commonly, the IEC Safety Integrity Level (SIL) is used to evaluate these systems [68]. Based on the probability of 'failure on demand', an SIL is given. Safety PLC reach levels of 3 and 4, whilst other units are typically 1 or 2. SIL rates are given in Table 2.6.

Table 2.6: Safety Integrity Levels

SIL	Probability of Failure on Demand
1	10^{-1}-10^{-2}
2	10^{-2}-10^{-3}
3	10^{-3}-10^{-4}
4	10^{-4}-10^{-5}

The USNRC standardizes safety PLC requirements in NUREG-6090 [70]. This standard covers criteria for intelligence, I/O structure, power supply, communications, error handling, and more. It also lists a number of recommended features, including [70]

- Module hot-swapping
- RAM battery back-up and battery monitor
- System battery back-up
- Redundancy
- Fault tolerance
- Acceptable system availability
- Clearly defined fail-safe modes

In order to minimize the V&V required, software and hardware is kept to a minimum. CANDU 600 units utilize PLC that lack operating systems, interrupts, keyboards, displays other than LEDS [67]. The software used consists of only 3000 words of EPROM and 100 words of RAM. It runs a single endless loop that passes every 35ms, in which every other pass is comprehensive self-test.

Since 1982, Canada has used PLC units in three of their plants, utilizing thirty-six systems in total [67]. There has since been no spurious trips nor failures to trip due to PLC malfunction. Self-checking features have always notified operators of hardware failures, with failure-to-repair time taking less than two hours in each instance [70].

USNRC approval for safety systems has been achieved by only four PLC devices [71]. These devices are Westinghouse Common Q, AREVA TELEPERM XS (TXS), Invensys Triconex, and HFC6000. These four devices have met USNRC highest criteria in reliability and availability are thus considered safe enough to utilize in the RPS.

2.9 Chapter Summary

This chapter provides the necessary background for the proposed work. Several key topics are introduced and discussed for relevance to RPSs.

First, an explanation of the CANDU reactor is given. Using the neutron dynamics of the reactor core, the importance of the protection scheme is demonstrated. Primarily, why the system must respond quickly, as well as why it must continue to operate, are explained using the concepts of runaway and decay reactions.

Next RPSs for CANDU plants are discussed. The two systems, SDS1 (cadmium shutdown rods) and SDS2 (gadolinium nitrate injections) are presented mechanically alongside

their controlling units. The design methods for these systems are then presented. Necessary design features such as monitoring parameters, redundancy, and diversity of design are reviewed to complement the challenges they exist to meet: damages, failures, and CCFs respectively.

The methodologies of choosing tripping set points are given. The design basis event is presented alongside standard methods of determining uncertainty. These lead into BE+UA analysis, the current methodology used in Canada. This leads into testing and V&V methods. This section visits the Canadian requirements, discussing the CNSC R-8 regulatory document. Further, the American equivalent for software (the NUREG-0800) shows the necessary steps for V&V in software systems.

Finally, safety PLC are discussed. Their performance in Canada since 1980 show these units to be highly reliable and available when utilized in CANDU NPP. Their desirable qualities working with nuclear safety are listed, making their selection as the control units for the RPS logical.

3 Cross-Comparison of NPCTF and CANDU NPP Signals

3.1 NPCTF Overview

The NPCTF is a physical recreation of a thermal power plant scaled down for IC research [72]. Though pressures, flow rates, and temperatures are reduced, the design produces similar responses to full NPP [2]. The NPCTF may operate in different configurations though the third generation CANDU is the default [72]. The system is capable of safely injecting faults and other conditions safely. The physical simulation replicates these scenarios so that control, safety, or other systems may be tested against them [72].

From a themal-hydrolic point of view, the NPCTF is a double loop thermal plant [72]. The water heater replaces the boiler as the thermal source. The steam generator has been replaced with a high efficiency heat exchanger. Primary loop temperature drop across the heat exchanger is measured, and the pneumatic system drives the turbine proportionally [72]. Pressure is maintained through a pressurizer, and a water chiller acting as the condenser completes the major components.

The NPCTF is capable of simulating a wide variety of thermal plants. Thus, the pressurizer, the chiller, or both may be disabled or bypassed [2]. Initialization may load control schemes specific to these configurations. This customizability increases the variety of designs available for equipment or design testing. An exact schematic can be seen in Figure 3.1 [72]. Note the primary loop is filled with water as coolant while the turbine loop utilizes air supplied from an external source.

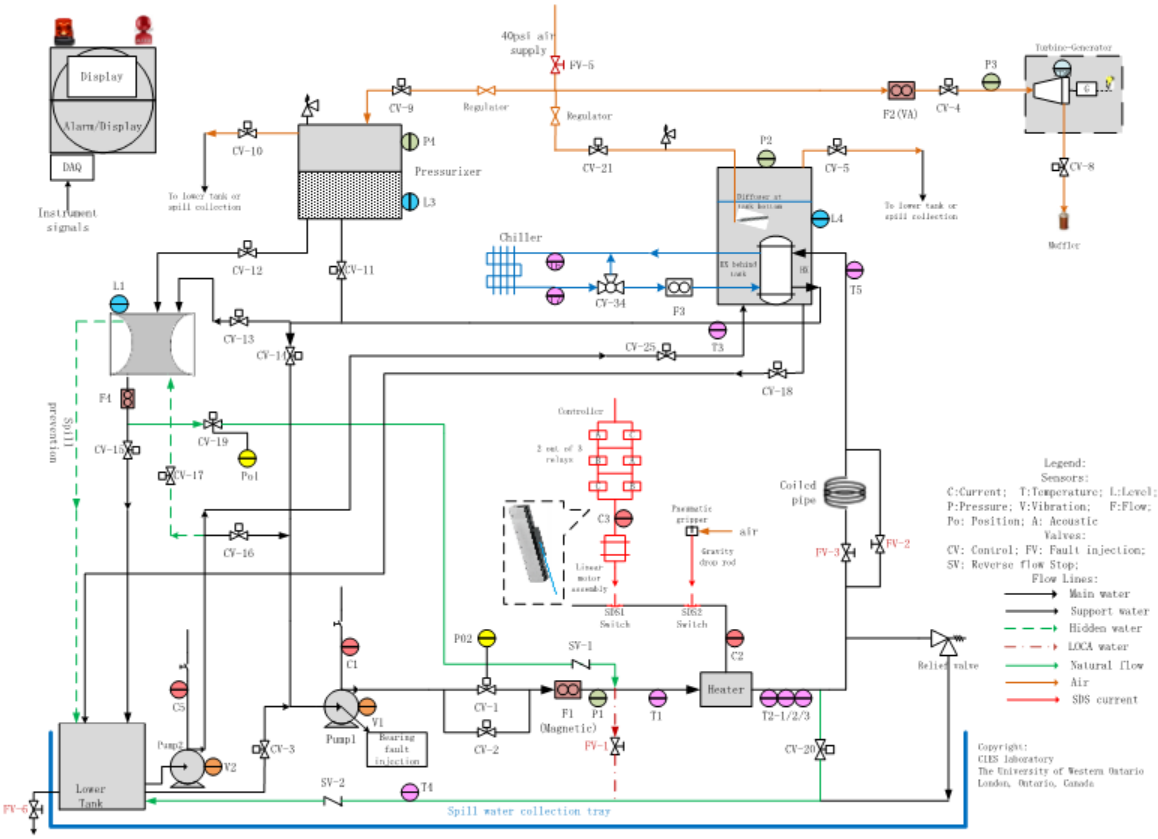

Figure 3.1: The NPCTF Schematic.

Electrically, the NPCTF is controlled through an ABB AC 700F controller [72], [73]. However, the ABB may be disabled and control turned over to an external system through a junction box [72]. This junction box includes all analog signals from the NPCTF in 4-20mA sources and all digital leads in short/open configuration [72]. The inputs for the system work possess same specifications. In total, there are 90 I/O ports by which to control or monitor the NPCTF [72].

As previously stated, the NPCTF is capable of safely simulating faults. This trait makes it an ideal platform with which to perform safety system V&V. The NPCTF allows the user to override the control system, opening or closing nearly every valve [72]. Additionally, there are manual release valves that drain into containers [72]. The ABB controller may deactivate

any major system or force values through the commands of the external controller [72]. This simulates emergency conditions such as pipe breaks, clogs, equipment failures, sensor mis-readings, and more.

The NPCTF uses industrially standard devices for near all components (examples given as [74-76]). Most NPCTF valves are Belimo B2 series, 2-way control valves [77]. These valves are driven by LF24-SR actuators [77]. These give 4-20mA readings of their current position and may be configured as normally open or normally closed. The full range actuation time is 150 seconds [77]. This rate is important as it characterizes response times, insertion of valve-based faults, and overall system dynamics.

As stated, the main controller is an AC 700F by ABB. This possesses a Class 1 Division 2 certificate under ISO 9001 [73], [78]. The AC 700F operates according to the IEC 61131 (programmable controllers) standard and verified under part 2 (equipment requirements) [73], [68], [79]. The controller is drastically quicker than any of the mechanical components of the system with response times as quick as 2ms [73]. This allows stable control even during the presence of most faults.

The controller has not been configured to operate the NPCTF optimally. Rather, its programming provides characteristics more similar to that of an NPP [2]. As an example, the shrink and swell phenomenon is simulated with the steam generator tank. More on this phenomenon is in section 3.2: Key Operating Characteristics.

During the work performed, the NPCTF was configured as a CANDU NPP (i.e. two loops with both pressurizer and chiller). The faults inserted were physically manifested such

that real, rather than simulated, dynamics were observed. This allowed a more thorough V&V of the safety algorithm through exposure to more valid NPP failures.

3.1.1 Comparison of CANDU NPP and NPCTF Parameters

The NPCTF is a high fidelity mock-up, but it is not an NPP. There are differences that must be recognized during the design and testing phases. Each major aspect of the NPCTF has been compared with its CANDU equivalent. These differences are summarized in Table 3.1.

Table 3.1: Comparison of Major Features between CANDU and NPCTF.

Item	Typical CANDU Range	Typical NPCTF Range
Source Outlet Temperature	310°C	30°C
Pressure	1,400 PSI(g)	7.25 PSI(g)
Main Pump	1.17MW	22W
Primary Flow Rate	38,000 l/min	6 l/min

Temperature: CANDU fuel bundles operate around 2000°C [6]. However, the coolant's greater volume means CANDU reactors have inlet and outlet temperatures of about 265°C and 310°C respectively [6]. The NPCTF does not have fuel bundles, but has standard 20^0C inlet and 30^0C outlet temperatures [2].

Pressure: The primary line of CANDU reactors are pressurized at, using Pickering as an example, 1,400PSI(g) [6]. This is heavy water in the primary line but has nearly identical fluidic dynamics. By comparison, the NPCTF uses light water at pressures centering at 7.75PSI(g).

Main Pump: Many CANDU systems use multiple pumps in the primary loop. Plants like Bruce use four 9,000HP pumps, while Pickering uses 12 pumps at 1,570HP, about

1.17MW [11]. It's worth noting the primary pump is the largest 'in-house' load for the station. The NPCTF uses a single primary pump that runs up to 22W [80].

Primary Flow Rate: With Pickering as an example, there is a nominal CANDU flowrate of 10,100 gallons per minute (~38,000 litres/minute) [6]. Often measured in lbs/hr, this represents 61,300,000 lb/hr. NPCTF primary flow rates nominally centre at 6 l/min.

The NPCTF possesses a single heater, steam generator, and pump in the primary loop. It operates at lower temperatures and uses light instead of heavy water in the primary line. No steam is generated in the NPCTF; instead, a high efficiency heat exchanger [81] connects the chiller and primary loops. The primary loop's incoming and outgoing temperatures are used to calculate energy loss which determines the simulated turbine speed.

The heater simulates a nuclear reactor but has different operating characteristics. Current has been used as a rough parallel for neutron activity. However, control of current is much quicker than control of neutron economy. Control rods make slow changes while the heater current is capable of quick responses that maintain constant heat [82].

The heater shutdown does not follow the same neutron activity dynamic of an NPP. Typical NPP shutdown curves appear below in Figure 3.2 [82] for a LOCA scenario when both the reactor protection system does and does not shutdown the reaction. Notice that in the shutdown scenario the LOCA occurs at on second, the trip is initiated at 1.44s, and normalized reactor power, though beneath 0.25 by 3s, does not manage to reach 0 by the end of the simulation. Contrarily, the NPCTF completely shuts down the current when shutdown is detected.

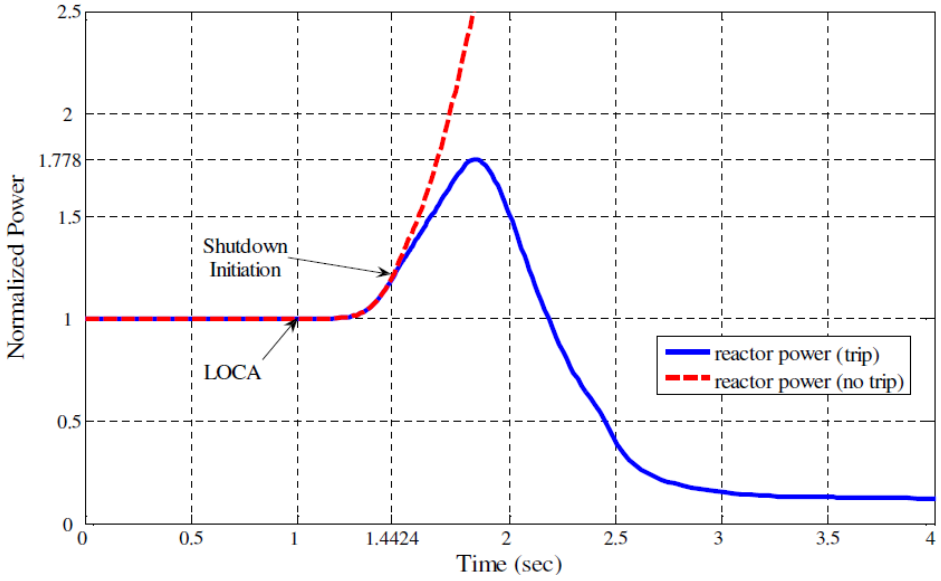

Figure 3.2: Typical Shutdown Curves of a Nuclear Reactor.

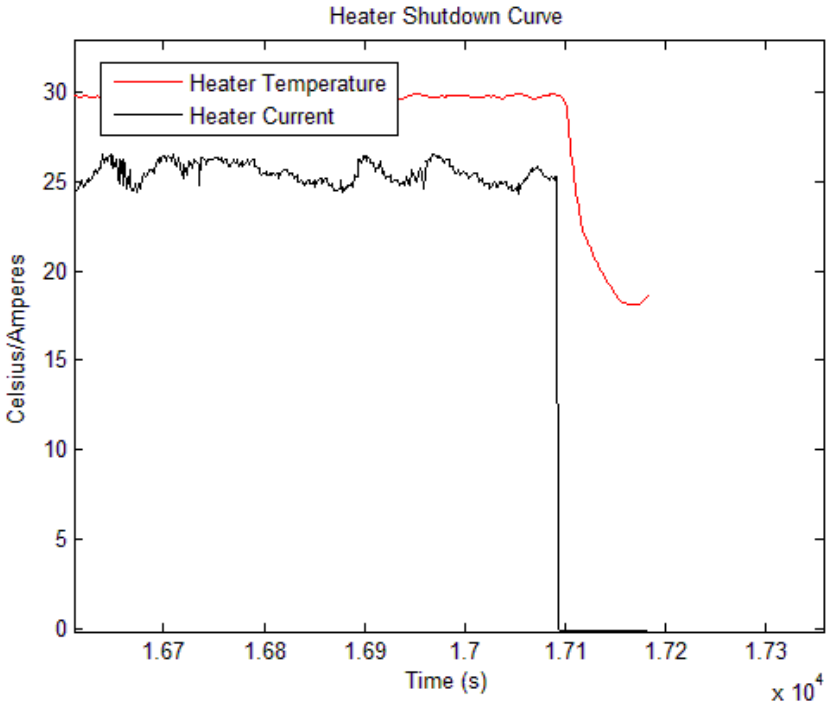

Figure 3.3: The Current Drop of NPCTF

3.2 Key Operating Parameters on NPCTF

As stated in section 2.3: Design of Reactor Protection System, CANDU safety systems typically use eleven key parameters to monitor the health of the system [37]. The NPCTF

lacks a nuclear reactor and thus not every parameter is paralleled. However, many CANDU parameters do have equivalents in the NPCTF, as displayed in Table 3.2:

Table 3.2: Parallel Parameters between CANDU Shutdown Systems and the NPCTF.

CANDU Critical Signal	Absolute/Conditional	NPCTF Equivalent
High Neutron Power	Absolute	None
High Rate of Rise of Neutron Power	Absolute	None
High Coolant Pressure	Conditional	Primary Loop Pressure (P1)
Low Coolant Pressure	Conditional	Primary Loop Pressure (P1)
High Building Pressure	Absolute	None
Low Steam Generator Level	Conditional	HX Tank Level (L4)
Low Pressurizer Level	Conditional	Pressurizer Level (L3)
High Moderator Temperature	Absolute	Heater Outlet Temperature (T2)
Low Coolant Flow	Conditional	Primary Water Flow (F1)
Low Steam Generator Pressure	Conditional	HX Tank Pressure (P2)
Manual Shutdown	Absolute	Manual Release Button

CANDU separates absolute and conditional tripping parameters. Absolute parameters remain active at all times, while conditional are disabled during start-up and shut-down. This prevents spurious tripping while flow, pressure, or water-levels are reaching their operating ranges.

All parameters on the NPCTF have been designed to display dynamics similar to their respective equivalents [2]. However, there remains some discrepancies. To investigate each parameter, the NPCTF was first operated for nearly 50 non-continuous hours. This investigated steady state operations in addition to transients. These properties were then statistically analyzed for trends so the dynamics of safe operation could be characterized.

From this point in the investigation, the NPCTF was assumed to operate at one of three defined operating points: 25^0C, 30^0C, and 35^0C heater outlet temperature. Though any value in this range is possible, specifying operating ranges greatly simplified the investigation and design. The found properties of the six key parameters are given in sections 3.2.1 to 3.2.6.

3.2.1 Primary Loop Pressure

Primary loop pressure is designated at P1 in the NPCTF schematic. It is monitored by an *American Sensor Technologies* AST4100 compact pressure sensor [72]. The AST4100 sensor has an accuracy of < +/- 0.5% BFSL, including non-linearity, hysteresis, and non-linearity [74]. The 4-20mA range has been formatted to give a range of 0-25PSI(g).

Within the NPCTF, the primary loop pressure experienced little change across all operating conditions. As the pressurizer maintains the primary loop pressure, the range stayed consistently between 7.2PSI(g) and 10.55PSI(g). 44 hours of operations is shown in Figure 3.4.

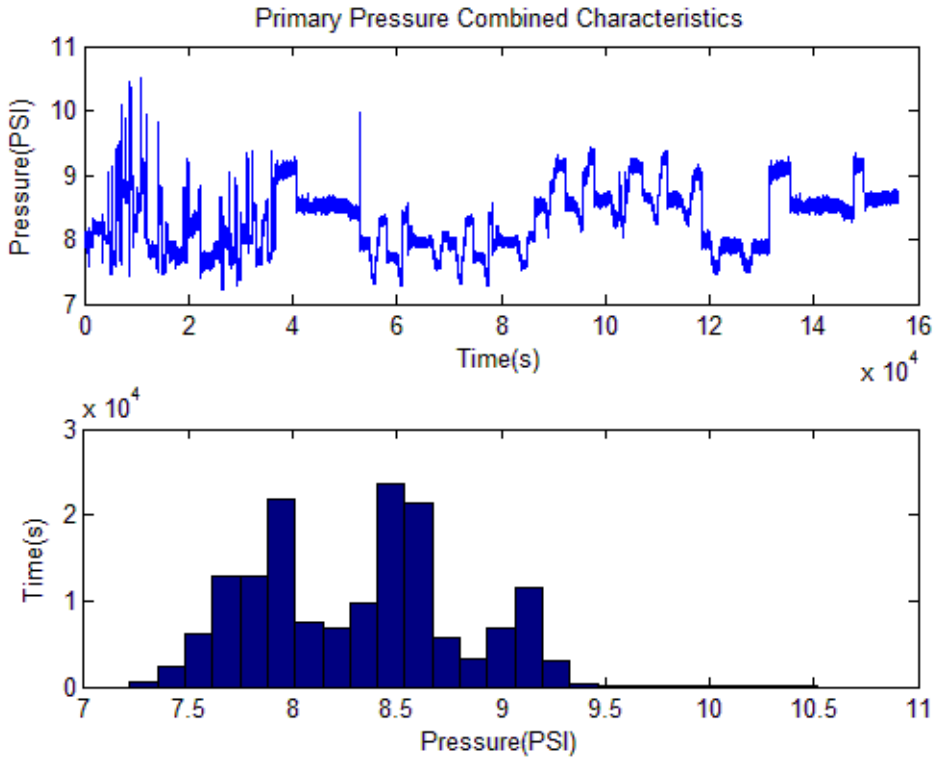

Figure 3.4: Operating Characteristics of Primary Pressure.

Primary loop pressure varies very little, even through several operating point transitions, as demonstrated in Figure 3.4. This general stability lead to the primary loop pressure being designated as a heater-independent parameter in the safety system design. The maximum and minimum values at various points for a single 5 hour operating period with each set-point met atleast once are shown below in Table 3.3.

Table 3.3: Maximum and Minimum Values of Primary Pressure Related to NPCTF Operating Point.

Heater Set Point	Minimum Value	Maximum Value
25^0C	7.545 PSI(g)	8.022 PSI(g)
30^0C	7.885 PSI(g)	8.116 PSI(g)
35^0C	7.675 PSI(g)	8.203 PSI(g)

3.2.2 Pressurizer Level

The pressurizer's water level is designated as 'L3' in the NPCTF schematic [72]. This parameter is measured by an *American Sensor Technologies* AST5100-Wet low differential pressure transmitter [72]. The AST5100 possesses a <+/- 1.0% of FS accuracy and has been configured in the 0-10 inch (0.0-0.254m) H_2O (25mbar) option [75]. The level in inches is converted to a percentage of the maximum level of the pressurizer (i.e. 0-100% full) before transmission in 4-20mA.

The pressurizer level is also heater-independent. The pressurizer's level did respond to transients, though these were highly transient. Pressurizer level over 44 hours is shown in Figure 3.5.

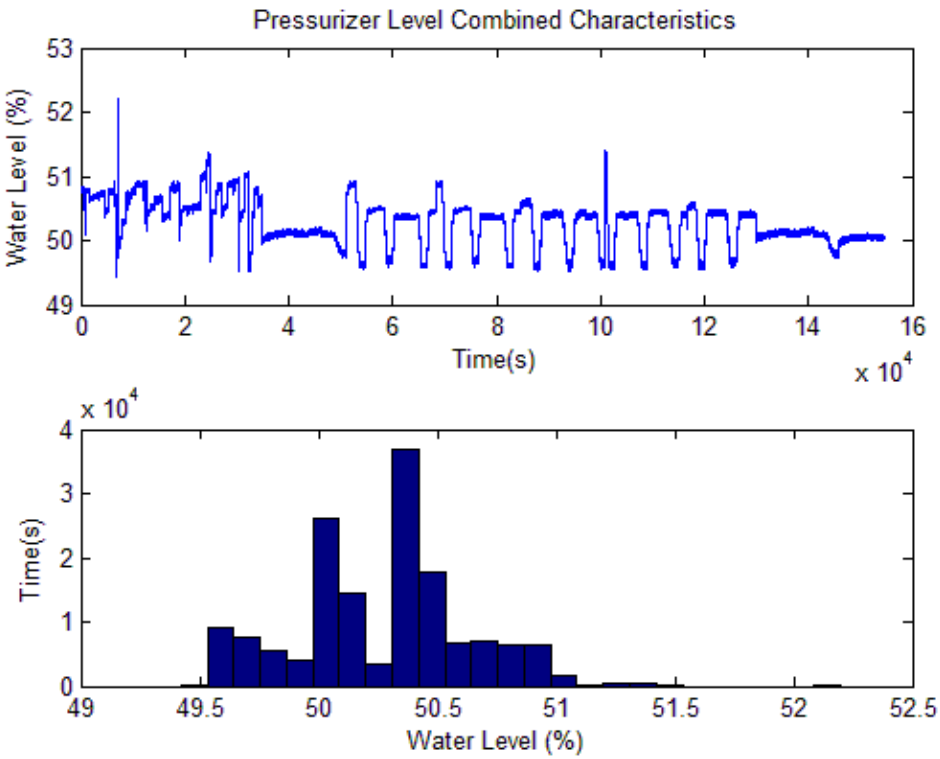

Figure 3.5: Operating Characteristics of Pressurizer Level.

Pressurizer level performs many quick drops, as shown in Figure 3.5. When operating point changes occurred, a water level drop would develop then quickly clear. This characteristic was later included into safety system design. When the system was free of faults, the minimum pressurizer level was 49.2% and the maximum was 52.3%. The histogram in Figure 3.5 shows how water level operated principally at 50% or 50.4%, with strays from these two values occurring rarely. Pressurizer level also dropped dramatically during the presence of faults, as will be shown later. The maximums and minimums during a normal operations trial are shown below in Table 3.4. Note that start-up transients have not been included.

Table 3.4: Maximum and Minimum Values of Pressurizer Water Level Compared to Heater Operating Points.

Heater Set Point	Minimum Value	Maximum Value
25^{0}C	49.595	50.405
30^{0}C	50.318	50.492
35^{0}C	49.798	50.405

3.2.3 Primary Water Flow

Primary water flow is the flow rate of the NPCTF's coolant through the primary loop [72]. This water flow is responsible for transportation of heat in the primary loop. The flow rate is designated as F1 in the NPCTF schematics [72] and is measured by *Lake Monitors'* FlowStat – Turbine Flow Sensor [76]. The flow sensor was configured to measure in litres/minute with a range of 2-60 l/m. Using the 1/2 inch porting, the flow sensor possesses +/- 2% FS accuracy [76].

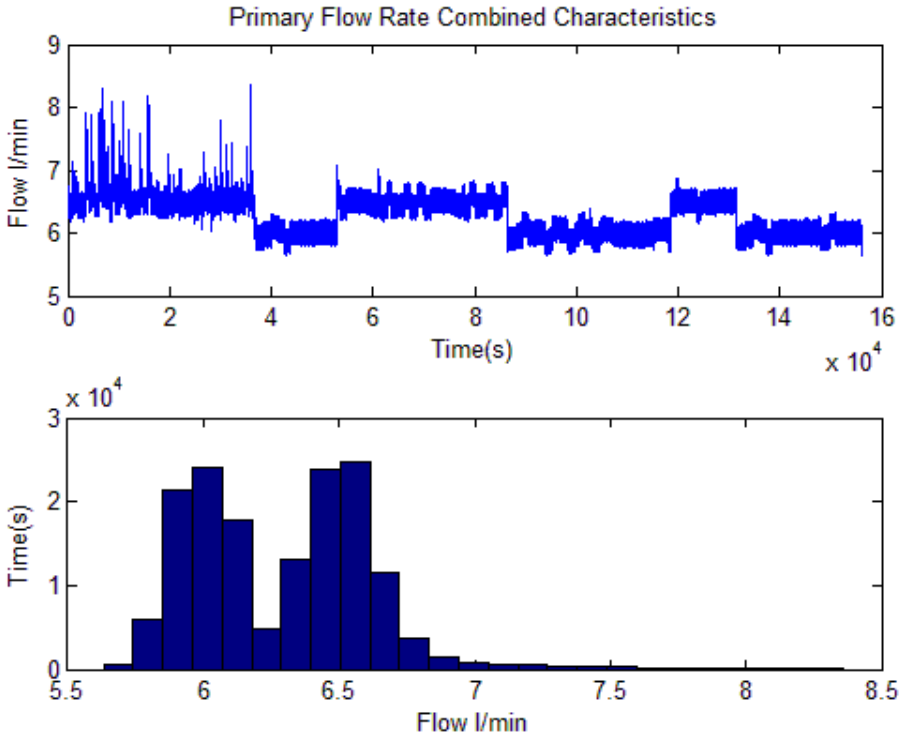

Figure 3.6: Example of Flow Characteristics of Primary Loop.

As with loop pressure and pressurizer level, the primary flow rate is heater-independent. However, flow rate exhibits considerable jitter. The jitter is fairly uniform around a midpoint in a Gaussian white noise fashion. However, there are rare occurrences of large

spikes momentarily observed during operations. These are solitary and do not indicate a disturbance when observed transiently.

Flow rate over 44 hours is shown in Figure 3.6. The jitter manifests as a thickness in the first subplot. As shown, the jitter is consistent and the flow average flow rate remains does not deviate greatly during normal operations. The maximum and minimum flow rates for various heater operating points during an example trial are shown below in Table 3.5. Note that this Table again excludes outliers.

Table 3.5: Flow Rate in Relation to Heater Set Point

Heater Set Point	Minimum Value	Maximum Value
25^0C	6.201	6.627
30^0C	6.234	6.817
35^0C	6.237	6.822

3.2.4 HX Tank Pressure

HX tank pressure (P2 in the NPCTF schematic [72]) is the final of the four heater independent parameters. Like the primary loop pressure, the HX tank pressure was measured by an *American Sensor Technologies* AST4100 [72], [74].

The HX tank pressure possessed considerable noise though remained within a tight envelope during operation. Though exhibiting tumultuous start-up, HX tank pressure was found to be largely independent of other conditions in the NPCTF. The maximum and minimum values as related to heater operating point are listed in Table 3.6.

Table 3.6: HX Tank Pressure vs. Heater Operating Point.

Heater Set Point	Minimum Value	Maximum Value
25^0C	4.890	5.252
30^0C	4.767	5.187
35^0C	4.753	5.136

HX tank pressure's independence from heater current is visually demonstrated in Figure 3.7. Note the range on the y-axis.

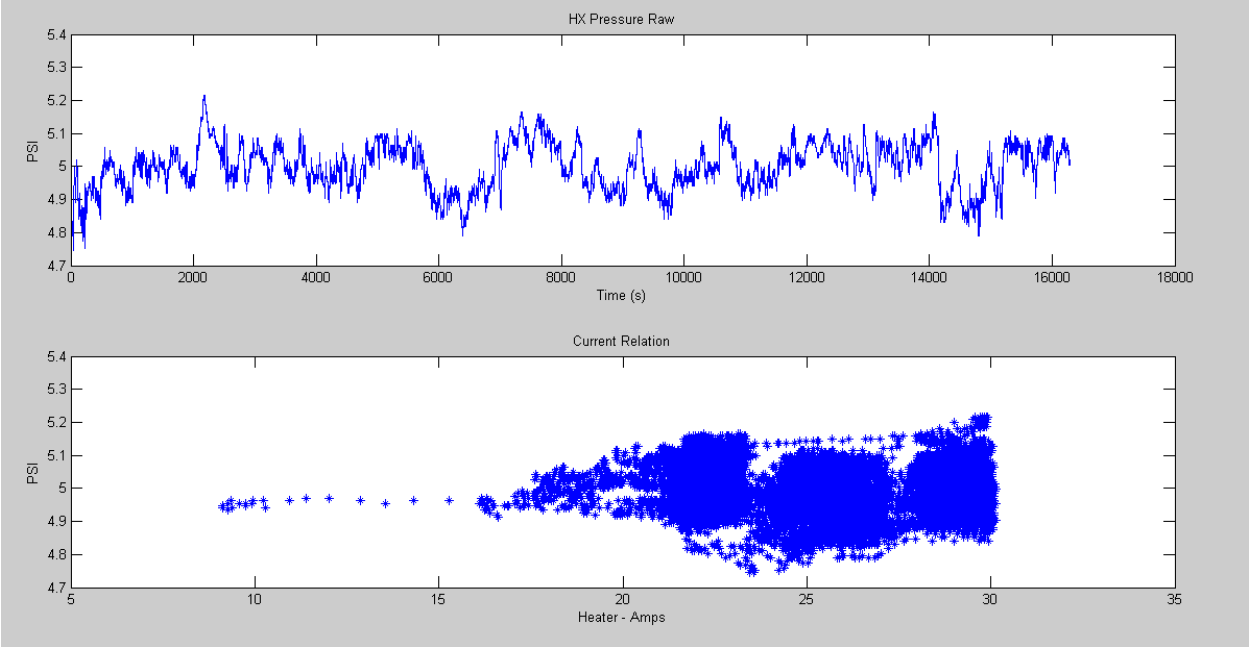

Figure 3.7: Example of Operating Characteristics of HX Tank Pressure.

3.2.5 Heater Outlet Temperature

Heater outlet temperature (T2 [72]) was the main reference points for the state of the system. The temperature was measured by the intempc MIST03 Temperature Sensor [72], an RTD with a built-in programmable transmitter [83]. Like all of the NPCTF sensors, it outputs 4-20mA linearly for measurements ranging from 0-50^{0}C in the model chosen. The NPCTF utilizes three of these sensors at the heater output, mimicking an NPP's triplicated measurement for reactor heat.

Heater temperature was the reference utilized for operating point changes. When at specific operating points, heater outlet temperature remained fairly consistent. This is partially demonstrated by Table 3.7.

Table 3.7: Actual Heater Temperatures at Operating Points.

Heater Set Point	Minimum Value	Maximum Value
25^0C	24.638	25.550
30^0C	29.354	30.758
35^0C	34.013	34.910

This consistency was maintained by the ABB controller's direct control of heater current. Values listed in Table 3.7 are only valid for periods when the heater temperature has been given sufficient time to settle into its operating point. It should be noted that the heater, even at the set point of 35^0C, is incapable of achieving a temperature of 35^0C under normal operating conditions. The heater itself is a 7.5kW Gaunmer process C15P3N18T2 circulation screw-plug heater [84].

Transition time between operating points was crucial for characterizing the NPCTF. Using the defined operating points, maximum observed transition times between the 25^0C, 30^0C, and 35^0C set points are listed in Table 3.8.

Table 3.8: Transition Times for Heater Outlet Temperature.

Transition	Time (s)
25^0C -> 30^0C	178
30^0C -> 35^0C	1011
25^0C -> 35^0C	1242
35^0C -> 30^0C	20
30^0C -> 25^0C	57
35^0C -> 25^0C	166

The direction and magnitude of the step strongly influenced the time required for transition. The largest upwards step, 25^0C to 35^0C, requires nearly 21 minutes to complete, while the smallest downward step lasted at longest 20s.

These times were utilized in the design of the safety system under the assumption that an unusually long transition could indicate a fault. As examples, transitions upwards progressing too slowly may indicate reactor issues, while too slowly downwards may indicate

coolant leaks. Transitions briefer than expected could likewise indicate concerns with coolant flow.

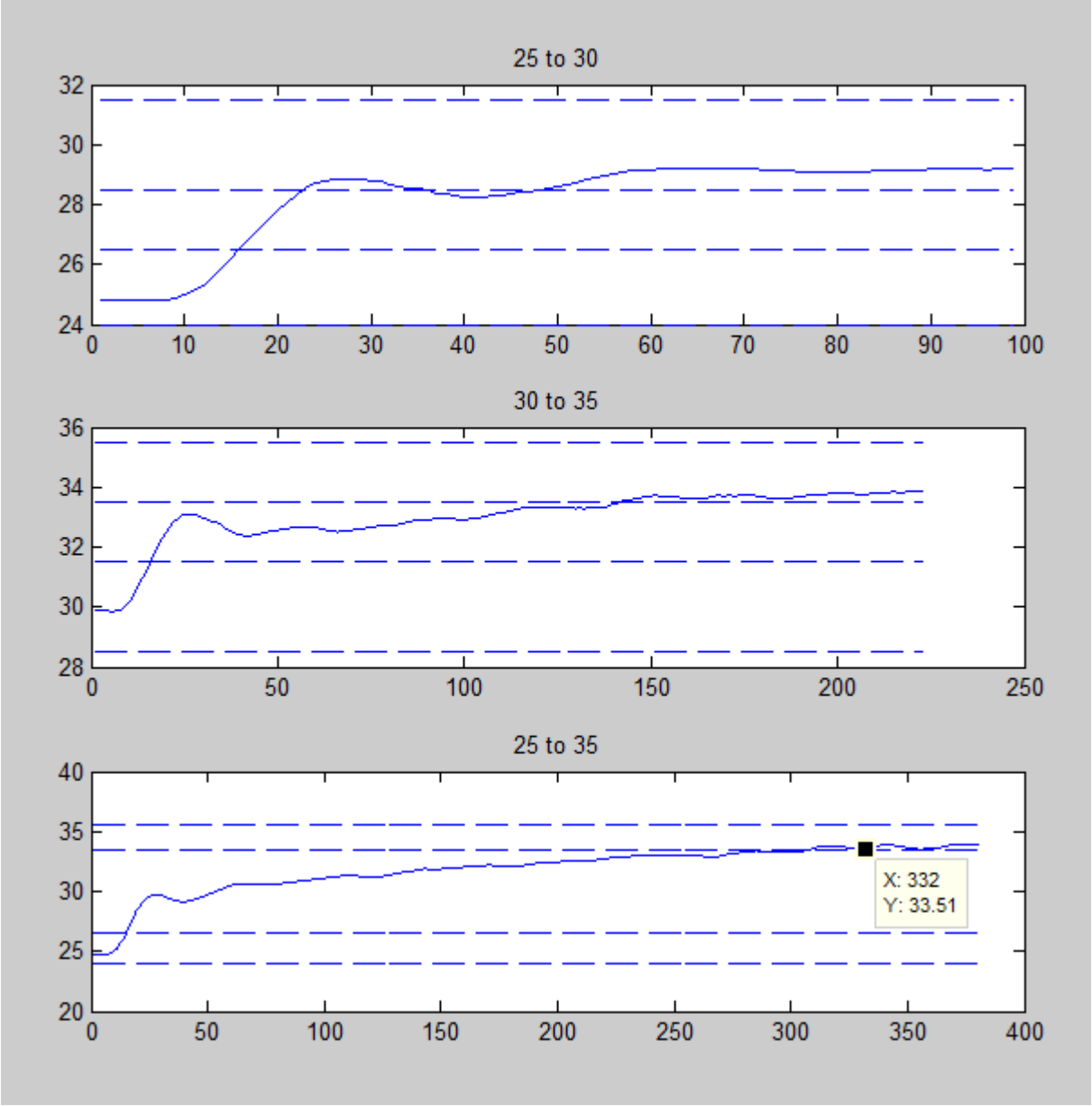

Figure 3.8: Demonstration of Transition Steps between Heater Outlet Set Points.

Figure 3.8 shows the measuring method for transition time. The transition is defined as commencing when the operating point is changed (time = 0s in Figure 3.8) until the heat

arrived at and stayed within the maximum and minimum values observed during settled operations without exiting the range again.

3.2.6 HX Tank Level

The HX tank level (L4 [72]) possessed the most complex characteristics amongst parameters investigated. Steam generators present inherent difficulties in their control [75]. The HX tank level, like the pressurizer level, was measured by an AST5100-Wet low differential pressure transmitter [75] and likewise converted to a 0-100% of full range measurement.

Steam generators exhibit the 'swell and shrink' phenomenon [85]. This phenomenon creates strong inverse response characteristic from the steam generator level as the result of strong compressive forces acting on the water/steam barrier in the tank. This is a two-step process [85]:

1) Decreasing the level of the steam generator: steam flow rate increases and thus pressure decreases. The two phase fluid composite expands and swell occurs. (a sudden increase in level)
2) Increasing the level of the steam generator: steam flow rate decreases and steam bubbles within the two phase fluid composite collapse under the pressure increase. The liquid water flows to occupy the void and shrink occurs (a sudden decrease in level)

The NPCTF mimics this effect as the heat and pressure is insufficient to produce a two-phased liquid. Its control characteristics imitate swell and shrink to increase fidelity to an NPP. The general set points the level are listed in Table 3.9.

Table 3.9: The HX Tank Level Operating Points Related to Heater Outlet Temperature Operating Point.

Heater Set Point	Minimum Value	Maximum Value
25^0C	48.901	68.895
30^0C	51.505	75.608
35^0C	74.421	81.912

The control loop of the HX tank level targeted a specified fraction (typically 80%) of the heater current's own percentage of maximum output. I.e. operating at 70% of maximum current would set the operating point for HX tank level at 0.8x0.7= 56% of its maximum value. However, multiple simulated effects resulted in difficulty attaining these targets.

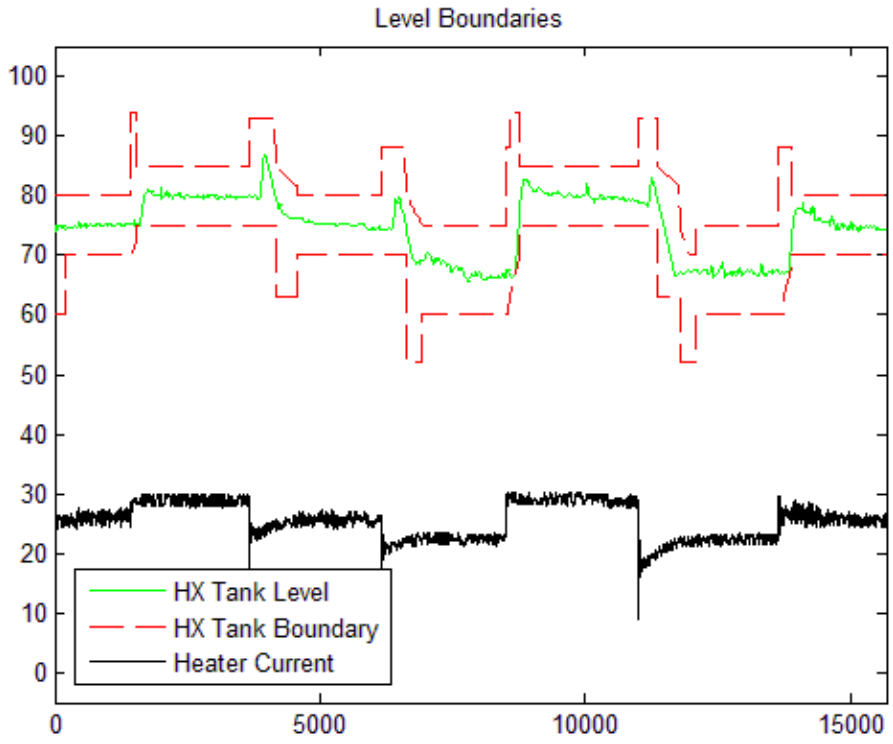

Figure 3.9: Swell and Shrink in HX Tank.

HX tank level is stable when settled but may settle at any point in a wide range for any given operating point. The eventual safety algorithm importantly had to also compensate for the simulated swell and shrink phenomenon. An example operation of HX tank level can be seen in Figure 3.9.

As the HX tank level is dependent on heater current, it too was measured for transition times. The maximum observed times under normal conditions for each step is shown in Table 3.10:

Table 3.10: Maximum Transition Times for HX Tank Level.

Transition	Time (s)
25^0C -> 30^0C	218
30^0C -> 35^0C	171
25^0C -> 35^0C	255
35^0C -> 30^0C	492
30^0C -> 25^0C	457
35^0C -> 25^0C	494

These times do not include the inverse response characteristic, which typically persists for two to eight minutes. Notably for the downwards transitions, the transition time required after the inverse response is independent of the step size. These processes were predictable though highly variable. These times have been used to aid the safety system in discerning whether the HX tank level is transitioning in a manner consistent with safe operations.

3.3 Chapter Summary

This chapter investigates the operating characteristics of the NPCTF. First, the NPCTF is discussed in detail. Its thermal-hydraulic configuration is discussed, alongside its fault insertion capabilities. The I/O and other communication devices are presented due to their role in the connection between the NPCTF and the designed control system. Next, CANDU NPP are compared to the NPCTF to quantify differences. The primary discovery is that though the NPCTF is substantially scaled down, this scaling is internally consistent, validating tests performed upon it.

The key operating parameters for the NPCTF are then discussed in detail. For each of these parameters, operating ranges are given, alongside minimum and maximum values

observed. The parameters are split into two distinct groups: Heater-Independent (those whose operating points do not change with heater current) and Heater-Dependent (those whose operating points do change with heater current). The heater-independent variables are primary loop pressure (P1), pressurizer level (L3), primary water flow (F1), and HX tank pressure (P2). The dependent parameters are heater outlet temperature (T2) and HX tank level (L4). For the heater dependent parameters, maximum observed transition times are discussed.

In summary, this chapter presents the necessary information for the design of the RPS. By observing the characteristics of the NPCTF under normal operating conditions, the implemented algorithm will be able to distinguish when conditions are aberrant and thus in need of a shutdown.

4 Implementation of Reactor Protection Systems Using HFC6000

4.1 Overview of HFC6000

The HFC6000 (HFC) is a PLC nuclear safety system developed by HF Controls [86]. The HFC is designed to perform functional safety control and is designed though not limited in scope to nuclear applications [87]. The HFC is the most recently developed product in Doosan's safety system product line. It was released in 2005 alongside its process control sister system, the ECS-1200 [86]. The system has three different models: FPC08, SBC06, and SBC04 [87]. The major difference between these three models is their eponymous main processing units. The remaining configuration is customizable according to the needs of the project [87].

Figure 4.1: HFC6000 Front Pane

For the work performed, the SBC06 model was used. The SBC06 is a multiple loop controller [88]. SBC06 models are able to access up to 1024 I/O points, dealt with through two I/O independent interface channels. The HFC and its previous iterations have been tested

in the USA and Korea continuously since 2001 [87]. The HFC itself began testing in the United States in 2003. Meanwhile, all updates, additional details, and any new parts have been continuously verified [86].

The HFC boasts a number of important features related to safety. Because it is an exclusively safety based system, all of its control, data, and communication links are dedicated [87]. It has considerable personal redundancy, and is hardened to nuclear and electromagnetic radiation.

Importantly, each of the processors are duplicated to achieve redundant control. On each remote controller, two main processors are tied to a single piece of dual port memory (DPM) [88]. The processor keeps status of being primary or secondary within its twin pairing so that the slave processors respond accordingly and the couple effectively as a unit. Should the processor be in primary mode, all of its public memory data is constantly transferring to the DPM, while in secondary mode the DPM contents are constantly imported into public memory [88]. This ensures constant congruence and a smooth transition can occur in case of failover.

The DPM also defines the HFC as a safety PLC. Because the cross-checking processors use parallel calculations, considerable reliability is added. The safety PLC is now able to verify its own decisions with a parallel unit receiving the same signals, decreasing the likelihood of error. This represents not only redundant hardware, but redundant calculations as well. Further, because of the failover characteristic, a spontaneous failure in a safety PLC does not immediately compromise the health of the system.

For a full discussion and diagram of the HFC/NPCTF interface refer to Section 4.4 and Figure 4.20. Discussion of the interface and functioning of the HFC requires first a discussion of the relevant hardware and implemented software.

4.1.1 The SBC06 Processor Board

Each SBC06 remote includes an Intel386 [89] system processor (SYS), with at least two dedicated communication processors [88]. SYS acts as the master while the two communications processors (ICL and C-Link) act as slaves. The ICL controls the intercommunication link: the link which interacts with I/O modules by transferring data to and from instrumentation and control devices [88]. The C-Link controls the communication link: the data exchange between intelligent devices [88]. Finally, the SYS is responsible for coordinating the other processors, running the applications, and monitoring the overall system status [88].

The SYS requires an application program [88]. This program contains five files: the I/O Configuration Table, the Equations File, the Block Request Table, the Blocks List, and the Block Data File. These files are written by the engineer and are the main software body of the system. The five files make up four structures (the blocks list and block data file are a single structure) which are created on an engineer's work station [88]. Once compiled using the HFC utilities, the structures are either burned into a PROM or loaded onto a flash memory depending on the safety level the application is controlling [88]. The function of each file is as follows:

- Equations File: Contains the logic of the system through a series of sequential statements typically displayed as ladder logic. Equation statements will each

perform a mathematical operation or make a call to one of the analog block algorithms

- I/O Configuration Table: An exhaustive list of the I/O hardware included in the system. The ICL may have a maximum of 64 slave station addresses, with digital locations and necessary data types for devices are stored in the I/O configuration table.
- Block Request Table: Specifies what information the remote will broadcast to other devices over the C-link and information received will be written into the station public memory.
- Blocks List: Stores the structure of analog database points (called CQ4 blocks in the HFC system) so that they may be called by the equations file.
- Block Data File: Contains the static data about the blocks. This static data includes the types of algorithm used and internal configuration parameters required by each.

In the C-link, each node is referred to as a 'remote' and given a specific number. Each C-Link processor's remote regulates, interfaces, receives, and validates messages sent over the C-link using a Master-For-a-Moment token passing method [88]. C-Link processor only interacts with the other processors in the same controller only through the Public Memory [88]. The C-link uses a network interface chip transmission buffer to store outgoing and incoming data before broadcast or transfer [88].

The ICL processor uses a proprietary design to control communications between a controller and its respective I/O modules [88]. The ICL processor works as master with all IOs operating as slave nodes, constituting a closed and single network. The ICL will always be the

instigator in communication with its devices [88]. In regular communication, the ICL will request updates from input channels or send digital images to the output channels. The ICL can also send ‘special messages’ which include diagnostic requests, secondary loop back requests, memory read/write commands, and more [88].

4.1.2 The I/O Cards

Each I/O card uses an onboard 16 bit processors [90]. These processors contain firmware code written in EPROM for initialization, diagnostics, ICL communication, I/O scan, and data processing functions. These processes are nearly identical for all I/O regardless of types, with the exception of the scan and data processing functions which are unique and based on the type of I/O [90]. I/O modules include onboard LEDs for visual status indication, jumpers for configuration options, signal processing capabilities for each input, and similar card edge connectors.

The I/O typically runs a single string of routines [90]. First, the I/O scan, in which input channels are read or the current image from memory is written to output channels. Data processing is next executed if necessary. After, self-diagnostic routines constantly check for errors or unintentional changes in code and memory until the next schedule I/O scan.

4.1.3 Engineering Workstation (EWS)

The Engineering Workstation (EWS) is the combined hardware and body of software responsible for writing and compiling software to the HFC [91]. It gives the user a single set of tools to create, read, or modify all application software in the system and is capable automatically documenting all worked performed by engineers or operators on the EWS [91].

There are limited database structures that can be created and recognized by the HFC. These structures are outlined in Table 4.1[91].

Table 4.1: Valid Equation Point Types.

Point Type	Definition	Structure
BL	Block Value	8 Bytes
CO	Counter	2 Byte Integer
DI	Digital Input	2 Byte Quality Word
DO	Digital Output	2 Byte Quality Word
DG	Digital Group	6 Byte Data Structure
FL	Flag	1 Bit
MS	Message	2 Byte Quality Word
RR	Remote Status	1 Bit Flag within 5 Byte Field
ST	CQ4 Strategy	11 Byte Structure
TI	Timer	1 Byte Status and 2 Byte Integer
VA	Value	2 Bytes (Integer) 4 Bytes (Floating Point)

These point types constitute the data structures that are usable within the equations list program. The coding may be configured as either structured text or ladder logic in compliance with IEEE Code 61131-3 [69].

These are written and operated using the Equations Editor (EE) custom software [91]. The equations editor gives the engineer access to the five files of the SBC06 discussed previously. To facilitate debugging or observation of code, the EE may ‘Monitor’ activities. When active, the EE will show the values of all blocks, inputs, outputs, flags, counters, etc. while the program runs. These values are only updated per second for the benefit of the operator/engineer [91].

The EWS includes the Memory Editor application which allows an operator to read from the remote directly [91]. The user is thus able to read statuses (with knowledge of the bit field of the point type), observe digital and analog inputs and outputs, and write directly to the

remote. The Memory Editor is also able to requests statuses from devices and take roll calls of all modules, remotes, and blocks on the C-link [91].

4.2 Soft Boundaries

As outlined previously, the heater-independent parameters possess a degree of variability. Particularly, the nature of pressurized flow causes the primary flow rate to be inherently noisy [32] and pressurizer level produces quickly fading transients in response to operating point changes. In order to adequately provide protection for the NPCTF, the history of operations was used as a basis for creating 'soft boundaries'. These boundaries would only result in a trip if a breach persisted for several moments.

Soft boundaries allow operating bounds to remain stringent without needless risk of spurious tripping. To determine the appropriate 'softness' for boundary breaches, investigations of NPCTF operating history were examined. Hypothetical tripping thresholds were investigated for expected breaching frequency and maximum lengths. From these, tripping set points and permissible breach lengths were decided.

The soft bounds approach is also used in CANDU tripping logic [33]. In CANDU, the primary loop over pressure condition uses two tripping set points [34]. At the first set point, a relief valve is opened and a timer is set. If the relief valve does not clear the issue within three seconds of initial breach, a trip occurs [34]. Contrarily, the second tripping set point immediately initiates a reactor trip [34].

Following this precedence, it was determined that set points shall utilize three second buffers. Especially safety-sensitive bounds such as reactor power (paralleled through C2) and moderator temperature (paralleled through T2) should never be given soft boundaries.

However, the heater-independent parameters do not present the same immediate action requirement. Thus, three second soft boundaries are reasonable to recognize the presence of faults without compromising system safety.

4.2.1 Primary Line Flow (F1)

Primary line flow, as all pressurized flow measurements, is inherently noisy [32]. The primary line flow was chosen to, like CANDU [33], utilize only a lower limit. Too little flow is a danger due to inadequate cooling to the reactor, though a high flow rate possesses no inherent dangers so long as pressure is maintained.

Table 4.2: Breaching Characteristics of Primary Flow Rate as a Function of Lower Boundary Point.

Boundary (l/min)	Breaches/Day	Longest Breach	Time Breaching/Hour
5.6	0.00	0	0.00
5.625	0.00	0	0.00
5.65	16.59	1	0.69
5.675	99.52	1	4.15
5.7	442.23	1	18.43
5.725	1559.10	1	64.96
5.75	**3875.63**	**2**	**161.71**
5.775	7751.26	2	325.04
5.8	12876.38	2	541.35
5.825	21860.54	2	928.13
5.85	33349.21	5	1482.85
5.875	45385.22	7	2299.48
5.9	52705.24	10	3326.21
5.925	54087.42	16	4569.94
5.95	53180.71	27	5822.43
5.975	50936.06	41	7094.72
6	48492.36	94	8381.07

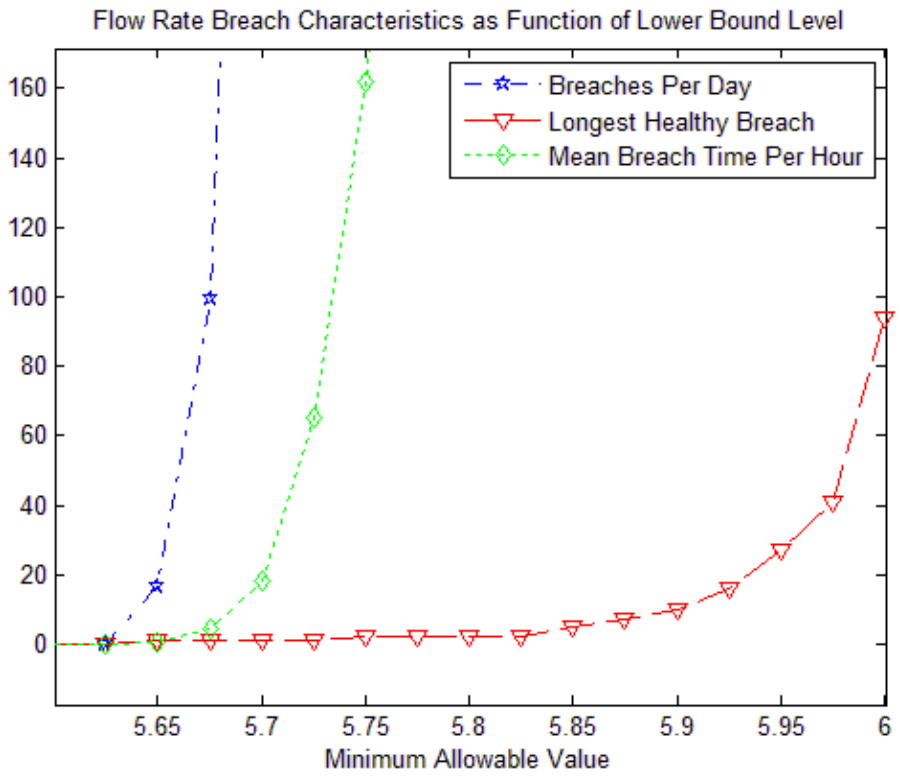

Figure 4.2: Breaching Characteristics of Flow Parameter as a Function of Lower Boundary Point.

The characteristics of the flow rate in relation to the boundary point are shown in Table 4.2 and Figure 4.2. As Table 4.2 shows, operating history suggests that normal operations will never breach a set point of 5.625 l/min. However, to tighten the operating limits and utilize CANDU paralleled 3s maximum breaching, the set point was set at 5.75 l/min. A theoretical 3875 breaches are expected to occur at daily this set point though none longer than 2s. The flow rate is anticipated to be below this boundary set point for an expected 162s every hour.

A 3s breach of this set point creates a strong indicator for the presence of a fault. The 5.75 l/min limit is demonstrated for the primary flow in Figure 4.3. Sample points from faulty trials are included in Figure 4.3 to display characteristics of primary flow during adverse conditions. As shown, many faults, though not all, would disrupt flow and could thus be identified.

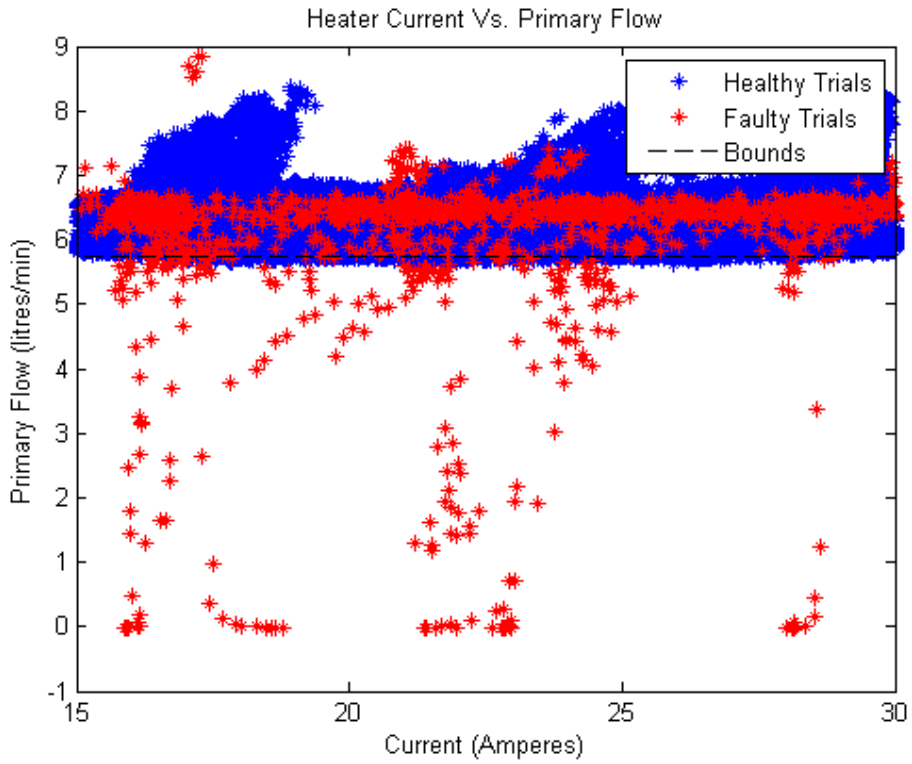

Figure 4.3: Characteristics of Primary Flow Rate in Healthy and Faulty Operating States.

4.2.2 Primary Line Pressure (P1)

For primary line pressure, the set points that would be needed if soft boundaries were not an option would be 7.2 PSI(g). However, as proof of concept, a two second boundary could be placed at 7.25PSI(g) as shown in Table 4.3. This 0.05PSI(g) difference leads to an average of almost 28 breaches per day, with an estimated average of only 1.61s of breaching per hour. Indicative of primary line pressure's characteristics, an additional 0.0725PSI(g) would have increased the longest permissible breach from 2s to 11s. The exact progression of the boundary in relation to its breaching characteristics is shown in Table 4.3 and Figure 4.4.

Table 4.3*:* Breaching Characteristics of Primary Line Pressure as a Function of Lower Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
7.150	0.00	0	0.00
7.175	0.00	0	0.00
7.200	0.00	0	0.00
7.225	5.53	1	0.23
7.250	**27.64**	**2**	**1.61**
7.275	33.17	2	1.84
7.300	204.56	4	11.75
7.325	619.22	11	41.47
7.350	1288.19	27	109.65
7.375	1730.49	27	198.11
7.400	2095.38	85	308.69

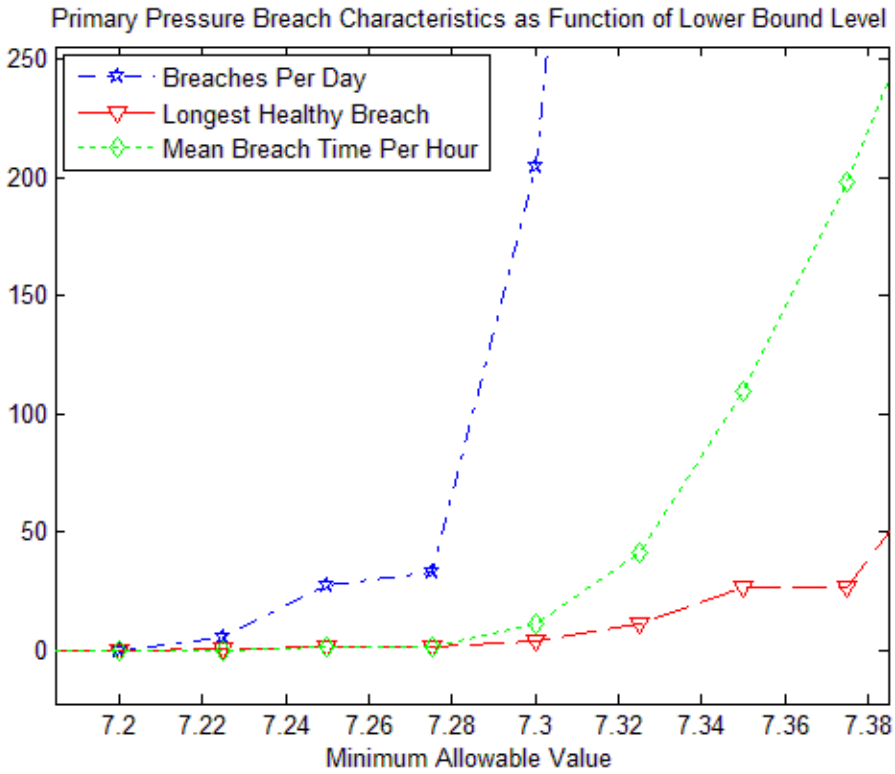

Figure 4.4: Breaching Characteristics of Primary Line Pressure as a Function of Lower Boundary Point.

The 7.25PSI(g) lower soft boundary was matched to an upper soft boundary of 10.5PSI(g). This was found using the information in Table 4.4 and Figure 4.5. The operating history necessitated a maximum breaching time of 2s. This turned the only two second timer

used in the safety algorithm. The next reasonable boundary, 10.45 PSI(g) have forced a maximum permissible breach of at least 9s. This is too long for fault detection. While the boundary could be set 10.525 as a hard limit, the 10.5PSI(g) point still saw a theoretical 22 breaches per day that could incorporated into the protection scheme.

Table 4.4: Breaching Characteristics of Primary Line Pressure as a Function of Upper Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
10.200	93.99	76	29.26
10.225	105.05	55	25.57
10.250	116.10	28	22.58
10.275	99.52	22	17.97
10.300	99.52	17	13.82
10.325	93.99	17	10.14
10.350	60.82	17	8.29
10.375	38.70	17	6.22
10.400	16.59	17	4.38
10.425	16.59	16	4.15
10.450	11.06	9	3.46
10.475	27.64	1	1.15
10.500	**22.11**	**1**	**0.92**
10.525	0.00	0	0.00
10.550	0.00	0	0.00
10.575	0.00	0	0.00
10.600	0.00	0	0.00

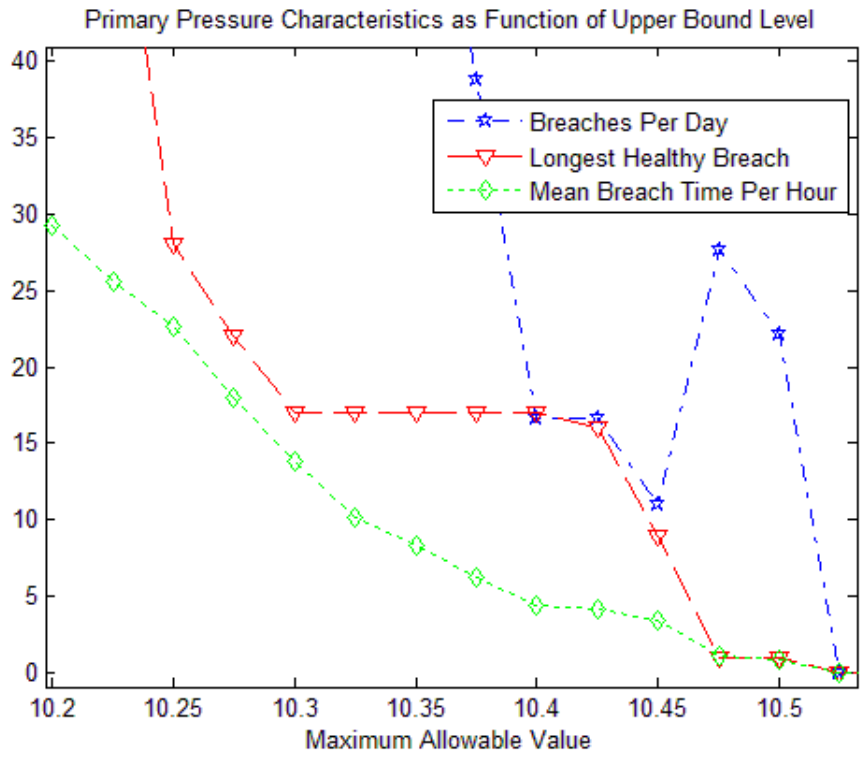

Figure 4.5: Breaching Characteristics of Primary Line Pressure as a Function of Upper Boundary Point.

Notice that the breaches per day decreases when the boundary is moved from 10.475PSI(g) to 10.45PSI(g). This is due longer breaches being considered a single instance, whilst noise along boundaries are counted as many short boundary trespasses.

The primary line pressure was therefore granted a 3.25PSI(g) operating envelope. The total operating range compared against the heater current is shown in Figure 4.6. The upper boundary was a poor indicator of faults in the data collection trials, as it was never breached during fault insertion. The lower boundary was the opposite, with sudden pressure drops being a common result of faulty conditions.

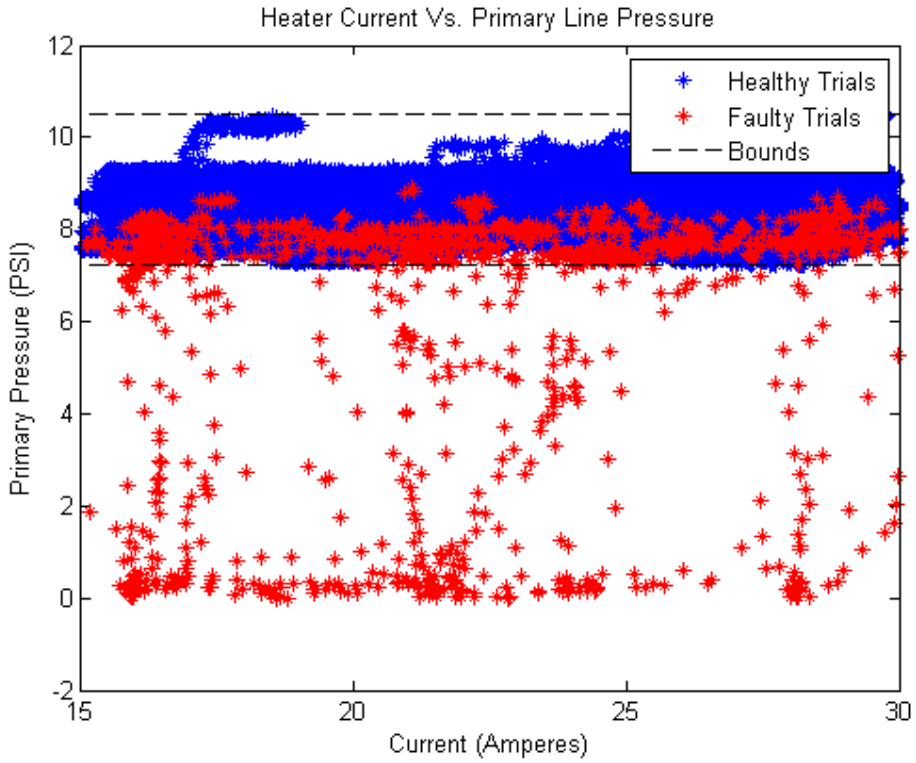

Figure 4.6: Characteristics of Primary Pressure in Healthy and Faulty Operating States.

4.2.3 HX Tank Pressure (P2)

Though HX tank pressure was not prone to responding to inserted faults, steam generator pressure is part of CANDU's safety system design. HX tank pressure, as steam generator pressure's parallel on the NPCTF, was necessary to include. It must be noted that the high pressures, temperatures, and potential for primary-to-secondary leaking in steam generators make their monitoring vital [38]. Table 4.5 and Figure 4.7 show the breaching characteristics of the HX tank as a function of its lower operating bound.

Table 4.5: Breaching Characteristics of HX Tank Pressure as a Function of Lower Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
3.100	0.00	0	0.00
3.125	0.00	0	0.00
3.150	0.00	0	0.00
3.175	0.00	0	0.00
3.200	**0.00**	**0**	**0.00**
3.225	11.46	8	3.58
3.250	5.73	60	14.33
3.275	5.73	60	14.33
3.300	5.73	61	14.56
3.325	5.73	61	14.56
3.350	5.73	62	14.80
3.375	5.73	63	15.04
3.400	5.73	64	15.28
3.425	5.73	66	15.76
3.450	28.65	68	20.78
3.475	114.61	134	100.04
3.500	143.26	281	172.63

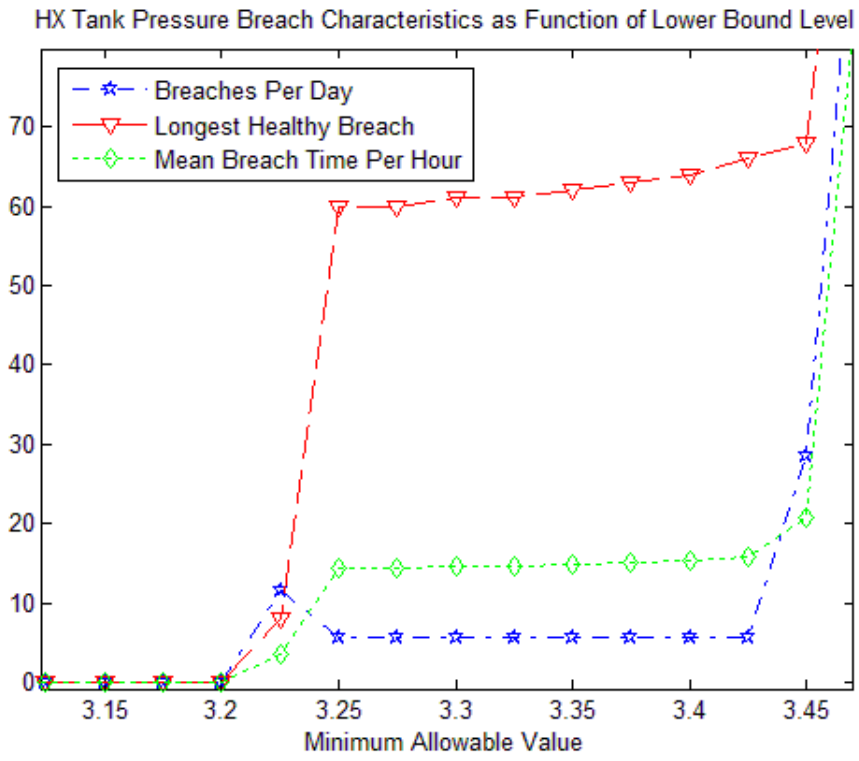

Figure 4.7: Breaching Characteristics of HX Tank Pressure as a Function of Lower Boundary Point.

As is shown, HX tank pressure does not exhibit a significant noise nor is it prone to quickly fading transients. HX tank pressure keeps steady values that change slowly. Thus, the soft boundary principle could not be applied and traditional set point for tripping was set. As can be seen, from the chosen lower set point of 3.2PSI(g) a rise of just 0.025PSI(g) moves the longest recorded healthy breach to 8s with an expected 11.5 breaches per day. These breaches were determined to be too long to be safely considered and thus the 3.2PSI(g) hard set point was necessary.

Table 4.6: Breaching Characteristics of HX Tank Pressure as a Function of Upper Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
5.550	17.19	88	30.56
5.575	28.65	43	22.21
5.600	17.19	34	11.94
5.625	5.73	13	3.10
5.650	**0.00**	**0**	**0.00**
5.675	0.00	0	0.00
5.700	0.00	0	0.00
5.725	0.00	0	0.00
5.750	00.00	0	0.00

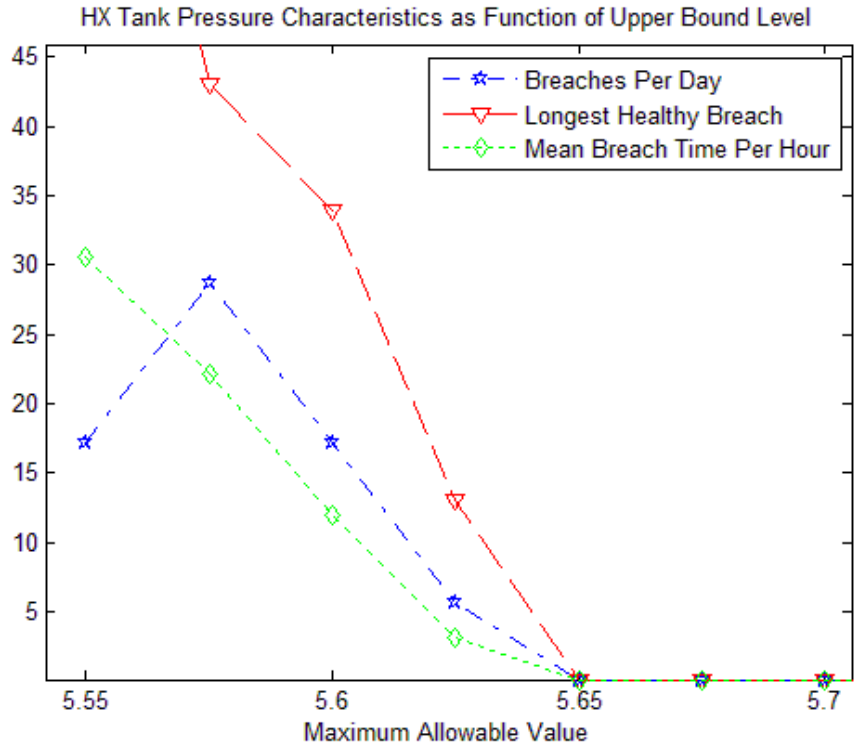

Figure 4.8*:* Breaching Characteristics of HX Tank Pressure as a Function of Upper Boundary Point.

The upper boundary presented similar breaching characteristics, as shown in Table 4.6 and Figure 4.8. The inherent nature of HX tank's pressure required 5.65PSI(g) to be chosen as a hard upper set point. A pressure as high as 5.65PSI(g) had never been met or breached during healthy operation. Because of this, it is believed that breaches of this bound are abnormal enough to provoke immediate response.

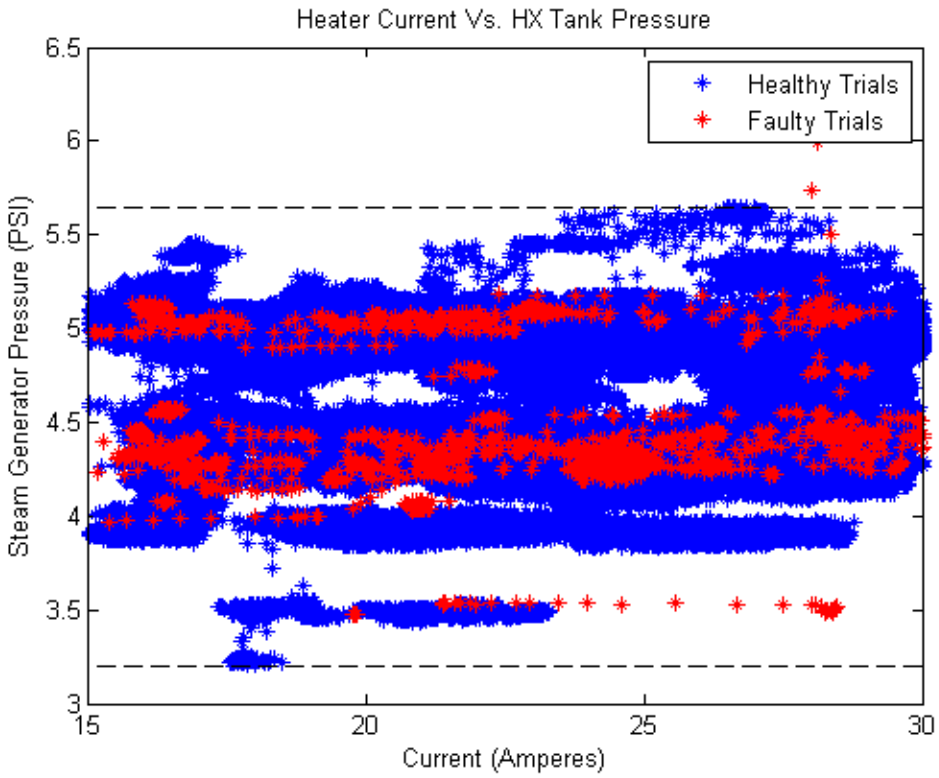

Figure 4.9: Characteristics of HX Tank Pressure in Healthy and Faulty Operating States.

The final operating range permitted HX tank pressure to operate between 3.2PSI(g) and 5.6PSI(g). Operation history shows that the HX tank's pressure would not exhibit behaviour in response to other conditions on the NPCTF. The HX tank pressure also was not a strong indicator of faults in the system, as demonstrated in figure 4.9. However, for the reasons discussed, boundaries on safe operations must remain. The safety system therefore immediately responds to pressures outside of the previously observed envelope.

4.2.4 Pressurizer Tank Level (L3)

Pressurizer tank level was arguably the best indicator for the existence of faults in the NPCTF (as will be demonstrated section 5.5: Experiment 2: Emergency Scenarios). The pressurizer level remains stable during normal operations. However, when the operating point

on heater outlet temperature is changed, the pressurizer tank level produces a quickly fading transient.

The pressurizer tank level remains near its operating point of 50%. The investigation showed a drop of 0.5% to lower boundary produced 2s maximum healthy breach. This is shown in Table 4.7 and Figure 4.10 with the 49.5% boundary theoretically producing less than six breaches daily. The pressurizer level's variations, even at the transients, was slight enough than an additional 0.1% produced no historical record of a breach during healthy conditions. The consistency in the breaches per day in the second column of Table 4.6 show that pressurizer transitions tended to dip the pressurizer level to near 49.425% before returning to the operating point.

Table 4.7*:* Breaching Characteristics of Pressurizer Tank Level as a Function of Lower Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
49.350	0.00	0	0.00
49.375	0.00	0	0.00
49.400	0.00	0	0.00
49.425	5.59	1	0.23
49.450	5.59	1	0.23
49.475	5.59	1	0.23
49.500	**5.59**	**2**	**0.47**
49.525	5.59	6	1.40
49.550	78.28	6	4.66
49.575	2918.82	12	184.76
49.600	5764.96	69	797.50

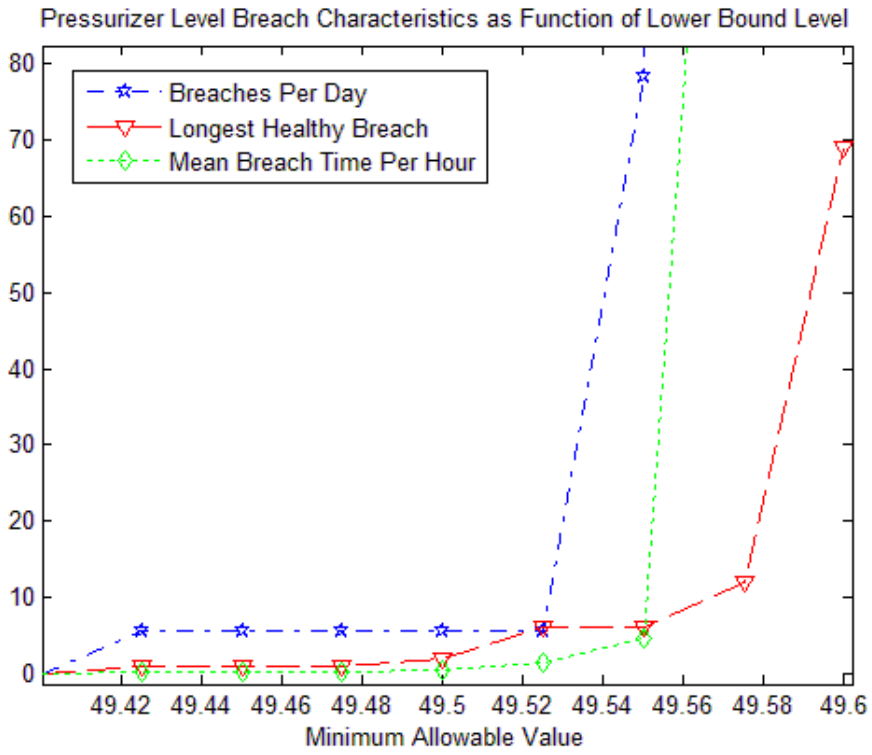

Figure 4.10*:* Breaching Characteristics of Pressurizer Tank Level as a Function of Lower Boundary Point.

The upper boundary produced similar characteristics as a 51.5% threshold gave identical characteristics in breaches per day, longest breach, and estimated time breaching per hour. The same number of breaches per day is expected for boundaries from 51.425% to 51.6%. This indicates the parameter would only occasionally travel from its operating point before steadily returning. Choosing the 51.5% soft boundary comfortably placed a 3s timer on breaches. This is outlined graphically and in detail with Figure 4.11 and Table 4.8 respectively. From these, it is possible to deduce that the pressure's progression back to the operating point slowed as it neared its previous value.

Table 4.8*:* Breaching Characteristics of Pressurizer Tank Level as a Function of Upper Boundary Point.

Boundary	Breaches/Day	Longest Breach	Time Breaching/Hour
51.350	229.26	31	53.82
51.375	201.30	5	11.88
51.400	22.37	5	1.86
51.425	5.59	3	0.70
51.450	5.59	2	0.47
51.475	5.59	2	0.47
51.500	**5.59**	**2**	**0.47**
51.525	5.59	1	0.23
51.550	5.59	1	0.23
51.575	5.59	1	0.23
51.600	5.59	1	0.23

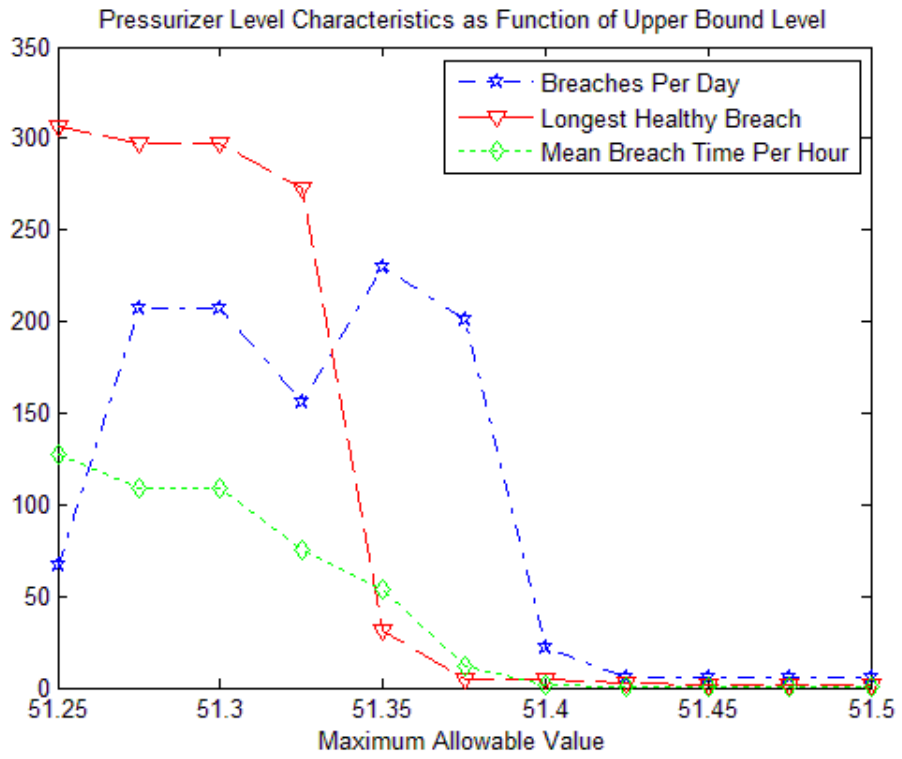

Figure 4.11*:* Breaching Characteristics of Pressurizer Tank Level as a Function of Upper Boundary Point.

As demonstrated in Figure 4.1.11, when a fault occurs, the level of the pressurizer tends to drop as the pressurizer attempts to maintain pressure in the system. The level's deviation from its normal operating bounds between 49.5% and 51.5% was almost always indicative of

a fault. It is visible in Figure 4.12 that increases in pressurizer level due to faults is not as common of a characteristic.

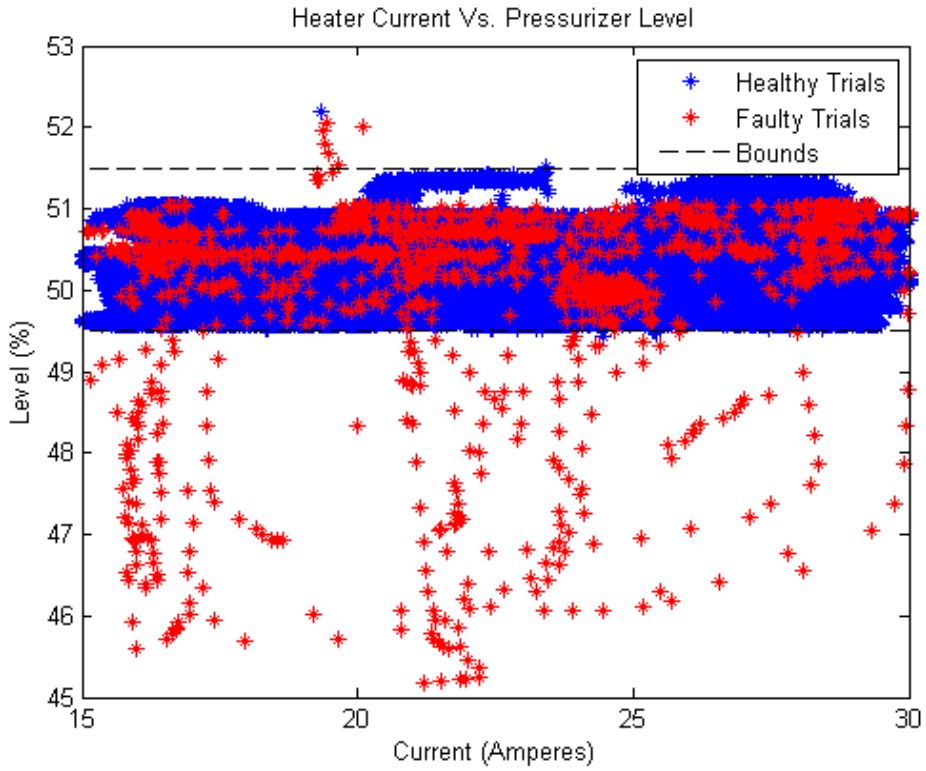

Figure 4.12: Characteristics of Pressurizer Level in Healthy and Faulty Operating States.

4.3 Description of Implemented Monitoring Software

The development of the safety algorithm necessitated several steps to be created. First, the investigation of NPCTF operating characteristics was performed with results as discussed in section 4.1. This was done over fifty hours of non-continuous operation on the NPCTF. The NPCTF uses a data-logger that samples each system parameter every second on a 72 hour continuous loop [2].

The data logger exported the recordings to a CSV file where they were converted to excel then read by Matlab. The data logger works on a continuous loop such that the most

recent sample point is the exact moment the data is extracted. As not all NPCTF recordings can be converted to CSV simultaneously, corrections for time difference were performed.

Matlab scripts were written to sort the data into usable and organized portions. Using current to the heater as a reference, a parallel to neutron power on CANDU systems [93], points of activity were isolated and similar operations grouped. Initial results were presented in section 3.2: Key Operating Parameters. This allowed statistical analysis after a high-level overview sorted the data by type (healthy, faulty, steady state, transitional, etc.).

Later, the sorting algorithm was utilized to investigate the faults' theoretical responses from the safety algorithm. Though signals from internal calculations on the HFC could not be recorded, these Matlab simulations provided a framework to estimate the algorithms functioning. For more on this, see section 5.1 Matlab Simulation and Verification Tests.

Observation was performed primarily on CANDU safety parameter parallels. However, control valves were also observed. The safety algorithm created imitates CANDU safety logic, though has been built for the NPCTF, for which bounds, settling times, and responses to state changes are all based.

4.3.1 Algorithm Overview

The algorithm utilizes operation history on the NPCTF to anticipate future operations. Though safety systems do not participate in control of an NPP [94], their development requires knowledge of normal operations as discrepancies between observed and anticipated may indicate faults. However, because safety systems are not control systems, it is not able, responsible, or accountable for correcting perceived errors [94].

The NPCTF flow of operations is therefore imitated in the safety algorithm. The safety systems expectations of operations are used determine when faults exist. The overall flow of the safety system as it monitors the NPCTF is described functionally in Figure 4.13

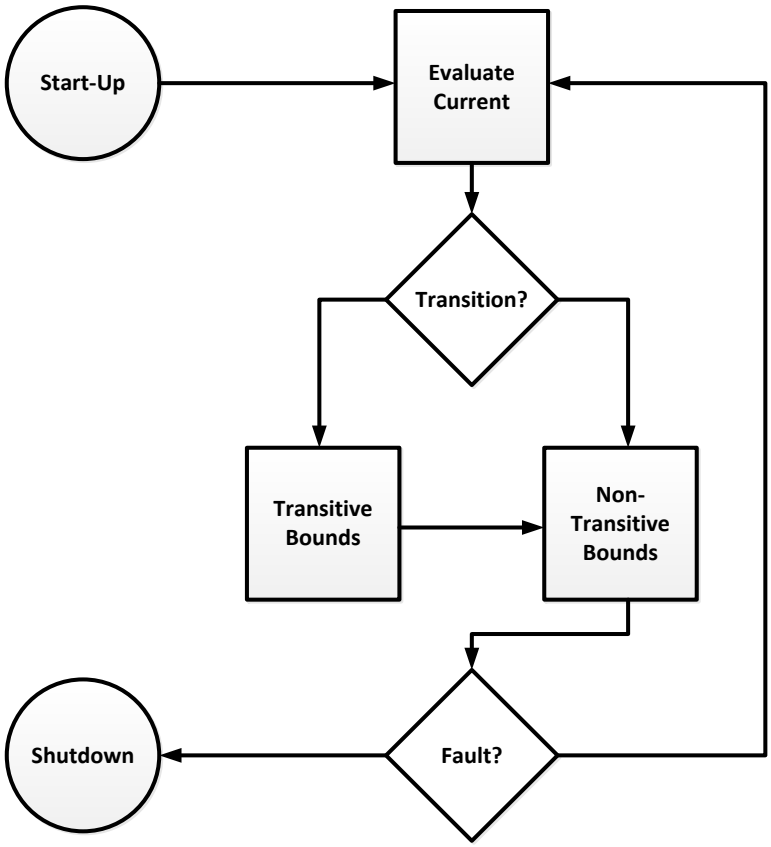

Figure 4.13: Overview of Safety Algorithm.

Figure 4.13 shows the general overview of the major operating features of the algorithm. The major operations are as follows. Each is further expanded upon in the following subsections.

- **Start-Up:** Handles low power state of NPCTF. Recognizes when operations have begun through monitoring of current. When operations are determined to have begun, start-up procedures pass off to the main operating loop.

- **C2 Tracker:** Distinguishes the NPCTF's operating point. Performs this task utilizing C2 signal as parallel to CANDU neutron power. Relies on several seconds of memory and thus requires substantial memory. C2 tracker is responsible for noticing and characterising the current spikes which precede transitions. May jump to shut down if C2 begins to deviate from normal ranges.
- **Non-Transitive Building:** Builds boundaries using flags set by C2 tracker and other subsections. Heater-independent parameters are first calculated. Calculates heater-dependent boundaries if transition flag is inactive, otherwise jumps to transitional boundaries subsection.
- **Transitive Boundaries:** Collection of four blocks in 4.13: Heat Up, Heat Down, Level Up, and Level Down. Each contains two stages that anticipate and monitor heater-dependent parameters through transitions. Use calculations requiring flags from C2 Tracker and one another.
- **Check Boundaries:** Parameters are compared against their tripping set points. If one of the five soft boundaries is breached, a timer begins. If a timer expires or one of six hard boundaries is bypassed, a trip signal is sent. If a trip is not necessary, the program jumps to the C2 tracker.

4.3.2 Start-Up Procedure

Start-up procedures are the necessary first tasks. Their collective duties are to initialize the program then stand-by until power output dictates a jump to operations. Like CANDU, the NPCTF continues to monitor C2 and T2 in this low power state. However, conditional bounds are not yet being checked against.

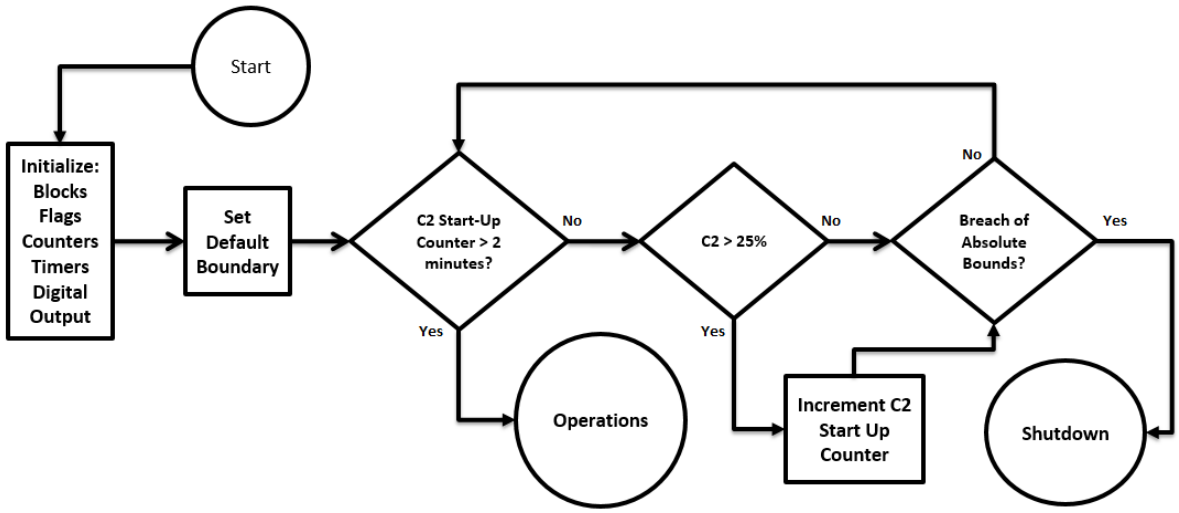

Figure 4.14: Functional Block Diagram of Start-Up Procedures.

The flow chart of the start-up subsection is shown in Figure 4.14. It contains three major sections:

- **Initialization:** All data blocks on the HFC are configured and initiated appropriately. This includes analog inputs, which must have scan times and remote numbers designated. Flags, counters, and digital inputs are set to logic low to protect against aberrant start values. All timers must be created and given pre-set values. Default tripping set points are set, though only absolute set points will be checked against.
- **Start-Up Monitoring:** Current is monitored for magnitude above 25% of its maximum value. This is below the lowest operating range but indicates operations are beginning. CANDU plants utilize a 2% full-power threshold to distinguish active to inactive states [94]. After approximately two minutes above 25%, transients of start-up are finished and normal operating procedures may begin. It must be noted the 35°C operating point is unobtainable after two minutes and may not be the initial state.
- **Absolute Threshold:** Heater current and temperature are monitored. As absolute thresholds, excessive heat or current require observance at all times. Heater

temperature (T2) is compared against the upper bound of 30°C as this is the highest possible initial operating point.

4.3.3 Boundary Procedure

After start-up, the safety system runs a single continuous loop. The boundary procedure is responsible for setting operating limits and comparing these against system parameters. The general overview of the boundary procedure is shown in Figure 4.15.

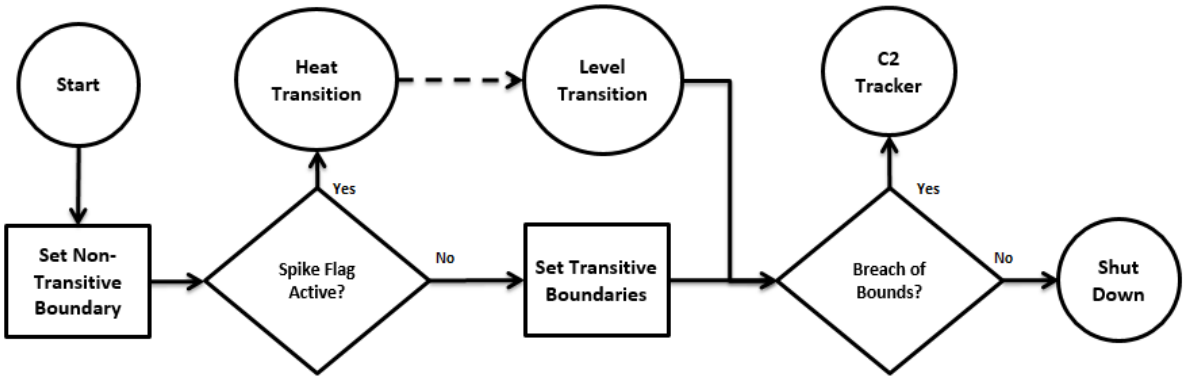

Figure 4.15: Functional Block Diagram of Boundary Checking Procedure.

The boundary procedure assumes that the appropriate flags have been set by the C2 tracker so it can build the appropriate bounds or know to outsource this to other subprograms. The procedure operates as follows:

- **Non-Transitive Bounds:** As the heater-independent parameters utilize persistent operating bounds, they are set first. These boundaries are declared at each iteration as a safeguard against corrupted or lost data.
- **Transitive Boundaries:** The 'spike' flag indicates a transition state in the NPCTF. If this is active, the boundary routine jumps to the heat transition. After both temperature and HX tank level boundaries have been set, a jump returning to the boundary

procedure is performed. If the flag is inactive, the heater-dependent parameters are set according to operating point.

- **Boundary Test:** The parameters are compared against their created threshold. For soft boundary breaches, timers continue to decrement. Soft-bounds not breached reset their respective timers. If timers have expired or hard thresholds have been breached, a trip will occur. Should no trip be necessary, the algorithm jumps to the C2 tracker.

4.3.4 Heater Current (C2) Tracking

The heater current (C2) tracking subroutine requires significant data, approximately 25% of total memory used. The C2 tracker utilizes heater current history to perform three major tasks: First, it determines the present operating point. Next, it notices, characterizes, and tracks operating point transitions. Finally, it observes C2 for drift of aberrant behaviour. An overview of its functioning is presented in Figure 4.16 and expanded upon below.

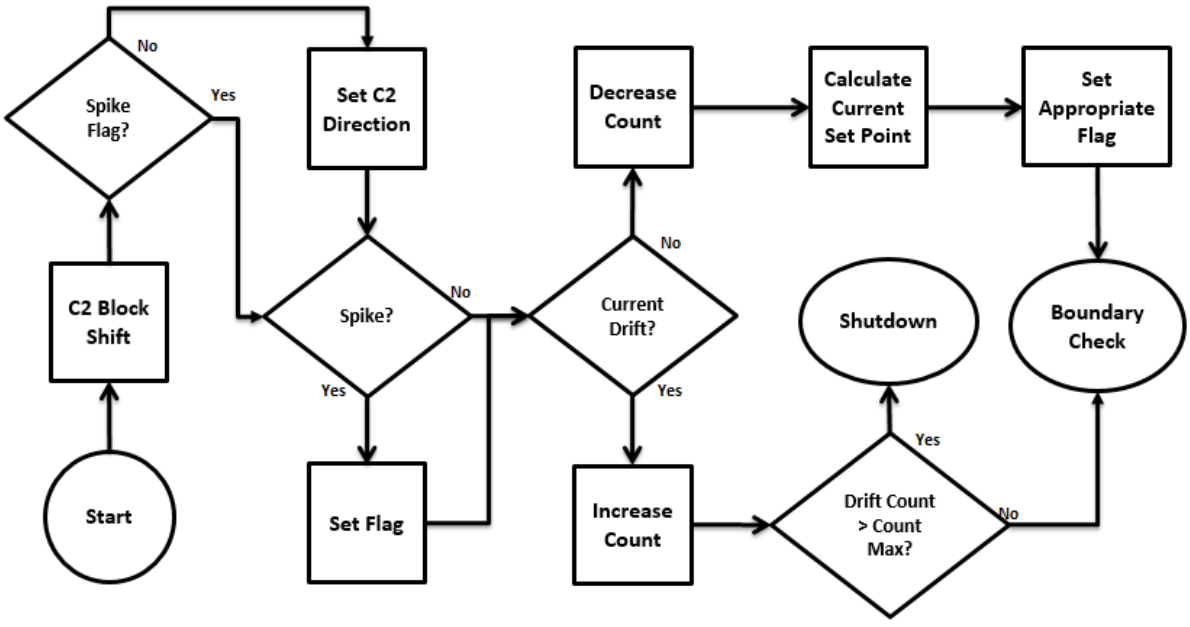

Figure 4.16*:* Functional Block Diagram of Current Tracking Program within Safety Algorithm.

- **Block Shift:** A memory shift of C2 recordings is performed. Each recording is shifted one stage with the oldest being overwritten. A new recording is placed into the first memory location.
- **Spike/Transition Detection:** C2 will always spike in response to an operating point change. As such, current spikes signal transitional procedures. Should no spike flag be active, C2 is compared to the second-most recent measurement to determine directional change. A C2 spike check is then performed. If a new spike is found, the direction is already known and the flag is set. This flag remains set until cleared manually.
- **Current Drift:** In CANDU, reactor control mechanism keep neutron power stable [12]. As parallel, the algorithm monitors C2 to ensure unintentional drift does not occur. C2 is compared to a look-up table for appropriate measurements based on operating point. If outside this range, a counter is incremented. This counter monitors for 2s of non-continuous drifting and trips upon occurrence. Drift is automatically false during transitions.
- **Operating Point Determination:** During transitions, it is necessary to determine the new operating point. Current is considered settled if two minutes non-continuous are spent within that range. This uses a penalty method: decrements occur when the range is exited. Upon settling, the appropriate flag is set. This flag is used in boundary and drift checks.

4.3.5 Heat Transition Algorithm

As heater temperature varies with set-point, proper handling of its transitions is required. Monitoring ensures a safe and predictable progression. The handling for temperature

transitions is similar for increases and decreases in set point, allowing a single sub process to be used. This process is shown functionally in Figure 4.17.

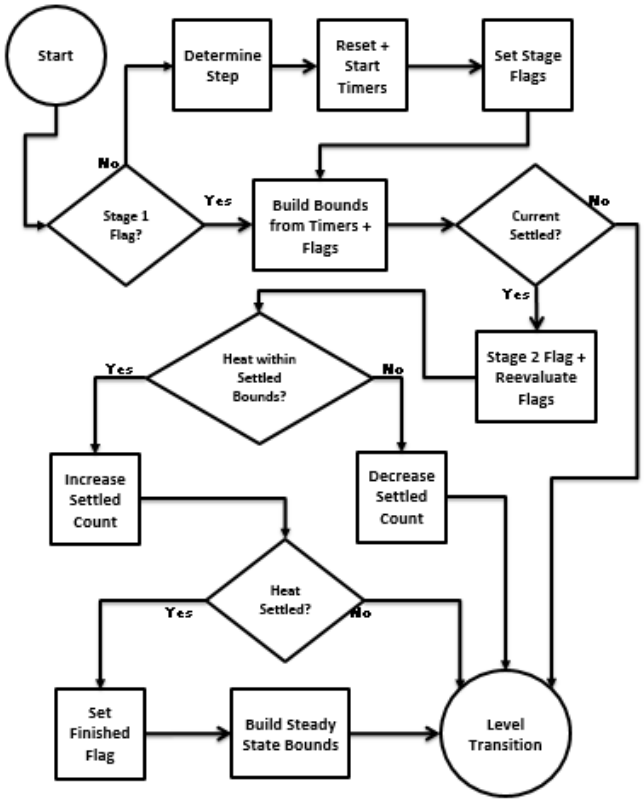

Figure 4.17: Functional Block Diagram of Heat Transition Program within Safety Algorithm.

- **Initialization:** Initialization is performed on behalf of both transitional subprograms. Flags from the C2 tracker determine the most likely step being taken. Timers are set and started for all transitions, regardless of likely step. Upon completion, the ‘stage 1’ flag is set so initialization is not repeated.

- **Bounds:** Bounds are established using step flags, transition timers, and stage flags. As transitions occur near quadratic fashion, the general boundary transition formula used is:

$$Bound = Destination - \frac{(Destination - Initial)}{Transition\ Time\ Total^2}(Time\ Remaining)^2 \frac{1}{Factor} \quad (8)$$

  This permits smooth transitions between two operating states. The 'factor' is a constant that jumps the transition part way to the next boundary immediately. This was necessitated by the quick change at the beginning of transitions. The factor was 3.5 for leading bounds (upper in upwards steps and vice versa) and 1 for the lagging. This value was found empirically to perform in all investigated transitions. When multiple steps were possible, the highest upper and lowest lower bound plausible were used until the correct step was identified.

- **Current Settling:** Current must settle for the transition to continue, though this is quick compared to other parameters. When detected, the flags are re-evaluated so step-uncertainty may end. The stage 2 flag is set and temperature settle tracking may begin.

- **Temperature Settling:** Heater temperature is monitored for settling within the projected range. This requires 40s within the final range, using a penalty method. When temperature has settled, a flag is set, and tripping thresholds are built using values of regular boundary operations.

4.3.6 Level Transition Algorithm (Up)

HX tank level transitions required different subsections based on direction of step. This is due to magnitude difference of inverse response characteristic (IRC) and overshoot. Upwards HX tank level transition have smaller IRCs and greater overshoot. A flow chart of the level transition algorithm (up) is presented in Figure 4.18.

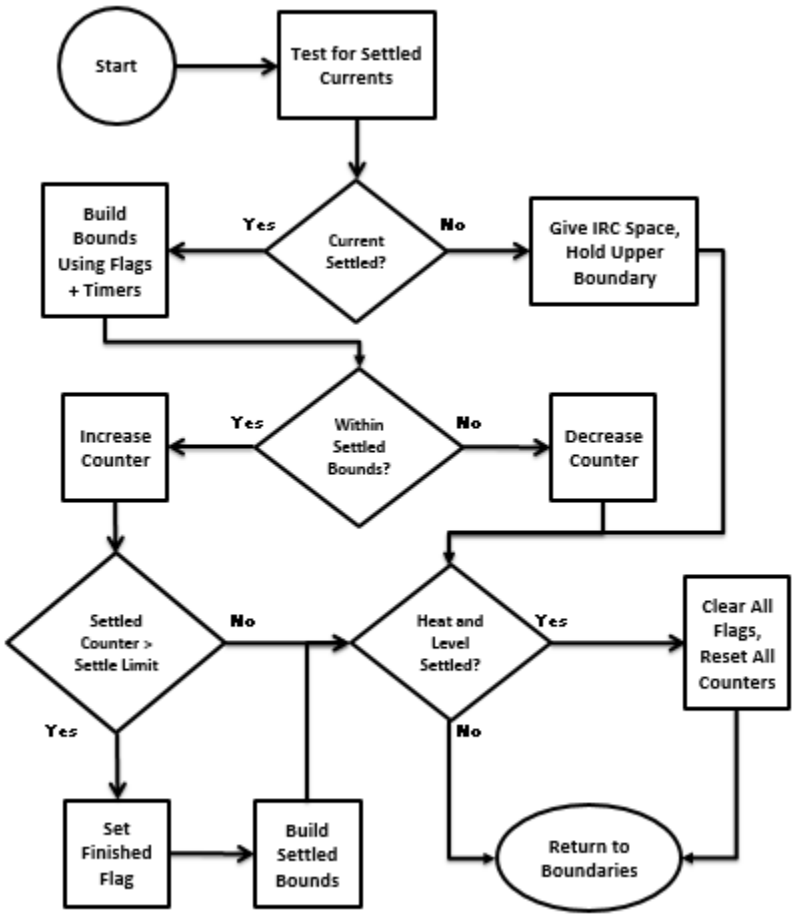

Figure 4.18: Functional Block Diagram of Level Transition (Up) Program within Safety Algorithm.

- **Test for Settled Current/Stage 1:** Upwards steps begin with a delay or small IRC. The lower boundary is lowered slightly to accommodate possible IRC. Upper boundary is unchanged. Current settles within 40s and signals the beginning of stage 2.

- **Bounds:** Using flags set by the C2 tracker, transitional bounds are built. No uncertainties exist as current has already settled. The lower bounds progress according to:

$$Boundary = Destination - \frac{(Destination - Initial)}{Total\ Time}(Time\ remaining) \quad (9)$$

  This guides the lower boundary smoothly, and requires no factor term. The upper boundary is immediately set to 10% over its maximum value to accommodate overshoot. HX tank level variability and overshoot make a transitive upper boundary implausible.

- **Level Settling:** The level is monitored for settling. This is defined as 2 minutes non-continuous within final range with penalty for exiting. The penalty and length required prevents falsely flagging settling while overshoot persists. Overshoot may persist for several minutes. When the conditions are satisfied, the settled flag is set and thresholds are calculated using normal boundary procedures.
- **Transition Finish:** When both heat and level flags are active, the transition is finished. All flags and counters of both transitions are reset, including the transition indicating spike flag.

4.3.7 Level Transition Algorithm (Down)

The level transition algorithm (down) is separated due to the significant IRC exhibited. The IRC is so pronounced that the stages of the level-down subroutine are separated by its completion. The process is shown in Figure 4.19.

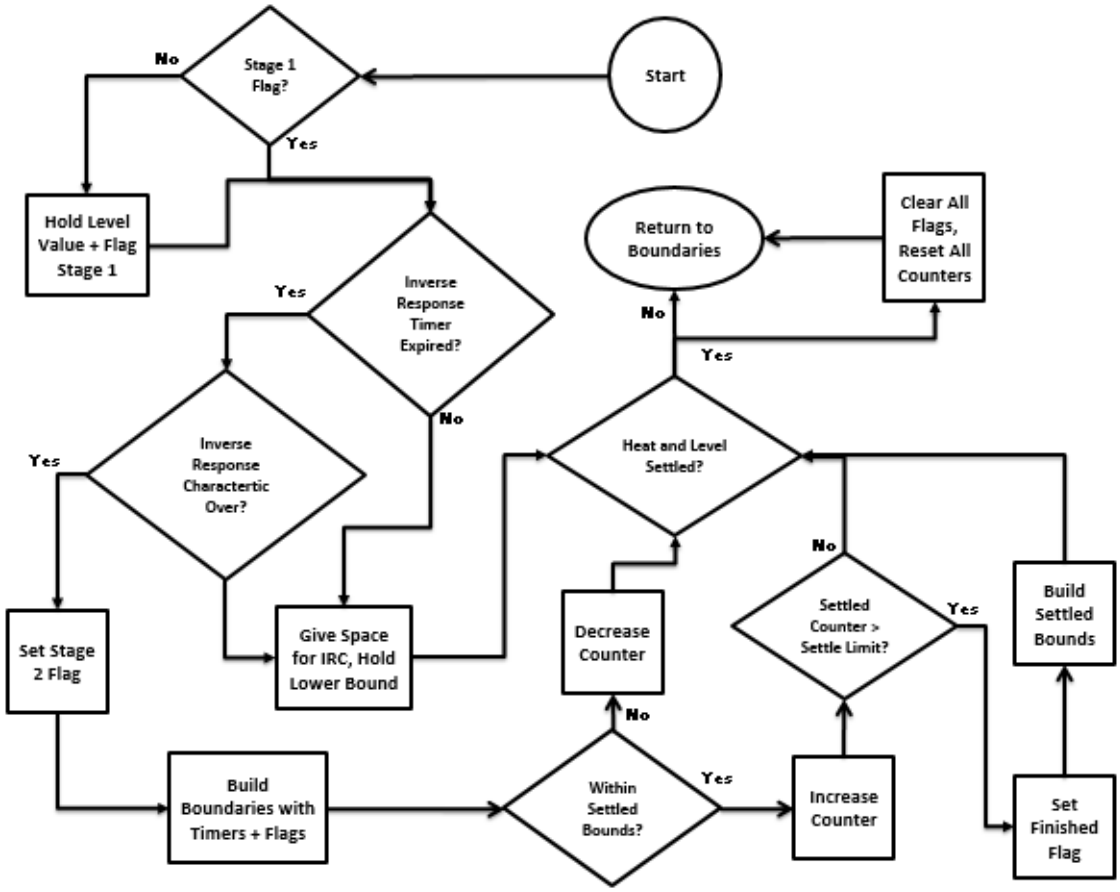

Figure 4.19: Functional Block Diagram of Level Transition (Down) Program within Safety Algorithm.

- **Initialization:** The initial HX tank level is recorded so it may be compared against later. The stage 1 flag is set so this value is not rewritten.
- **Inverse Response Characteristic/Stage 1:** The IRC dominates the first stage and must be cleared before progressing. The upper threshold is raised by 20% to give space for the IRC, while the lower is unchanged. A timed delay occurs before checking for completion of the IRC, as there is a delay before the IRC manifests. After the delay, the HX tank level is compared against the value recorded during initialization. When HX tank level is below this point, stage 2 begins.

- **Bounds Building:** Using flags set by the C2 tracker, transitional boundaries are built. This utilizes the same linear equation from the upwards transition for the upper boundary, while the lower boundary immediately takes it final value. Overshoot is negligible and thus not considered.

- **Level Settling:** The level is monitored for settling. This is defined as 2 minutes non-continuous within final range with penalty for exiting. When the conditions are satisfied, the settled flag is set and thresholds are calculated using normal boundary procedures.

- **Transition Finish:** When both heat and level flags are active, the transition is finished. All flags and counters of both transitions are reset, including the transition indicating spike flag.

4.4 Overall System Diagram

The overall connection between the HFC, the NPCTF, and its relevant communication are outlined in detail in Figure 4.20. Note that while the HFC initiates the shutdown during the implementation, this is done through the NPCTF's onboard computer. Further, because the shutdown action of the heater is handled digitally, the shutdown of the heater is again handled through the onboard controller. The separation of heater dependent and heater independent parameters, as well as the flow of logic when characterized in hardware are shown graphically in Figure 4.20.

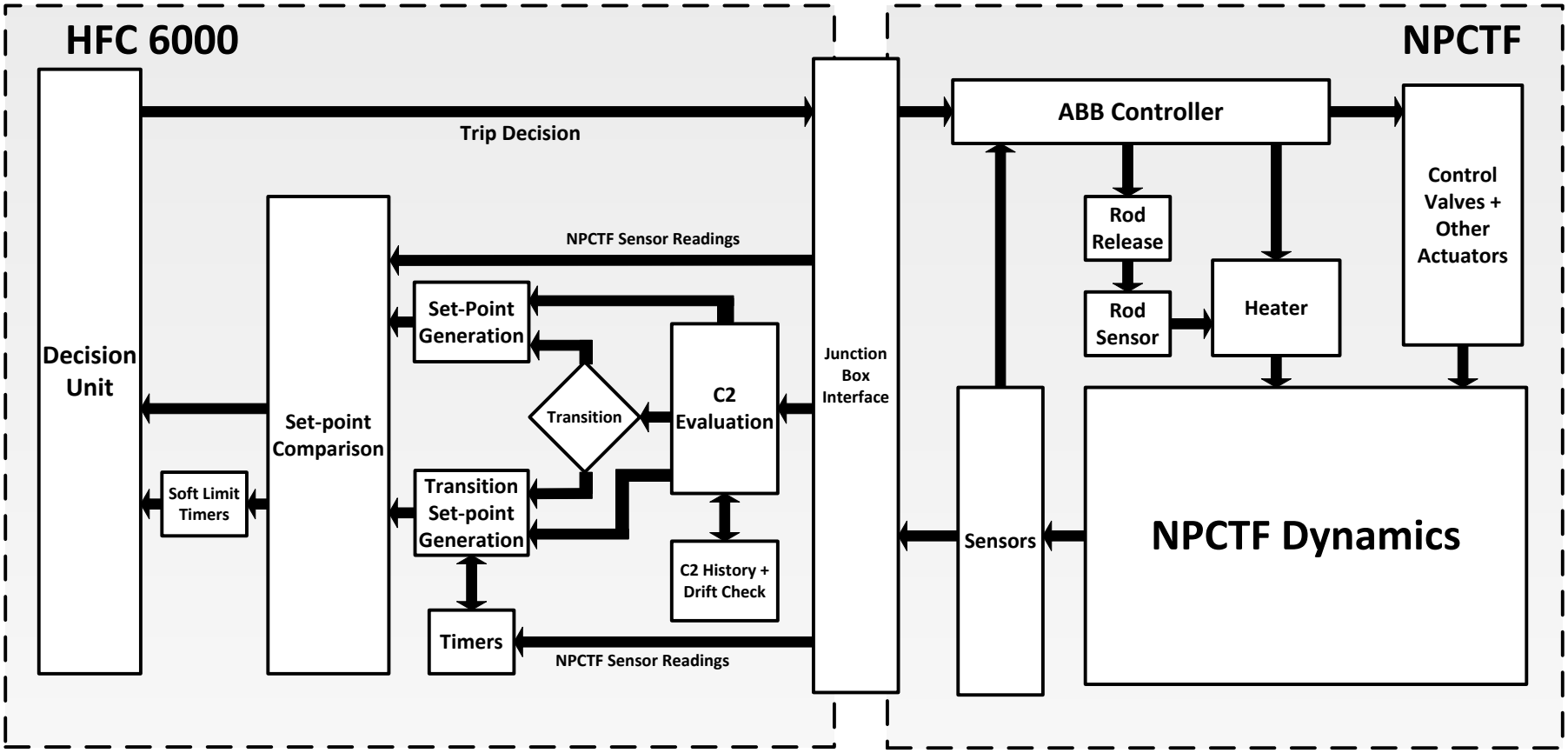

Figure 4.20: HFC and NPCTF Hardware/Software Logical Diagram

4.5 MATLAB Simulation of Developed Software on NPCTF Operations

A simulation on Matlab was performed to ensure overall functionality. This was performed using the operations history of the NPCTF then building a mock replication of the safety logic to upon it. This permitted incremental improvements, calibration, and analysis of theoretical internal states.

Safeguards were taken to ensure conversion between HFC and Matlab was seamless as possible. Variable names and permissible values were identical between the two sets of code. An ‘update’ script was used increment time while ensuring counters, timers, and other blocks kept within the maximum ranges available. Flagging was implemented, then identical logical statements of the HFC ladder logic were created.

Importantly, unlike HFC ladder logic, Matlab does not permit coding jumps. Jumping was instead imitated through careful looping (which HFC does not permit) and additional flagging to enable or disable segments of code.

Simulations were an extension of the initial sorting algorithms used to investigate the NPCTF characteristics and design the safety logic. The faux coding made obvious certain soft boundaries or conditions that were either too stringent or lenient. It further revealed errors in jumping logic that would have been otherwise missed.

One product of the simulations is the penalties used in determining settling. As stated in section 4.3, there is a penalty utilized when transitive parameters strays from their final boundaries. This necessity was discovered through Matlab simulation, as premature settled flags resulted in spurious tripping. The penalty was chosen as the optimal solution as longer

settling periods or resetting timers resulted in inappropriately long transition periods. These prolonged transitions caused spikes from new set point changes to go unnoticed, subsequently causing spurious tripping.

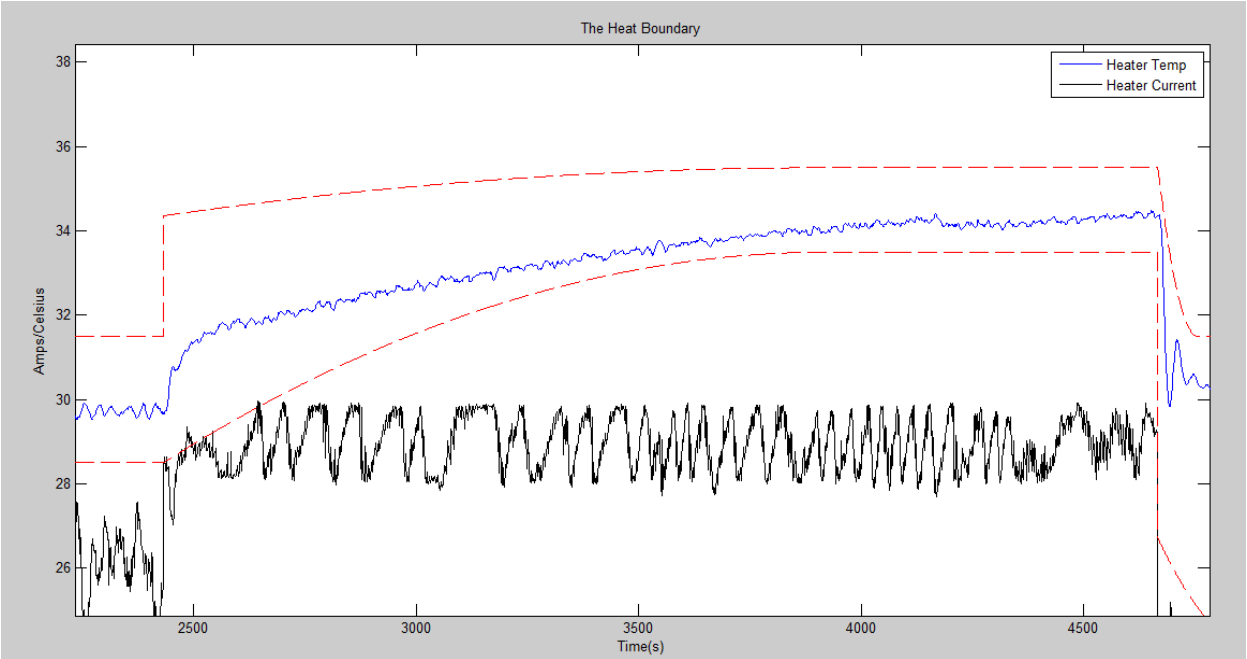

Figure 4.21. Theoretical Boundary Evaluation during Transition

In Figure 4.21, the heater temperature is shown in its transition in blue, the heater current in black, and the algorithmically calculated boundaries in striped red. The simulation software made visible the values of the theoretical boundaries at any given moment. The figure demonstrates the progression transitions: the current spike is detected, boundaries frame their respective parameter, and the transition is cleared after settling.

In Figure 4.22 the simulated status of flags during a transition is shown. This allowed the theoretical state logic of the coding to be observed and debugged. This capability exposed flaws in logic statements as discussed earlier. As an example of the safety algorithm's process and interpreting of transitions, an example is giving in Figure 4.22.

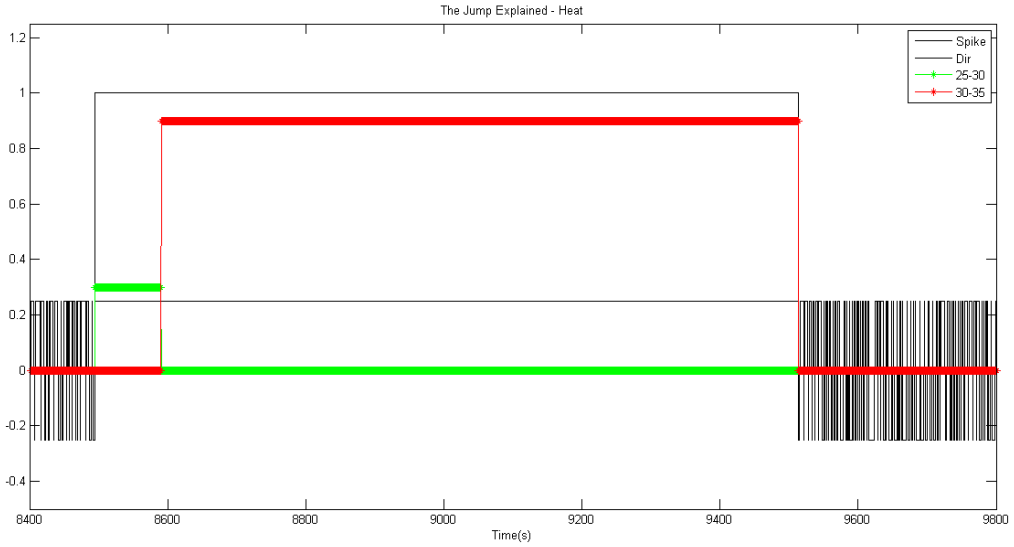

Figure 4.22: Level Transition Flags Simulation.

In the example, the transition flag, direction flag, and 25°C -30°C transition flag all go 'high' in the same clock cycle (tall black, short black, and green respectively), at approximately 8500 seconds.. It can be seem through the high status of the direction flag that the algorithm recognizes the jump as positive. The algorithm makes the default assumption that the upwards transition from a 25°C indicates a 25°C -30°C transition. This is an incorrect assumption, though is satisfactory for the first stage of the transition.

At approximately 8600 seconds, the current to the heater has settled to its new operating range. The algorithm therefore forces the 25°C -30°C transition flag to go low, and simultaneously raises the 25°C -35°C flag as a correction. This transition continues in the correct state until approximately 9500 seconds.

At this point, nearly 17 minutes after the beginning of the transition, the transition flags are cleared by the algorithm. The transition has ended and the algorithm has returned to monitoring the direction and operating point of the current in its typical method. The Matlab

simulation, through examples such as this, provide insight into the operations and logic of the system much more quickly and thoroughly than would be possible otherwise.

The factor term discussed in section 4.3.5 heat transition was created due to simulation. As demonstrated in Figure 4.23, the initial drop by the heater temperature during the operating point change necessitates the factor term. It may be readily observed the heater temperature would surpass the lower boundary early in its transition without the factor term. The term was calibrated by observing the minimum fraction successful in all investigated scenarios. The final value was chosen as 3.5, rounded out from approximately 3.2.

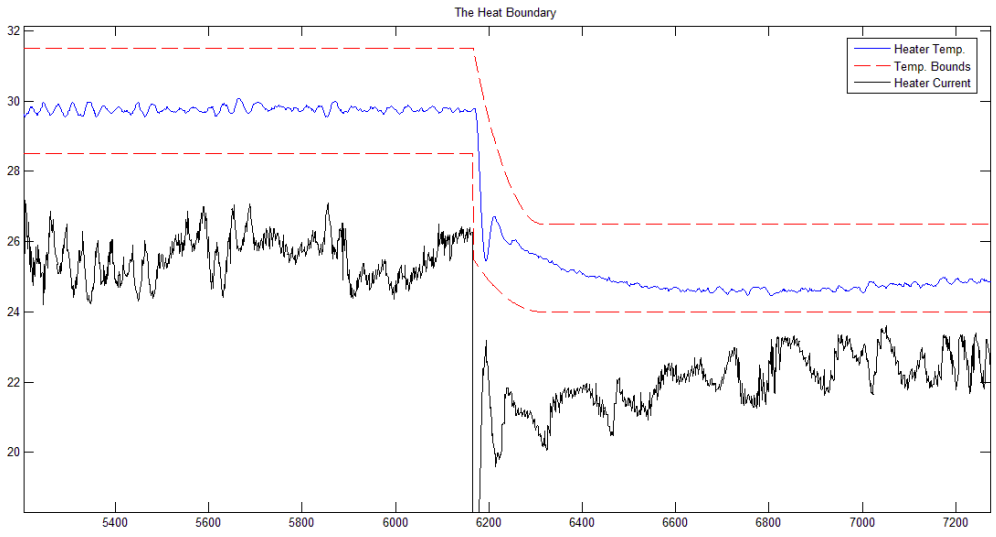

Figure 4.23: Sudden Drop in Heater Temperature.

As will be discussed in sections 5.4 and 5.5, the set points and timers of simulation were used to demonstrate the HFC's logic during live trials. Tripping parameters and state processes discussed in chapter 5 were determined through the Matlab simulation.

4.6 Theoretical Shutdown Time

A system shutdown as initiated by the RPS will follow through a number of discrete steps. The total time for this produces a maximum theoretical time between breach of trip set-points and a full system shut off. These steps, along with their maximum required time are as follows:

1. Parameter breaches set-point: Each safety parameter is read by industry grade analog sensors as discussed previously in this chapter. This breach is t=0ms and it is assumed, for this purpose, that the sensor produces an instaneous response
2. The HFC reads the new signal: The HFC analog inputs have been programmed to read all analog inputs every 100ms. In the worst case scenario, the breach takes place immediately after one reading, requiring a full 100ms until it is detected.
3. Processing and output: The SBC06 response time is listed at 50-100ms [90]. The worst case scenario, given that the output of the shutdown signal would occur on the same cycle as detection, is thus 100ms.
4. The NPCTF controller detects the shutdown signal: Once received, the shutdown signal must be recognized in the interface by the NPCTF's ABB controller. The controller has a 2ms refresh rate, and this is taken as the maximum time required [73].
5. Rod drop: The rod gripper is deenergized and the shutdown rod falls towards the shutdown sensor. This distance is 40cm. Thus, it is assumed the descent requires approximately. At 40cm, this time is approximately 285ms.
6. Detection of dropped rod: This is again handled by the ABB controller. With the same 2ms refresh rate, it is then assumed the heater can be shutdown instaneously from this point.

The total time is then 489ms with HFC response time taking at maximum 200ms. This is beyond the resolution of the NPCTF's capability to record, which is 1s. It is then taken that the total time of shutdown, including rod drop and heater shutdown, will be within one recording cycle of the NPCTF.

4.7 Chapter Summary

This chapter focuses on the design and implementation of the RPS. The HFC is presented as the choice of PLC unit with details of use its design and relevant applications expanded upon. Following, thresholds for the heater independent parameters are given after expansion of their breaching characteristics. The primary flow rate is chosen to have a lower boundary at 5.75 l/min with a 3s timer; the primary line pressure has a 7.25PSI(g) lower boundary and a 10.5PSI(g) upper boundary with 3s and 2s timers respectively; the HX tank pressure is given 3.2PSI(g) and 5.65PSI(g) lower and upper boundaries; and pressurizer tank level is given a 49.5% and 51.5% lower and upper boundaries, each with 3s timers.

Next, the implemented monitoring algorithm as implemented on the HFC is presented logically. The algorithm is a single loop after start-up, with 6 major subprocess including the initialization/start-up. These major subprocesses are: start-up, boundary procedure, heater current tracking, heat transition, level transition (up), and level transition (down). The various flags and pieces of information passed between these subprocesses control the creation of boundaries such that faults may be identified.

5 Verification and Validation

5.1 Summary of Tests Performed

V&V procedures necessitated several stages of testing. The V&V procedures further aid in discerning the source of errors: faulty code, equipment failures, incorrect implementation, or poor design. Revisiting the Figure 2.4 of Section 2.6, the following stages have been performed:

Requirements: A full RPS for the NPCTF is to be realized. This is to parallel a CANDU safety system. The requirements are discussed in chapter 1. Specific safety aspects of CANDU are discussed in section 2.3: Design Methods of RPSs.

Design: The safety system is designed using characteristics found during investigation. The investigation is discussed in chapter 3.

Implementation: Safety software has been developed for the HFC to operate on the NPCTF, creating the safety system. The software is the subject of chapter 4.

It now follows that the testing procedures must also occur. They are discussed in this chapter as follows.

Component Test: The sensory equipment of the NPCTF and communication with the HFC have been tested and verified. These tests are outlined in section 5.2.1.

Integration Test: Response testing has been performed on the HFC using controlled inputs. These tests verified software section by section. These tests are discussed in section 5.2.3.

System Test: The full system has been validated through standard operations and AECB design basis events. The design basis events, standard operations, and the system's response are discussed in sections 5.3 and 5.4, 5.5, and 5.6 respectively.

5.2 Verification Tests

V&V procedures necessitated several stages of testing. Not all of these stages will be discussed. However, emphasis is placed on the NPCTF equipment and communication verification and HFC response testing. These correspond respectively to component and integration tests in accordance with standardized V&V procedures.

5.2.1 NPCTF Equipment and Communication Verification

To verify the components, the 4-20mA outputs were observed by both the HFC and the NPCTF. This verified not only successful transmission, but also congruent measurement between the two systems. This verification performed primarily through the HFC memory editor application, part of the EWS (as discussed in section 4.1.3).

The HFC was configured only to recognize 4-20mA analog inputs as 0-100% of full scale input [91], this caused proper range of the sensors to be crucial when fabricating the safety algorithm. To test, two operating points were observed: one when the NPCTF was shut down and another during steady operations. For both observed points, the value was recorded from both the HFC's memory and the NPCTF's user interface. A linear progression was assumed and the full range was deduced.

Table 5.1: HFC to NPCTF Readings.

Signal	Short	NPCTF	HFC %	NPCTF	HFC %	Theory Max	Most Likely	Sensor Spec
Heater Current	C2	0.0 A	-0.050	22.6 A	45.10	50.08	50 A	50 A
Heater Temperature	T2	25.1^{0}C	50.09	29.1^{0}C	58.53	48.75	50^{0}C	50^{0}C
Primary Loop Pressure	P1	0.15 PSI(g)	0.65	10.05 PSI(g)	40.09	25.09	25 PSI(g)	25 PSI(g)
HX Tank Pressure	P2	-0.1 PSI(g)	-0.02	4.3 PSI(g)	17.60	24.88	25 PSI(g)	25 PSI(g)
Pressurizer Level	L3	4.2 %	3.59	50.8 %	50.83	99.3	100 %	100 %
HX Tank Level	L4	-1.8 %	-1.61	64.6 %	59.44	108.7	100 %	100 l/min
Primary Water Flow	F1	0.0 l/min	-0.33	5.9 l/min	62.49	9.42	10 l/min	10 l/min

From Table 5.1, it can be seen that the theoretical maxes stayed close to the sensor specifications. Deviations were likely from slightly mistimed measurements and noise. Note that the HFC's memory is recorded in hexadecimal, scaling from 1999 (4mA) to 7FFF (20mA) [91]. In Table 5.1, the HFC '%' reading is shown after conversion.

The opposite direction of communication was verified as well. The memory editor was used to set the digital outputs to 'closed', which could then be used to trip the NPCTF. This proved the NPCTF could be tripped through an HFC signal.

5.2.2 HFC6000 Response Testing

The safety software on the HFC was incrementally tested after implementation. First, AI and AO cards were tested for their interactions. Including the 1999_{16} bias previously mentioned, the HFC was allowed to read 4, 12, and 20mA signals from its own AO card into its AI card. This was confirmed through cross checking the memory editor, the equation editor, and the CQ4 editor.

Testing of each subsection of the code is then performed. The subsections are first written to the HFC one by one. Using the AO cards as inputs, the program is inspected using the display LEDs. This verifies trip point are located where designed. Following, the entire code is tested as a whole. The AO card is again used to isolate code segments of coding and inspect boundaries. This coding is slightly altered so that the tripping subroutine can be escaped.

5.3 AECB Standard Scenarios

The AECB was the precursor of the CNSC, existing until reorganization in 2000 under the Nuclear Safety and Control Act [20]. The AECB functioned similarly to the CNSC but was focused solely on nuclear power reactors.

The AECB released and upheld a number of regulatory documents, evaluated NPPs, and gave operating licenses at their discretion [95]. In February of 1991, the AECB released a body of regulations as an update to the previous iterations. Amongst these was the R-8: Requirements for Shutdown Systems for CANDU Nuclear Power Plants [22].

This document outlined many mandatory safety requirements, including two diverse and independent safety systems. It also specifies, in two tables, design basis events which the safety systems must be capable of detecting and controlling. The first of these tables is replicated in Table 5.1 [22]. Demonstration of capability of these design basis event was therefore a licensing requirement.

Table 5.2: Replica of Table 1 of AECB R-8.

Item	Failure
1.	Failure of reactor control systems
2.	Failure of normal electric power
3.	Seizure of a primary heat transport system main pump
4.	Failure of any feeder pipe in the primary heat transport system
5.	Failure of an end fitting
6.	Failure of a pressure tube and its associated calandria tube
7.	Blockage of a fuel channel
8.	Failure of a fuelling machine to replace a closure plug
9.	Inadvertent opening of pressure relief or control valves on the primary heat transport system or associated systems
10.	Failure of steam generator tubes
11.	Failure of feed water/steam systems
12.	Failure of moderator system
13.	Failure of service water system
14.	Failure of any other equipment in reactor systems which, in the absence of shutdown action, could result in damage to fuel in the reactor

The second table lists only "*Failure of any pipe or header in any fuel cooling system"*. Other safety system requirements include careful documentation procedures following a planned or unplanned shutdown, ability to prove that shutdown will not compromise integrity of the fuel rod sheaths, damage equipment, or release radiation [22].

The standard CANDU design basis events as shown in Table 5.2, are to be used as for the system's test. As the final stage of V&V, this tests the safety system against its initial requirement: To be a fully realized CANDU parallel system for the NPCTF. Unfortunately, not all the scenarios are possible to simulate on the NPCTF. The NPCTF lacks a nuclear reactor and thus does not utilize fuel channels or end fittings (items 5, 7, and 8). Similarly, the heat exchanger functions differently than a steam generator. It thus does not have tubes to rupture (item 10). However, the remaining failures have been designed into the NPCTF as fault insertion scenarios [2].

The AECB document does not specify a rate of response. The only explicit requirements are preventing damage to fuel sheaths and release of radiation [22]. Performance

requirements of the systems may be set by the licensee but must be explicitly stated, documented, and then upheld with justified design reason. These quantified performance requirements may later be compared against when determining the ongoing health of the RPSs.

5.4 Systems Testing and Simulated Faults

As previously discussed, the NPCTF is designed to safely simulate faults and does so in a number of methods. The NPCTF may override an external controller to alter the states of control valves. This allows it insert faults or simulate other unusual conditions. For example, the set point of a valve may be altered to simulate the 'jamming'. This 'jam' persists even when the external controller commands a set point change, effectively simulating a mechanical fault.

The NPCTF also possesses components for physically altering the system during live operations [2]. The critical primary line LOCA is simulated in this way: a valve has been built immediately preceding the heater which may be opened manually, 'spilling' coolant into the lower collection tank.

Additionally, the NPCTF can also introduce sensor biases to the external controllers [2]. This is done to simulate the failure of one or more sensors in the NPP. This scenario is highly plausible fault for control systems. This should likewise be readily noticed by safety systems for the danger it presents.

Faults may be dangerous for different reasons. The large LOCA on the coolant intake pipe of the reactor is the most critical fault that requires the quickest response [6]. However, the LOCA is easily detected as sudden spikes in heat, loss of pressure, and an uncontrollably changing neutron economy are recognizable indicators. Faults such as the partial loss of the

heat sink through a feed water pump failure are dangerous due to their effects manifesting slowly [97]. Faults like this require comprehensive understanding of system parameters. Their detection tests the accuracy of the safety system's implemented logic.

The safety system must also be tested for its security. Though CANDU safety systems must always err to safety, spurious trips are costly [42]. This risk is partially mitigated through the 2oo3 voting logic, but false positives represent poorly designed safety system logic. To test this, every operating procedures that is safe within the NPCTF has been performed in live trial to ensure that the safety system is not inappropriately cautious.

5.4.1 Normal Operations

'Normal Operations' experimentation tests the system's capability to accurately recognize safe operations. Normal has here been defined as scenarios in which an error has not occurred and no fault has been inserted. A safety algorithm is therefore expected to produce no spurious trips during these experiments.

These tests assess the design logic which predicts the appropriate operating range for all critical system parameters. It does this in real time, without operator guidance or control of the NPCTF. The algorithm will monitor the system parameters, track their changes, and make proper assumptions during the transitions.

Normal operations will be any of the nine states of operation. For reference, the nine states of operation are in Table 5.2. It must be reminded that the investigation of NPCTF conditions used three operating points. Operations will thus be limited to these.

Table 5.3: States of Operation.

State	Type
25^0C, 30^0C, 35^0C	Operating Point
25^0C->30^0C, 30^0C->35^0C, 35^0C->30^0C,30^0C->25^0C, 25^0C->35^0C, 35^0C->25^0C	Transition

Each of these nine states in Table 5.2 are tested by cycling between the three operating points in approximately forty minute increments. The forty minute windows allow the heater to settle into its new operating point before the next transition as the longest settling time (the rise from 25^0C to 35^0C) is 30 minutes. An additional ten minutes has been added so that all system parameters have totally ceased their transients. The total step-length is therefore 40 minutes, which every transition has been permitted for consistency.

5.4.2 Fault Insertion Methodology

As explained in Section 5.2: AECB Standard Scenarios, there are 15 standard CANDU design basis events [22]. The safety system must therefore be able of detecting and signalling a trip for each of these faults. This is the most critical testing procedure as it determines whether the safety system could halt potential catastrophes. Though a spurious trip is costly to the NPP operations, a missed fault is a potentially global event [98].

While the NPCTF is capable of testing many faults, time constraints limit the total number of faults that can be reasonably inserted. Assessing the worst case scenarios is instead assumed to umbrella other faults [99]. As the NPCTF lacks a reactor, it cannot simulate some of the most dangerous faults: those that compromise the fuel channels. However, many of the AECB design basis events possesses NPCTF parallels. Using the 14 items of AECB Table 1 of the R-8, fidelity to the V&V procedure of an NPP safety system is retained. These events are listed in Table 5.2 with their equivalents on the NPCTF.

Table 5.4: NPCTF Equivalents to AECB Design Events.

Item	AECB Event	NPCTF Equivalent
1	Failure of Reactor Control System	C2 Drift
2	Failure of Normal Electrical Power	(Matter for ECCS System)
3	Seizure of Primary Heat Transport System Pump	Pump1 Failure
4	Failure of Any Feeder Pipe in Primary Loop	SV-1 Force Open
5	Failure of an End Fitting	LOCA
6	Failure of a Pressure Tube Associated With Calandria	Void (No Reactor)
7	Blockage of Fuel Channel	Void (No Reactor)
8	Failure of A Fuelling Machine to Replace a Closure Plug	Void (No Reactor)
9	Inadvertent Opening of a Pressure Relief or Control Valves On Primary Loop	CV-20 Force Open
10	Failure of Steam Generator Tubes	Void (Steam Generator and Primary Not Connected)
11	Failure of Feed water/Steam System	CV-18 Force Open
12	Failure of Moderator System	Void (No Reactor)
13	Failure of Service Water System	Pump3 Failure
14	Failure of Any Other Equipment Which, in The Absence of Shutdown Action Could Result in Damage to Fuel In The Reactor	Open to many other faults

Some notes must be stated for items in Table 5.3 that do not possess NPCTF equivalents on the NPCTF. For event item 2, the failure of a normal electrical system implies that safety must be created through back-up generating supplies. This test is primarily meant to ensure that loss of power can still be handled through passive cooling, back-up generators, and other designed safeguards to manage residual heat. Though the NPCTF does possess an emergency core cooling system [2], this test has no bearing on the performance of the safety algorithm.

Event item 10, the failure of the steam generator tubes, is not able to be simulated with NPCTF. However, another fault meant to disrupt the operation of the heat exchanger has been included. This is the opening of CV-18, as parallel to item 11, failure of feed water/steam system.

Finally, event item 14 is unspecific but left to the discretions of the engineers designing the NPP. Additional faults have thus been added to the list in this item slot. These faults are

amongst NPCTF designed faults and expand the variety of scenarios tested. Adding two faults the NPCTF is capable of simulating for this item brings the total number of faults to nine; as many faults as there are stages of operation.

Time restraints prevent every fault from being tested in every stage. The experiment process requires a full start-up, stabilization, insertion of the fault, detection, shutdown, and cooling (using the ECCS). The start-up and shutdown processes in the NPCTF (as with NPP) are very time consuming. For this reason, each fault is inserted into three different stages, and each stage is tested under three different faults. The faults are listed in Table 5.4 and the organization of fault insertion is outlined in Table 5.5.

Table 5.5: Faults Inserted as Part of System Validation.

Fault	AECB Item	Event
A	1	C2 Failure
B	3	Pump1 Failure
C	4	CV-3 Force Open
D	5	LOCA
E	9	CV-20 Force Open
F	11	CV-18 Force Open
G	13	Pump3 Failure
H	14	CV-1 & CV-2 Force Close
I	14	CV-9 Open/CV-10 Force Close

This distribution of faults maximizes the variety of scenarios each fault is inserted into. Each stage receives a unique configuration of three faults, while each fault is ideally placed into settled operation, an upwards transition, and a downwards transition. When possible, the upwards and downwards operating point stages include one large jump (25^0C to 35^0C or vice versa) and one small jump. However, of the six transitional stages, four are small and two are large. The coordination of fault insertion therefore attempts to maximize diversity to the extent possible.

Table 5.6*:* Organization of Fault Insertion.

Operating Stage	Fault 1	Fault 2	Fault 3
25^0C	A	B	C
30^0C	D	E	F
35^0C	G	H	I
$25^0C \rightarrow 30^0C$	A	E	G
$30^0C \rightarrow 35^0C$	B	F	H
$25^0C \rightarrow 35^0C$	B	C	D
$35^0C \rightarrow 30^0C$	C	G	I
$30^0C \rightarrow 25^0C$	D	H	I
$35^0C \rightarrow 25^0C$	A	E	F

For the testing involved, multiple fault scenarios are not considered. It cannot be assumed that being able to detect both faults individually would cover the faults concurrently, though the CNSC R-8 documents have not specified the requirement for dual-fault scenarios. As such, it is then assumed that single fault scenarios are sufficient for full-system testing.

It is additionally assumed that the R-8 design basis events cover the 'worst-case' scenarios for the NPP. Other faults are therefore assumed to fall under the umbrella of these scenarios, such that protection against these most significant faults is sufficient evidence for protection against lesser occurences.

5.4.3 The Faults

Fault A: C2 Failure

Fault A simulates a failure of the reactor control system. This is any scenario in which the controlling mechanisms of the reactor have failed to properly curtail a super criticality. These faults are characterized by rapid growth of neutron economy. Neutronic propagation's exponential characteristic causes super criticalities to become more dangerous each moment it persists.

There several reasons why a reactor may begin to suddenly produce excess energy [100]. Amongst the most common is the build-up of reactor toxins. Though toxins decrease energy output, they are 'burnt off' slowly as they collect neutrons and are eventually made radioactive [101]. Burn off may then conversely increase neutron activity. This should be actively detected handled by reactor control system.

C2 denotes the current to the heating unit. This can be overridden with a value, or a bias may be placed. In order to simulate a sudden and uncompensated neutron spike, the NPCTF will manually alter the current for a brief period. After, the controller will be readmitted to the heater. This spike will simulate a failure in the control or measurement of neutron economy, both requiring active intervention.

Fault B: Pump1 Failure

Fault B, the failure of Pump1, simulates the seizure of the primary heat transport pump. This fault played a major role in the Chernobyl cataclysm [102] and contributed to the eventual meltdown at Fukushima Daiichi [103]. The primary pump keeps coolant running through the reactor and without its continued operation the reactor becomes unable to shed heat. The major danger of item 2 of Table 5.3 (loss of power) is also loss of the primary pump.

The NPCTF presents a number of modes that test system response to pump1 failure. These range from decreases in performance to outright shutdowns. Using a conservative approach, the primary pump will undergo a complete failure for this fault insertion. This can be user performed from the control panel.

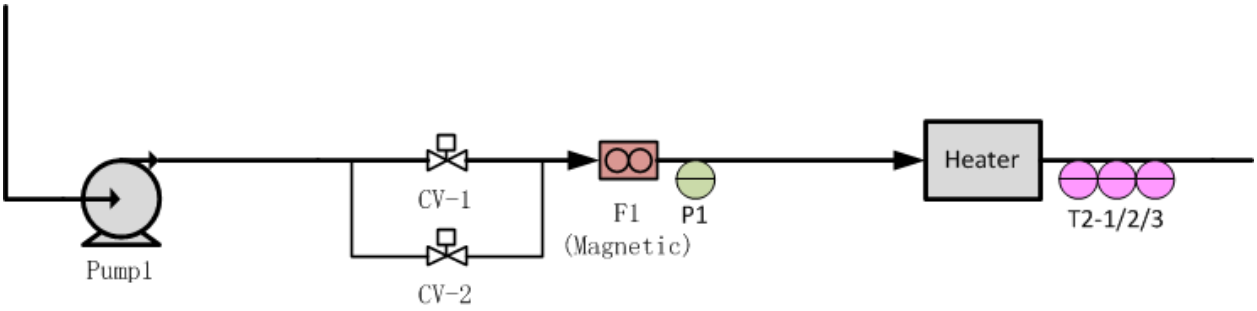

Figure 5.1: Schematic for Pump1 Failure.

Figure 5.1 shows the schematic of a pump 1 failure. Pump1 powers the primary flow which is controlled by CV-1 and CV-2. F1, and P1 measure primary loop flow and pressure respectively, while T2_1/2/3 measure heater outlet temperature. Pump1 is fed from the heat exchanger (simulating the steam generator) and pumps water back through the heater.

Fault C: CV-3 Force Open

Fault C simulates the failure of a feeder pipe in the primary loop. CV-3 is brings water into the primary loop during start-up. This fault breaches the primary loop, resulting in several system backlashes. These include pressure drops, pressurizer failures, and maladjusted flow as coolant is drawn into the lower holding tank.

The NPCTF will likely attempt to compensate for this primary loop breach by invoking the pressurizer to increase pressure. When the pressure of the primary loop fails to increase, the pressurizer water levels and pressure will drop.

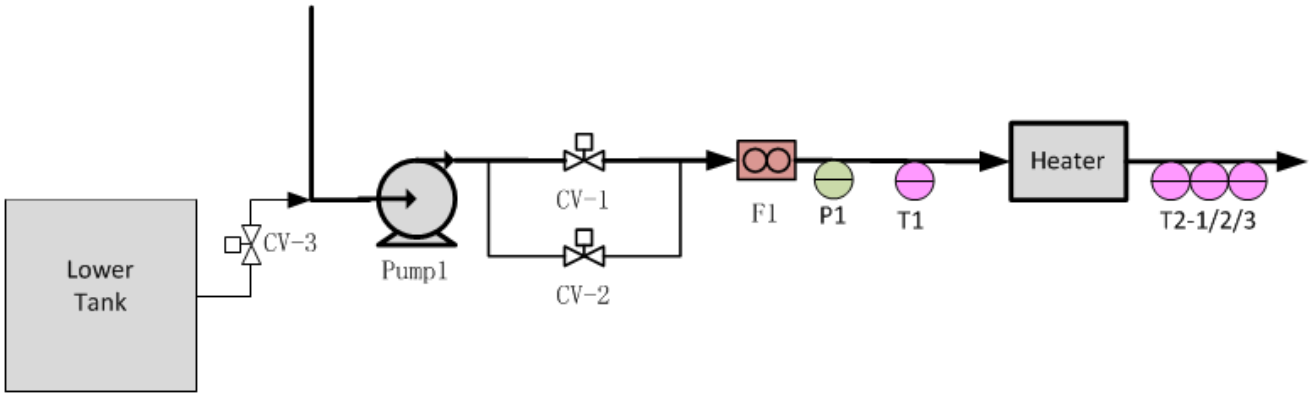

Figure 5.2: Schematic for Fault C: CV-3 Force Open.

Figure 5.2 shows the location of valve CV-3. CV-3 connects the lower tank to the primary loop to fill and empty the coolant during start-up procedures. Pump1 powers the coolant flow that is controlled CV-1 and CV-2 and measured by F1. P1, T1, and T2_1/2/3 measure primary loop pressure, and heater intake and outlet temperatures respectively.

Fault D: LOCA

Table 5.3's item 5: the failure of an end fitting is a LOCA. However, this has been reformatted in the testing to increase the accident severity. A large LOCA immediately entering the reactor represents the worst case scenario. This empties the reactor of coolant as the water backflows and spills. Once the reactor is void of coolant, the now dry fuel sheaths continue to be surrounded by moderator but lack heat dissipation. The large LOCA thus has the capability to overheat and meltdown the reactor within moments [96]. This scenario is so severe that the RPS's speed is evaluated against this event [96].

The LOCA is simulated on the NPCTF through the release of FV-1 valve. This is a manual valve that drains water into a lower holding tank, simulating the worst case scenario LOCA. This should result in a sudden increase in flow (as water drains from the primary line), a decline in pressure, and a pronounced and obvious spike of heater temperature.

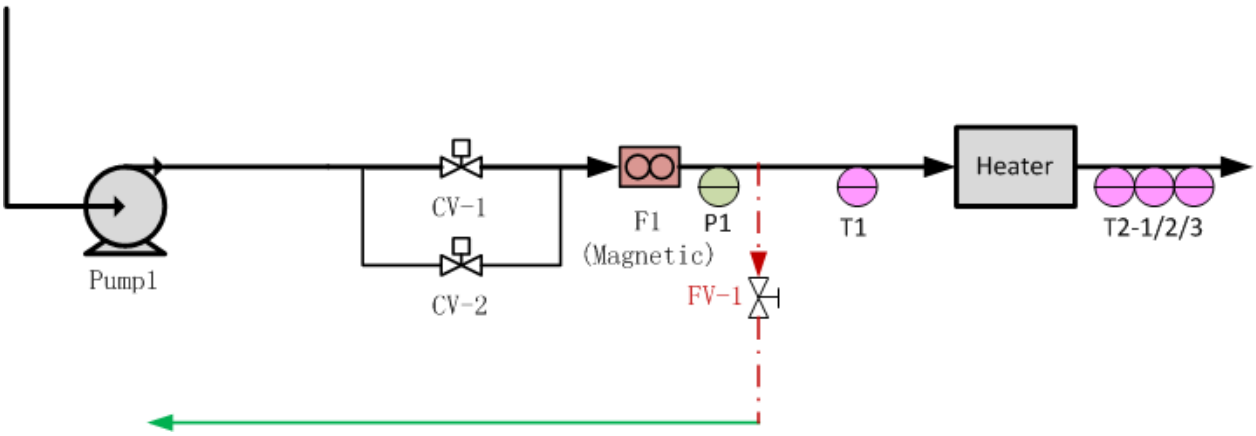

Figure 5.3: Schematic for Fault D: LOCA.

The flow valve FV-1 is located immediately before the heater in the primary line as shown in Figure 5.3. Pump1 powers the coolant flow which is controlled by CV-1 and CV-2 and measured by F1. FV-1 is a manual release valve that leads into a lower collection tank. P1, T1, and T2_1/2/3 measure primary loop pressure, and heater intake and outlet temperatures respectively. FV-1 is opened fully in each trial for both experimental consistency and as a 'worst case' scenario.

Fault E: CV-20 Force Open

Fault E simulates the 9th Item in Table 5.3: The inadvertent opening of a pressure relief or control valve on the primary loop. This has been simulated through CV-20. The inadvertent opening of the pressure relief valve should cause a sharp decline in pressure on the primary line. Like with the LOCA, this involves spillage of water, though its location dictates the sudden rise in temperature is delayed. The fault will likely cause the same pressure loss and subsequent overcompensation by the pressurizer of fault C.

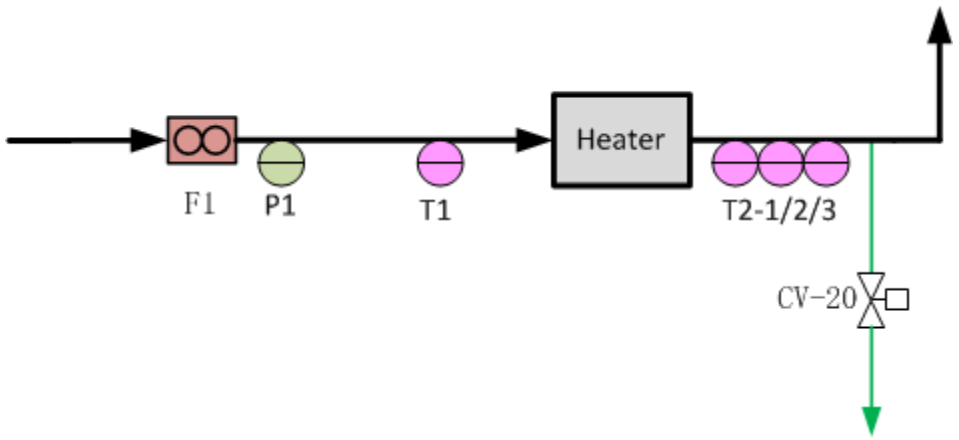

Figure 5.4: Schematic for Fault E: CV-20 Force Open.

The location of CV-20 is shown in Figure 5.4. CV-20 drains to the lower tank immediately proceeding the three heater outlet temperature sensors, T2_1, T2_2, and T2_3. Other major primary loop measurements are primary flow rate, primary temperature, and heater intake temperature F1, P1 and T1 respectively. Similar to the LOCA in that coolant is lost, this simulates the inadvertent opening of a pressure relief valve on the primary line. However, because this fault is controlled through the NPCTF's main control system, CV-20 can be opened consistently to the same degree. Therefore, CV-20 can be used to simulate a steady loss of fluid (i.e. a leak) rather than a rupture that drains the primary line quickly.

Fault F: CV-18 Force Open

A forced CV-18 opening simulates item 11 on the AECB list: Failure of the feed water/steam system. In this fault, water being transported out of the HX tank will drain faster than pump2 can replenish it CV-25. This fault thus presents an overheating danger in NPPs as it drains the steam generator and halts heat transportation.

CV-18 and CV-25 jointly control the level of the HX tank. This event may manifest slowly, especially during steady operations when HX tank level is steady. Both the pressure

and the level of the steam generator will be affected by the fault, allowing the safety system to detect its presence.

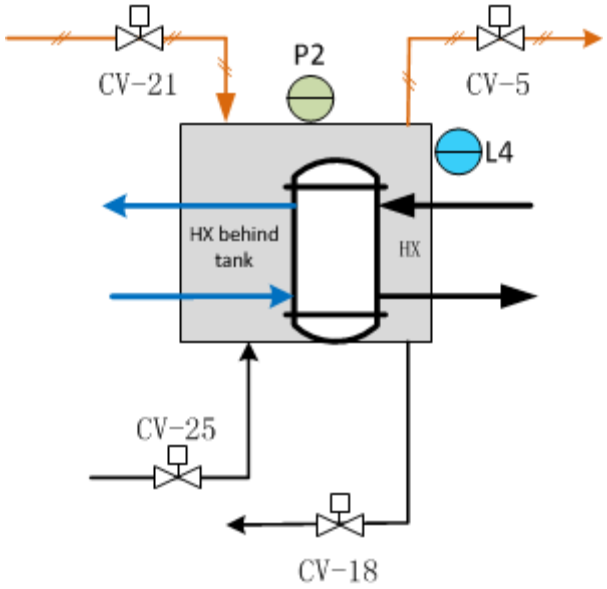

Figure 5.5: Schematic for Fault F: CV-18 Force Open.

The control of HX tank water level is illustrated in Figure 3.5. Inventory control of the HX tank is performed by air intake and outlet valves CV-21 and CV-5 respectively, along with water intake valve CV-25 and outlet valve CV-18. The HX tank's pressure and level are measured at P2 and L4 respectively.

Fault G: Pump3 Failure

Pump3 failure as fault G simulates item 13: the failure of the service water system. Pump3 controls the water flow of the chilling circuit. Initially, failure of the chilling circuit causes drastic decreases in turbine efficiency as condenser fails to generate appropriate energy gradients. As the secondary loop stagnates, the event becomes the dangerous loss of heat sink scenario. Steam generators overheat first as their feed water warms. In turn, coolant no longer sheds heat in the steam generator and returns to the reactor still hot, causing overheating.

The chiller pump (pump3) failing will likewise cause rising temperatures in the primary loop. Though secondary loop heat will rise more quickly, this is not a monitored parameter. The current to the heater will attempt to compensate against rising temperatures, thus this fault may be detected through heater current drift or heater temperature increase.

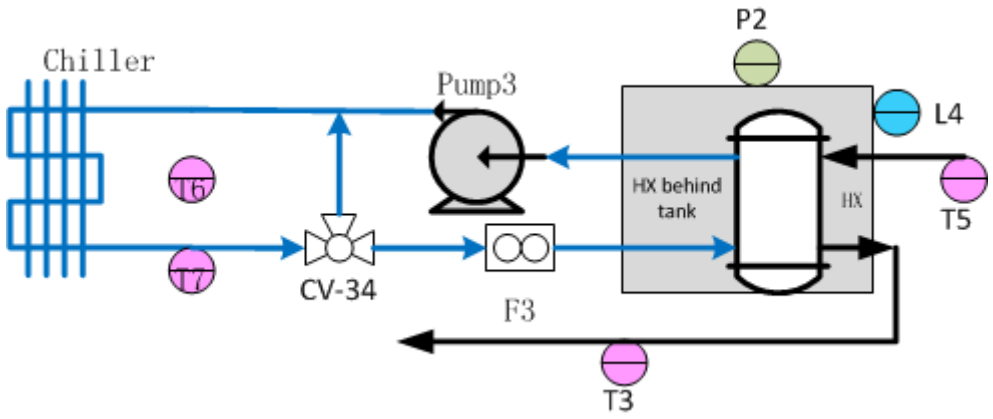

Figure 5.6: Schematic for Fault G: Pump3 Failure.

The schematic position of Pump3 is shown in Figure 5.6 as between the HX tank and leading to the chiller in the chiller loop. The chiller temperature is measured by T6 and T7 at intake and outlet respectively, while CV-34 controls flow on the secondary side, as measured at F3 and powered by pump3. The HX tank's sensors P2, L4, T5, and T3 measure pressure, level, intake and outlet temperature respectively.

Fault H: CV-1 & CV-2 Force Close

The NPCTF possesses two available modes to control the flow of water coolant through the primary loop. First, the current to pump1 can be altered to increase or decrease its power. Second, two control valves, CV-1 and CV-2, can vary their position to manipulate flow rate. The position of these two valves is shown in Figure 5.7. For the work of this thesis, the latter option was chosen.

CV-1 and CV-2 simultaneously being forced is fault H, within the open item 14 of the AECB list. This represents steady loss of flow, complementing the sudden failure of pump1 in fault B. The safety algorithm is thus expected to detect this fault through flow rate. However given the valve locations, pressure losses and rising temperatures will also occur.

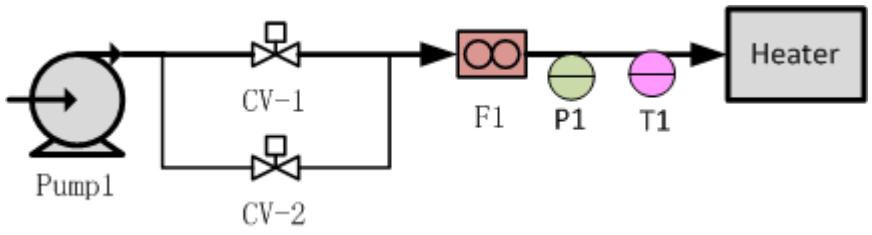

Figure 5.7: Schematic for Fault H: CV-1 and CV-2 Force Close.

As shown in Figure 5.7, pump1 is the primary pump, CV-1 and CV-2 control the flow in the primary, and F1, P1, and T1 measure the primary flow rate, primary pressure, and heater inlet temperature respectively.

Fault I: CV-9 Open/CV-10 Force Close

Fault I is also part of item 14 on the AECB list. The fault is the forced opening of CV-9 coupled with the closure of CV-10. These two valves control simulated steam flow in the pressurizer (pressurized air in the NPCTF), which in turn maintains the pressure in the primary loop. These can be seen in Figure 5.8.

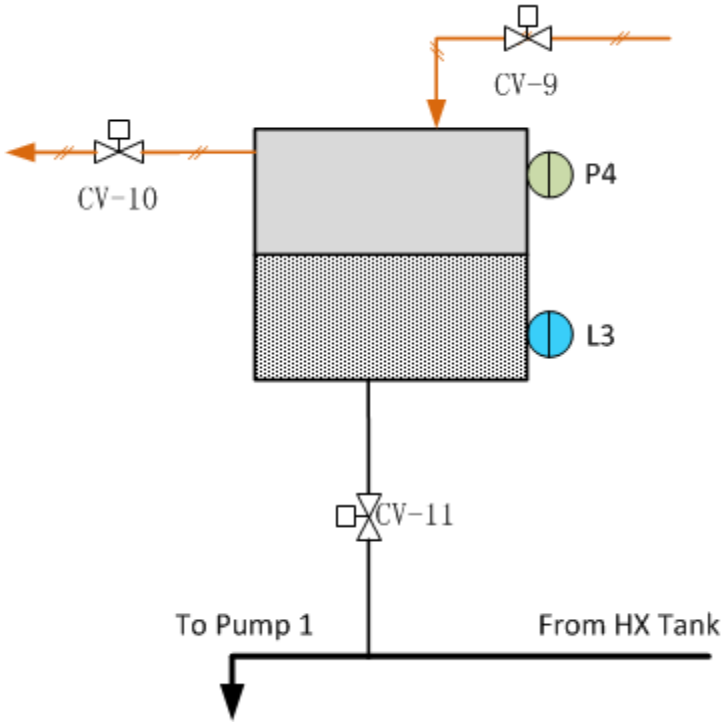

Figure 5.8: Schematic for Fault I: CV-9 Open/CV-10 Close.

CV-9 and CV-10 are the air intake and outlet valves respectively, where CV-11 is the liquid connection between the pressurizer and the primary line. P4 and L3 are the pressurizer pressure and level respectively

With this mismatch, air will be able to flow into the pressurizer but will be unable to flow out. This fault may be initially overlooked until the pressurizer is needed. However, pressurizer level responds to operating point changes and suppresses normal permutations during steady operations. The mismatch will likely cause pressurizer level to drift during operations, resulting in trip.

5.5 Experiment 1: Normal Operating Conditions

Normal operations testing determines whether the system is too conservative and will generate spurious trips. Though it is preferable to produce false positives over false negatives, a needlessly active system can cost a plant time, money, and cause system strain [42].

The test was performed through two five hour experiments. During the experiments, the system was cycled through its three operating stages such that every transition occurred once, creating six total transitions. Each transition was given 40 minutes to complete before the next transition was begun. Both experiments were identical except for minor operator timing differences.

The safety algorithm succeeded and produced no spurious trips. Between the two experiments, more than 10 hours of operations were carried forth, strongly verifying the security and discretion of the implemented system.

5.5.1 Heater-Independent Parameters

The four heater-independent parameters were be analyzed for operating ranges and breaching characteristics observed during experimentation. The recorded data has been interpreted using the Matlab simulations with results as follows.

Primary Line Pressure (P1)

The primary line pressure is bounded by 7.25 PSI(g) and 10.5 PSI(g). The overall current/pressure relationship is shown below in Figure 5.9.

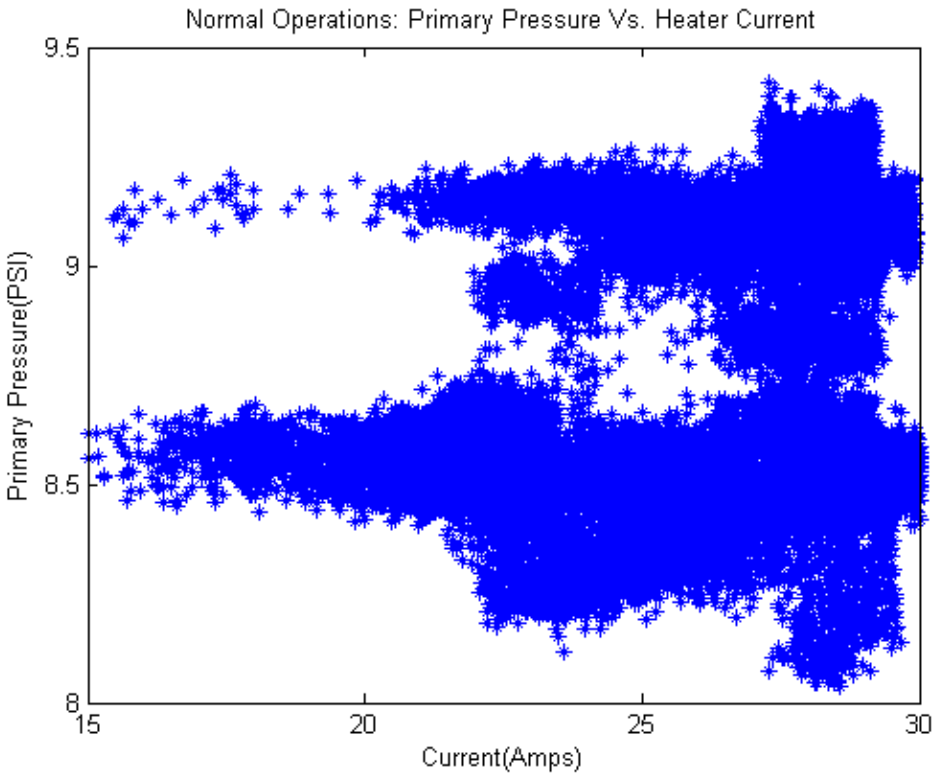

Figure 5.9: Primary Pressure vs. Heater Current.

Further, the primary pressure spent the entire experiment between 8PSI(g) and 9.5PSI(g); utilizing only 1.5 PSI(g) of the 3.25 PSI(g) envelope. There were no breaches of upper or lower boundaries observed during experiments. The time recording of both trials is displayed together in Figure 5.10. This demonstrates that while there are remained transients during operations, these remain well within the expected range.

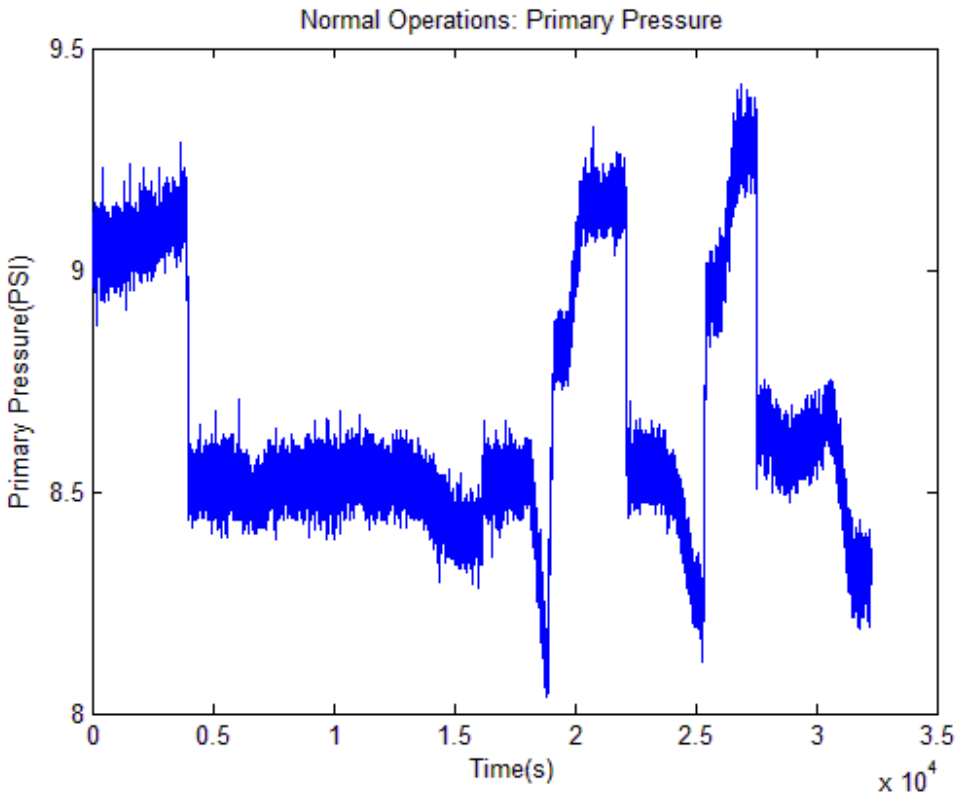

Figure 5.10: Timeline of Primary Pressure during Normal Conditions Experiments.

HX Tank Pressure (P2)

The HX tank has pressure limits of 5.65PSI(g) and 3.2PSI(g) for maximum and minimum pressure respectively. It is reminded that HX tank pressure, unlike the other heater-independent parameters, does not utilize soft boundaries. As such, no breaches occurred during the two trials. A statistical interpretation of the operating bounds for both trials is shown in Figure 5.11.

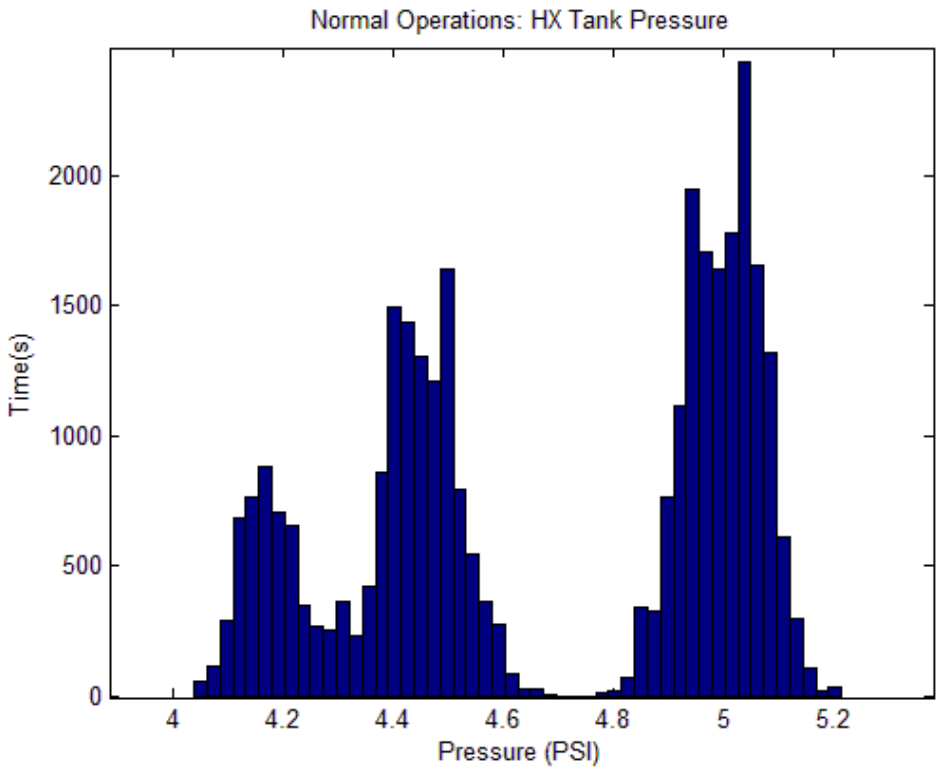

Figure 5.11: Operations of HX Tank Pressure.

The HX tank pressure remained between 4.78PSI(g) and 5.22PSI(g) for the first trial and between 4.68 and 4.03PSI(g) for the second. Both these dichotomous operating ranges were within the safe operating bounds. Even outliers stayed well within the appropriate bounds. This was expected as HX tank pressure tends to change very slightly, even during the presence of faults.

Pressurizer Level (L3)

The pressurizer level has bounds of 49.5% on the lower bounds and 51.5% for the upper bounds. The water level of the pressurizer remained uncharacteristically steady during the two trials. There occurred no breaches of the soft boundaries during both the first and the second round of experimentation. The pressurizer level did respond to operating point changes,

though the magnitude of these transients was less than typical. Display of the deviations into the lower operating ranges is shown in Figure 5.12.

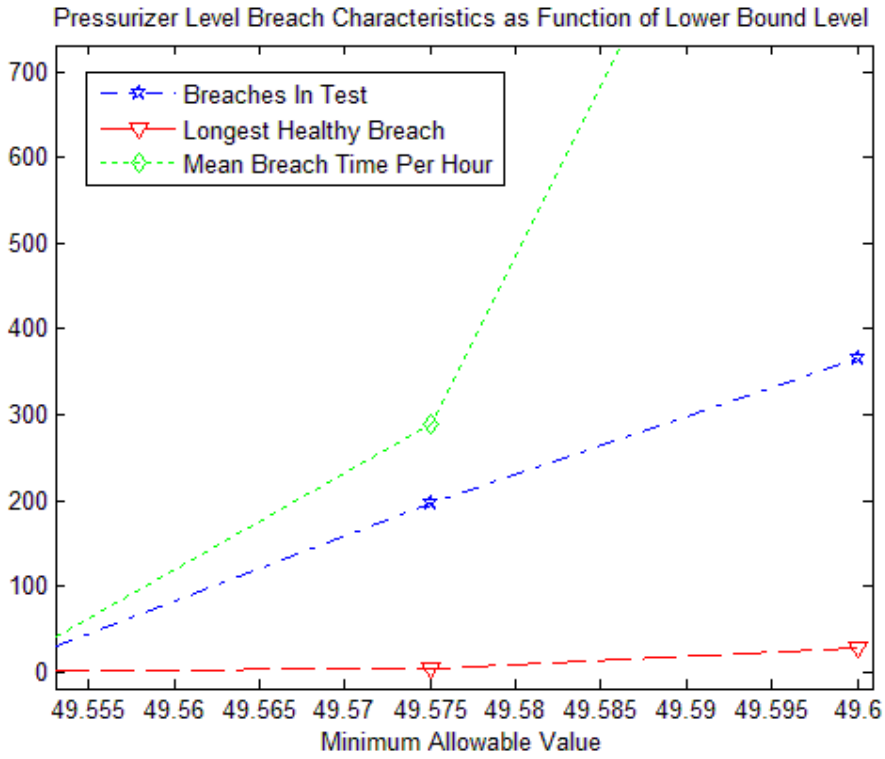

Figure 5.12: Breaching Characteristics for Lower Boundary of Pressurizer Level during Normal Operations Experiment.

Pressurizer level, during the 10 hours of operation, had a maximum value of 50.67% of the total level of the pressurizer tank, and a minimum level of 49.55% of the total tank level. The level approached very near the soft boundaries but did not breach them during the time observed.

Primary Flow Rate (F1)

The primary flow rate utilizes only a lower limit. This lower limit of 5.75 l/min saw 426 breaches between the two experiments, though the longest of which was between one and

two seconds based on the operations recording. The total operating characteristics are shown in Figure 5.13.

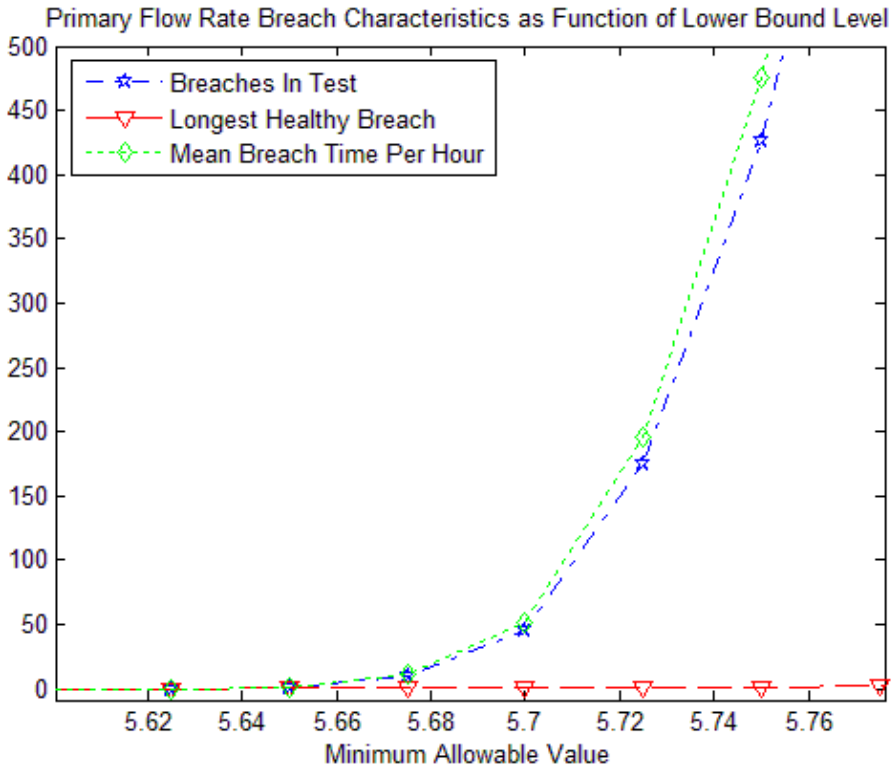

Figure 5.13: Breaching Characteristics Flow Rate Lower Boundary during Normal Conditions Experiments.

The breaching characteristics for primary flow rate again demonstrate the noisiness of the flow rate parameter. The 10 hours of operations saw an average of 35.5 breaches per hour, approximately one breach every 100s. However, the soft boundary principle permitted this feature. None of the 426 breaches persisted for three or more seconds to cause a spurious trip.

5.5.2 Heater-Dependent Parameters

The heater-dependent parameters required drastically different monitoring than the others. Because their operating limits move with the operating point of the system, the transitions greatly tested the safety system. Unlike the heater-independent parameters, these

parameters a given slightly wider operating bounds though no soft limits. This is especially important for heater temperature as reactor overheating is the primary danger of an NPP. Breach of temperature bounds on the NPCTF are therefore always faults, even when no abnormalities exist.

Heater Temperature (T2)

The safety system was able to properly calculate heater temperature bounds during the experimentation. The heat made its transitions within the windows and times permitted. The safety system demonstrated its capability to anticipate coming temperature changes through the use of current spikes. This resulted in no spurious tripping. The heater temperature and its theoretical boundary for the first trial is shown in Figure 5.14.

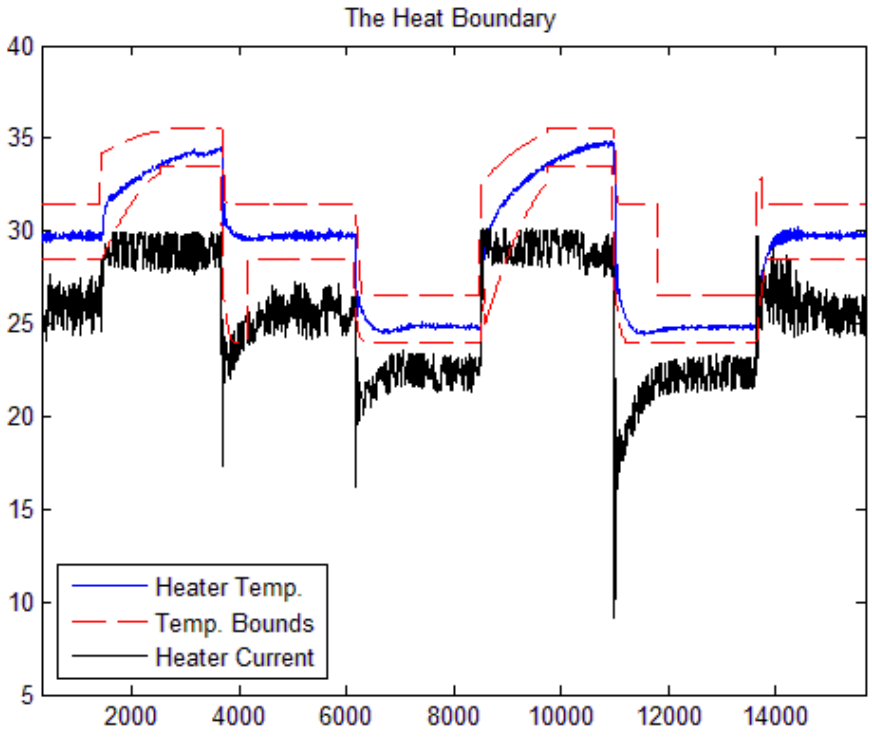

Figure 5.14*:* The Heat Boundary vs. Heater Temperature for First Normal Operations Experiment.

As shown in Figure 5.14, the boundaries (striped in red) are able to use the current in the heater (black) to accurately anticipate oncoming changes in operating conditions of the heater temperature (blue). This demonstrates the calculated transition logic used in the safety system. These transitions were performed correctly and the flagging logic's capability was demonstrated for each operating point change. The times for transition are shown in Table 5.6. The differences between the two trials show clearly the wide variance of transition times that must be accommodated by the safety system.

Table 5.7*:* Transition Times and Maximum Permitted for Temperature in Heater During Normal Operations Conditions.

Transition	Time – 1st Experiment	Time – 2nd Experiment	Maximum Allowed
25^0C -> 30^0C	175s	47s	240s
30^0C -> 35^0C	1130s	141s	1500s
25^0C -> 35^0C	1240s	330s	1800s
35^0C -> 30^0C	16s	19s	90s
30^0C -> 25^0C	55s	24s	150s
35^0C -> 25^0C	109s	164s	240s

These times have been calculated using the flagging of the theoretical flags of the safety logic as simulated on Matlab, as no operating history can be drawn directly the HFC. These characteristics again demonstrate two considerations from the design of the heater transition coding. First, steps that decrease heater temperature are significantly quicker. Second, moving from the center operating temperature (30°C) outwards is more timing consuming than the reverse. Regardless, the maximum time limits for transition were not violated in any scenario. The nearest was from 25^0C to 30^0C on the first trial, which at 175s still required 65s less than maximally permissible.

HX Tank Level (L4)

Like with heater temperature, the HX tank level bounds were continually re-evaluated during operations. Testing of the HX tank level required both subsections of code dedicated to its transition to be properly functioning. The safety system succeeded in calculating the safe operating bounds during the live trials. The IRC, overshoot, and transitions were all correctly included and the algorithm produced no false positives. The HX tank level and simulated boundaries during the first trial's operations are shown in Figure 5.15.

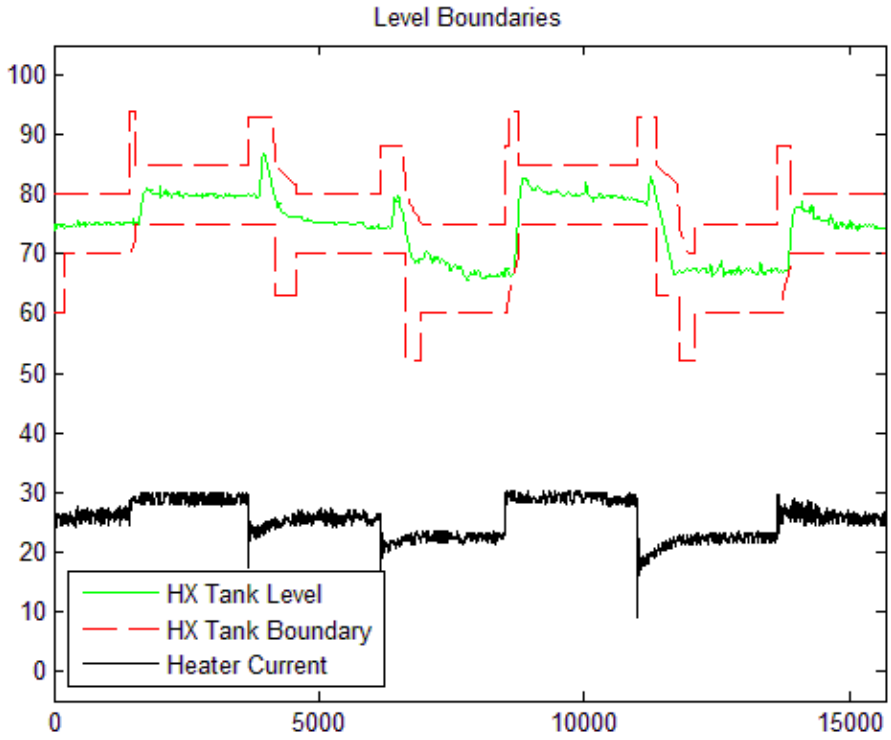

Figure 5.15: Level Boundary vs. HX Tank Level for First Normal Operating Conditions Experiment.

In Figure 5.15, the HX tank level (green) stays between the bounds created by the algorithm (dotted red) using input from the heater current (black). The IRC at the beginning

of downwards steps is clearly seen in Figure 5.15. The flagging used by the safety algorithm was able to correctly identify the stages of the transition and steps being taken.

5.6 Experiment 2: Fault Insertion

Capability to detect and respond quickly to dangerous conditions is the most important aspect of a safety system. In order to test the implemented safety algorithm, the AECB scenarios as outlined in section 5.2 were implemented as referenced in section 5.3. All but two experiments provided successful results. 25 of 27 experiments ended with a trip as initiated by the safety system, while two experiments provided a null response as the NPCTF's own safety system shut down operations first. The full summary of the trips are listed in Table 5.7.

Table 5.8*:* Trigger Parameter of Each Experimental Trip.

Operating Stage	Fault 1	Trip	Fault 2	Trip	Fault 3	Trip
25°C	A	--	B	L3	C	P1
30°C	D	L3	E	L3	F	L4
35°C	G	T2	H	F1	I	L3
25°C → 30°C	A	--	E	L3	G	T2
30°C → 35°C	B	F1	F	L4	H	F1
25°C → 35°C	B	F1	C	L3	D	T2
35°C → 30°C	C	T2	G	T2	I	F1
30°C → 25°C	D	L3	H	F1	I	P1
35°C → 25°C	A	T2	E	P1	F	L4

**'--' indicates an invalid trial*

This strongly implicates success in the validation of the safety algorithm as implemented on the HFC. Reorganizing this information into Tables 5.8 and 5.9 shows the identifying parameter of each fault more clearly:

Table 5.9*:* Trigger Parameter by Fault and Operating Point

Fault	Stage	Trip	Stage	Trip	Stage	Trip
A	25°C	--	25°C → 30°C	--	35°C → 25°C	T2
B	25°C	L3	30°C → 35°C	F1	25°C → 35°C	F1
C	25°C	P1	25°C → 35°C	L3	35°C → 30°C	T2
D	30°C	L3	25°C → 35°C	T2	30°C → 25°C	L3
E	30°C	L3	25°C → 30°C	L3	35°C → 25°C	P1
F	30°C	L4	30°C → 35°C	L4	35°C → 25°C	L4
G	35°C	T2	25°C → 30°C	T2	35°C → 30°C	T2
H	35°C	F1	30°C → 35°C	F1	30°C → 25°C	F1
I	35°C	L3	35°C → 30°C	F1	30°C → 25°C	P1

'--' indicates an invalid trial

Neglecting tested operating state:

Table 5.10*:* Trigger Parameter by Fault

Fault	Trip	Trip	Trip
A	--	--	T2
B	L3	F1	F1
C	P1	L3	F1
D	L3	T2	L3
E	L3	L3	P1
F	L4	L4	L4
G	T2	T2	T2
H	F1	F1	F1
I	L3	F1	P1

'--' indicates an invalid trial

The parameter that results in trip for each fault type is shown most clearly in figure 5.10. It can be seen that faults F, G, and H tripped through the same parameter on each trial. Contrarily, faults C and I tripped by means of a different parameter on each insertion. Details for each fault are as follows:

5.6.1 Fault A: Heater Current Failure

Fault A is the simulation of a failure by the reactor control system. This is the first item on the AECB required scenarios and was simulated by an override of the NPCTF heater. It was inserted into operating points: 25^0C, 25^0C →30^0C, and 35^0C →25^0C.

Fault A produced both of the null responses in the experiment. Rather than the algorithm tripping the system in these scenarios, one of the NPCTF's internal mechanisms disabled the heater before a fault could be detected. As the NPCTF contains some safety mechanisms that are unable to be supressed, it cannot be easily determined which was responsible for prematurely shutting down operations. Most likely, the sudden increase in current inadvertently activated the emergency core cooling system, which in turn shut down the primary pump.

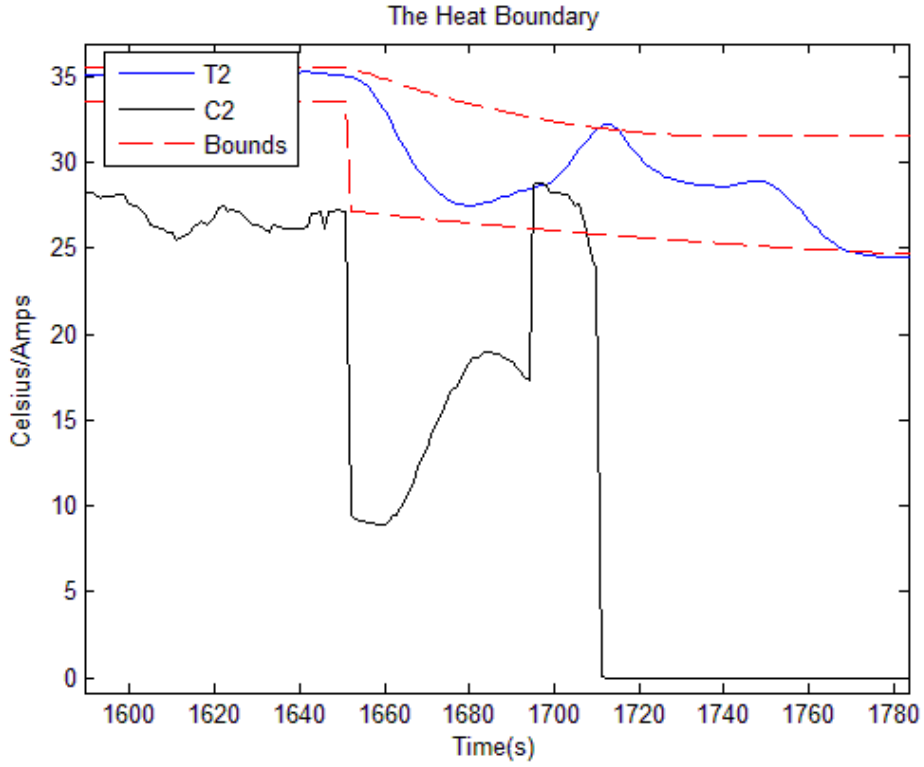

Figure 5.16*:* Result of Fault A when inserted during 35^0C→25^0C Transition*.*

The only instance of the C2 error being correctly inserted is in Figure 5.16. The error produced the expected results, being tripped by aberrant decline of the heater temperature during transition. As demonstrated in Figure 5.16, after the transition begins and the heater temperature begins to rapidly decrease, the fault is inserted and current suddenly rises. This remains high and overheats the heater, preventing it from performing the downward step as

expected. As the temperature behaved abnormally, the safety system recognized the presence of an error and tripped the system.

5.6.2 Fault B: Pump1 Failure

Fault B is the simulation of a failure of the primary pump. This was done by cutting power to the primary pump, representing item 3 on the AECB list. This was inserted into the 25^0C, 30^0C → 35^0C, and 25^0C → 35^0C operating points.

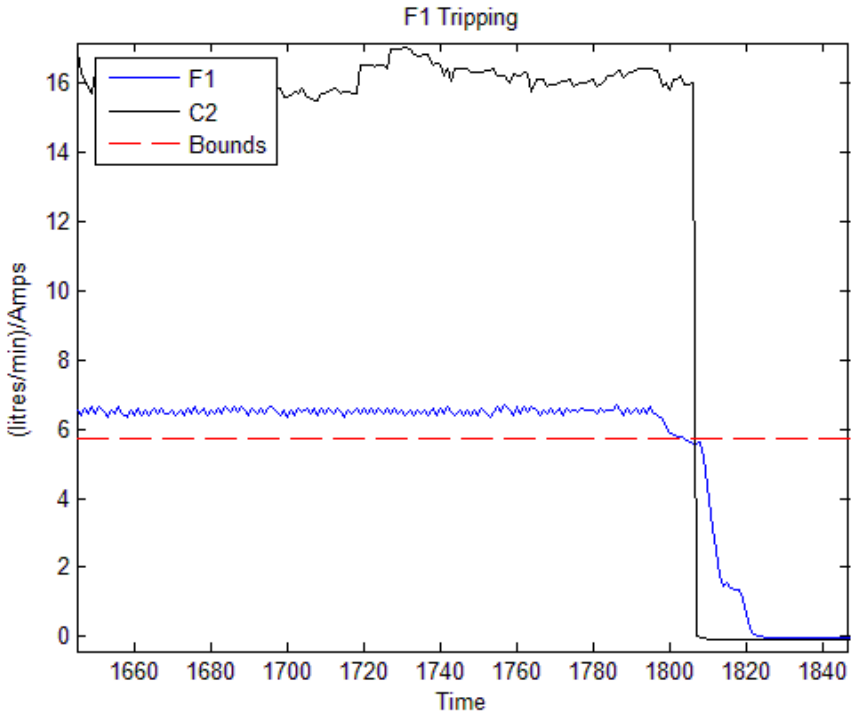

Figure 5.17*:* Result of Fault B when inserted during 25^0C→35^0C Transition.

One instance of the fault insertion is shown in Figure 5.17. Fault B was once detected by a drop of pressure resulting in the pressurizer level dropping, and twice by the diminishing flow in the primary line. The flow responds drastically, as demonstrated in Figure 5.17. In this instance, the flow spent a few seconds decreasing in magnitude before breaching the

bounds. Three seconds following, the soft boundaries had been breached long enough to indicate a fault.

5.6.3 Fault C: CV-3 Open

Fault C is the opening of CV-3 on the primary line, representing item 4 on the AECB list. This represents a failure of a feeder pipe on the primary loop. This fault was inserted into the 25^0C, 25^0C→35^0C, and 35^0C → 30^0C. Fault C tripped on a different parameter on each insertion, tripping on P1, L3, and F1 on the stable, ascending, and descending operating points respectively.

When inserted at the 25^0C operating point, the CV-3 opening caused a sudden pressure drop that resultingly tripped the system. However, during the 25^0C→35^0C, the pressure was maintained slightly better by the pressurizer, though its level consequently fell. The persistent low level of the pressurizer resulted in the safety system tripping the NPCTF, as can be seen in Figure 5.18.

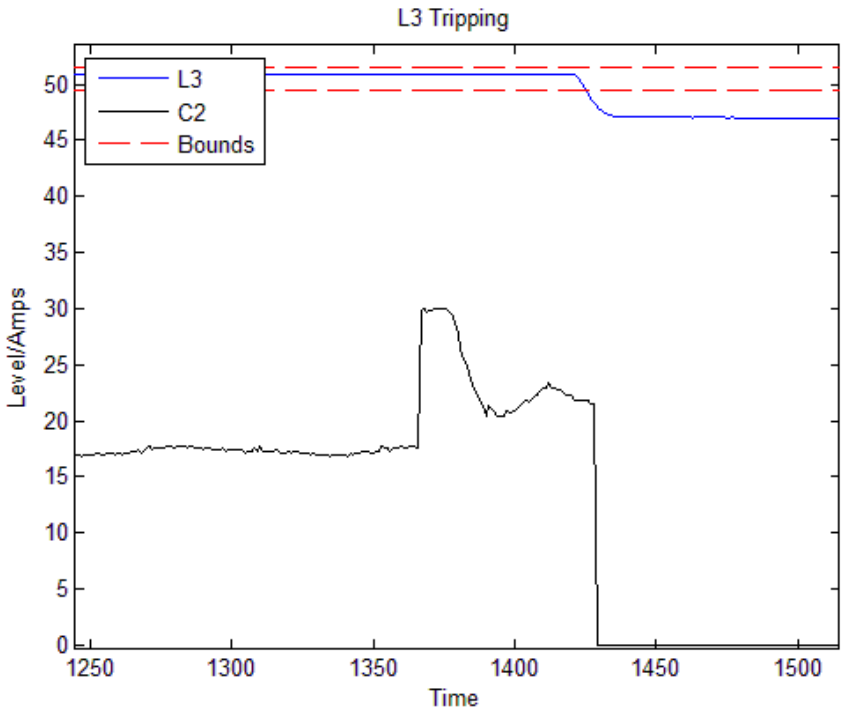

Figure 5.18: Result of Fault C when inserted during 25^0C→35^0C Transition.

When inserted into the 35^0C → 30^0C transition, the opening of CV-3 instead caused a loss of flow. As the valve was opening it likely robbed flow from the primary line and redirected increasing quantities into the lower tank. This particular trial is shown in Figure 5.19.

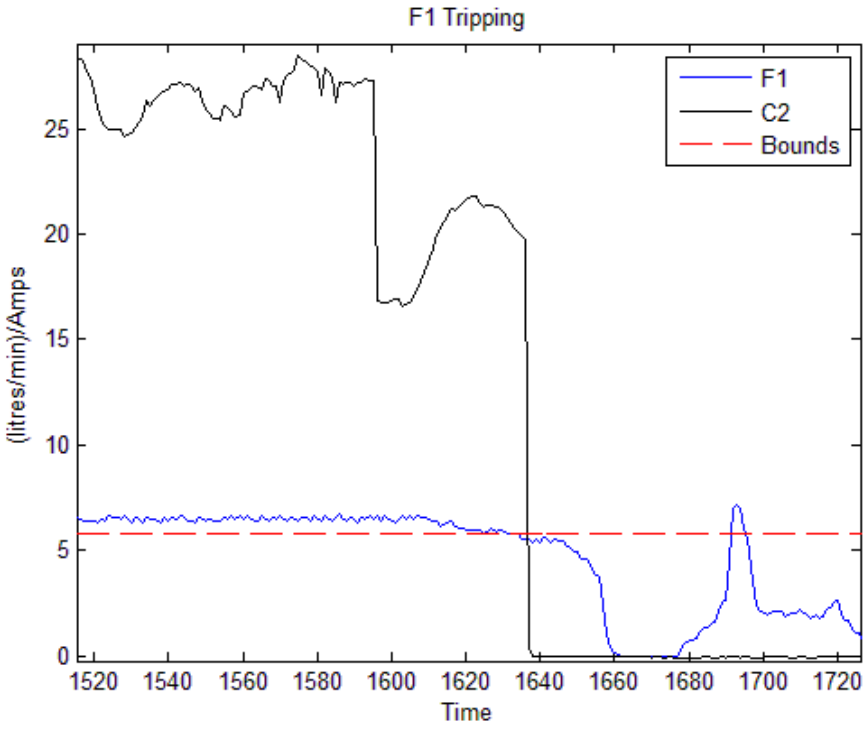

Figure 5.19: Result of Fault C when inserted during 35^0C→30^0C Transition.

All three trials demonstrate success of the safety system in identifying issues in the primary loop as the fault was able to be detected from multiple parameters.

5.6.4 Fault D: LOCA

Fault D represents the infamous LOCA and item 5 on the AECB list. Fault D was created by manually opening FV-1 as explained in section 5.2. Fault D was inserted into the 30^0C, 25^0C →35^0C, and 30^0C → 25^0C. The LOCA trip parameters L3, T2, and L3 respectively.

Though temperature of the reactor is the primary concern, the loss of coolant tripped on pressurizer in two of the three trials. This is seen in Figure 5.20

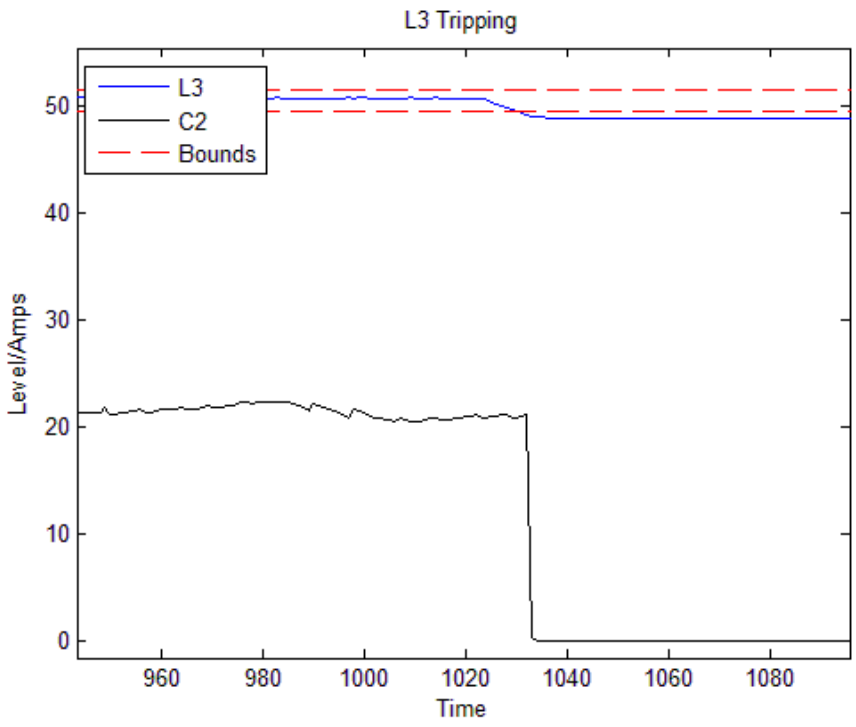

Figure 5.20: Result of Fault D when inserted during 30^0C Operating Point.

As water rushed from the primary line, the pressurizer would have attempted to compensate. Because of the rupture, this attempt was ultimately unsuccessful and led to a loss of water inventory and trip.

When the LOCA was inserted into the 25^0C-35^0C transition, the temperature of the heater incited the trip. This was partially delayed by the heater's control loop attempting to slow the rate of overheating by decreasing the current, as shown in Figure 5.21. Despite the heater control, the temperature quickly exceeded the boundaries and a trip was initiated.

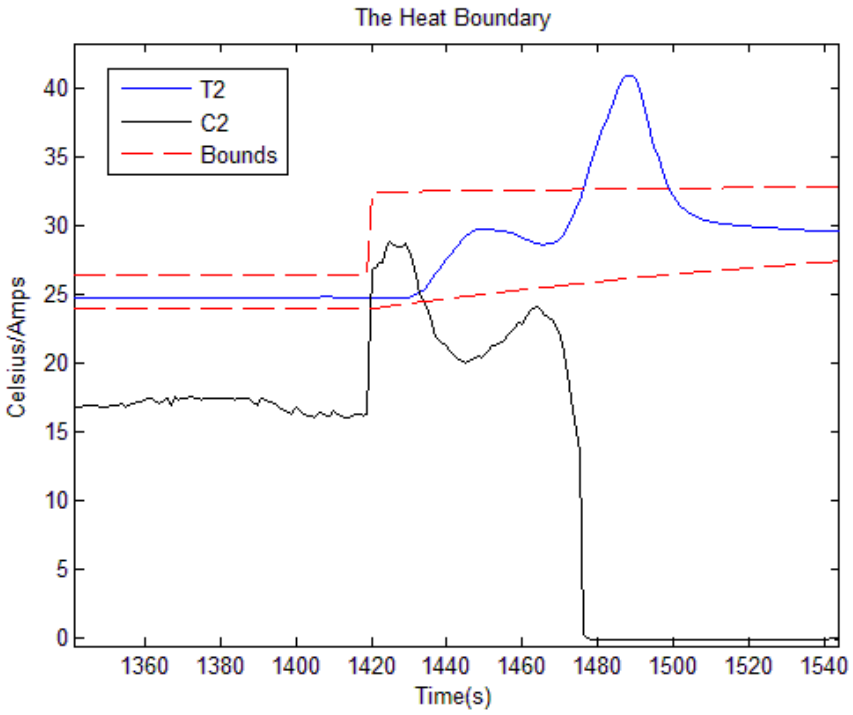

Figure 5.21: Result of Fault D when inserted during 25^0C→35^0C Transition.

5.6.5 Fault E: CV-20 Force Open

Fault E, the opening of CV-20, represents item 9 on the AECB list: the inadvertent opening of a pressure relief or control valve on primary loop. Fault E was inserted into the 30°C, 25°C → 30°C, and 35^0C → 25^0C set points. Fault E tripped based on L3 in the first two trials, and P1 in the third. As CV-20 is a pressurizer error, it is logical to see the faults detected through these parameters.

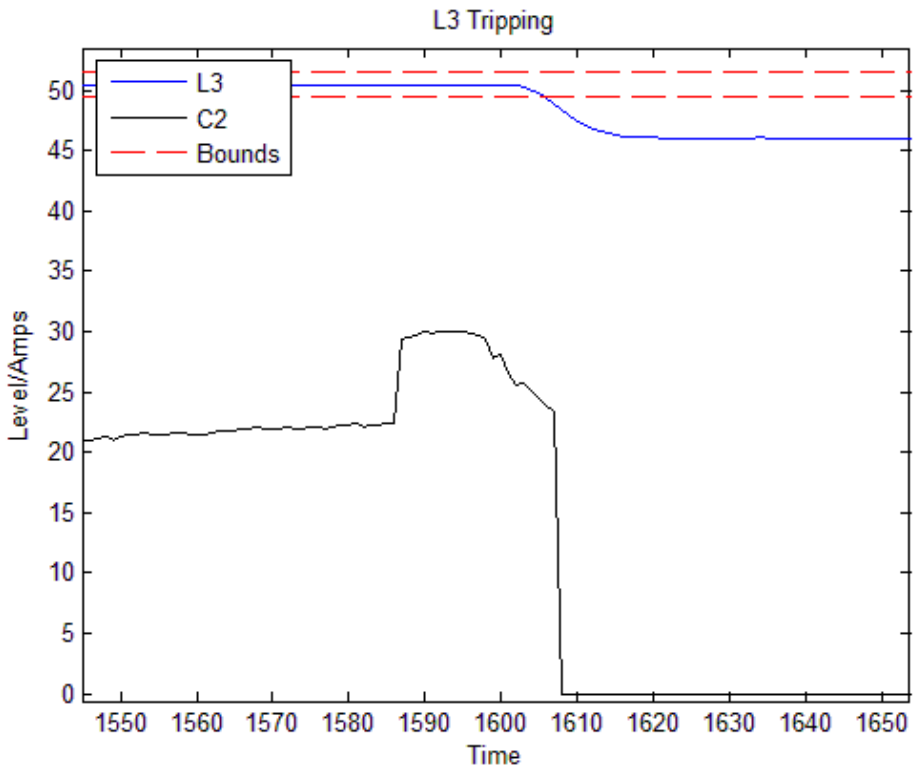

Figure 5.22: Result of Fault E when inserted during 25^0C→30^0C Transition.

The result when inserted into the 25°C → 30°C is shown in Figure 5.22. The pressurizer's water level dropped as inventory loss in the primary line drained the coolant. Consequently, while pressure was maintained, the level of the pressurizer caused the algorithm to initiate a trip.

5.6.6 Fault F: CV-18: Force Open

Fault F is the opening of CV-18, meant to drain the heat exchanger. This simulates the failure of the feed water/steam system and is item 11 on the AECB list. This was inserted into the 30^0C, 30^0C →35^0C, and 35^0C → 25^0C set points. As CV-18 is an HX tank valve, it follows that each fault was detected through the HX tank level, L4.

During the insertions, outgoing water was maximized and the intake could not match pace. The 35^0C → 25^0C insertion interesting as the water level, rather than collapsing, caused a trip due to its failure to produce its characteristic IRC. This is seen in Figure 5.23.

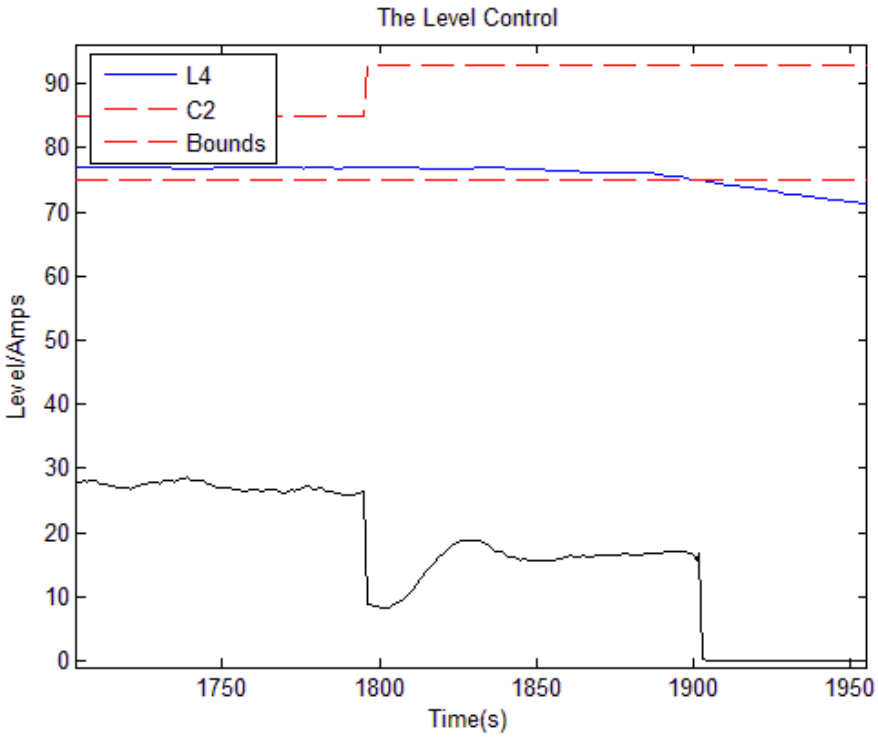

Figure 5.23: Result of Fault F when inserted during 35^0C → 25^0C Transition.

The fault is initiated by the IRC failing to perform, as shown in Figure 5.23. This is due to the IRC being simulated internally by the HX tank control loop. Because the intake and outtake valves have been made faulty, this is not possible. When the IRC does not occur, the safety system recognizes the behaviour as abnormal and initiates the NPCTF trip.

5.6.7 Fault G: Pump3 Failure

Fault G is the failure of Pump 3 in the chiller loop. This is the 13th item on the AECB list and simulates the failure of the service water system. It was inserted into operating points: 35^0C, 25^0C → 30^0C, and 35^0C → 30^0C. The failure of the service water system is a risk due

to the loss of the heat sink. It thus follows that each insertion resulted on a trip based on overheating in the primary loop.

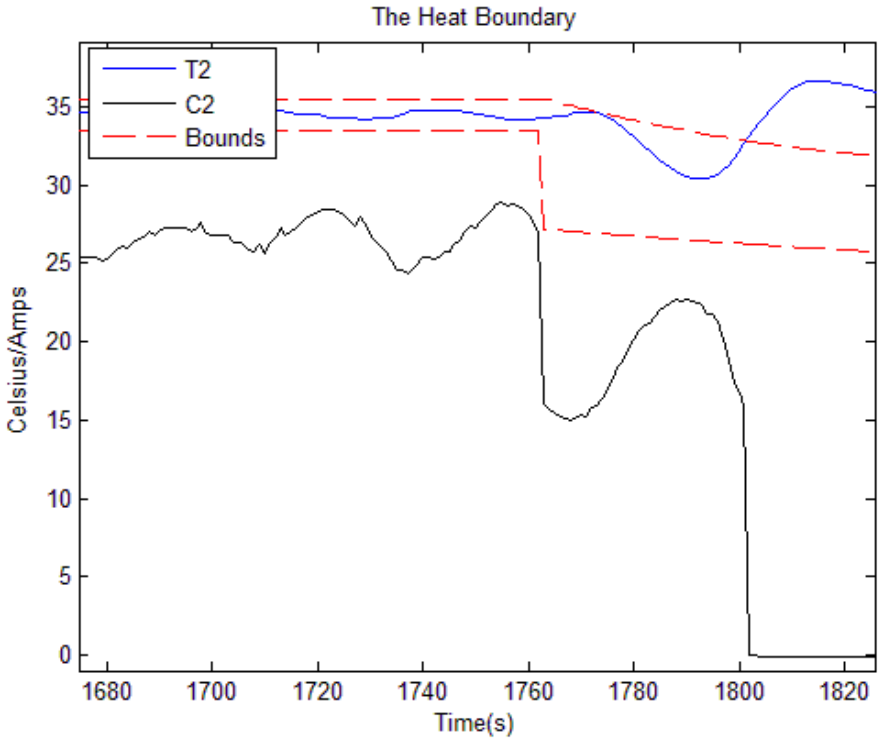

Figure 5.24: Result of Fault G when inserted during 35^0C→30^0C Transition.

The pump3 failure, inserted during a downwards transient as shown in Figure 5.24, overheats the primary line. Though the temperature set point was lowering, the loss of the heat sink is so severe that primary temperature rises above even its initial value. The moving boundary of the safety algorithm are breached, immediately tripping the system.

5.6.8 Fault H: CV-1 & CV-2 Force Close

Fault H is the simultaneous closures of CV-1 and CV-2 on the primary line. This fault was inserted according the 14th item on the AECB list. This the 'any other' requirement on the list and was inserted into the 35^0C, 30^0C →35^0C, and 30^0C → 25^0C set points. The two valves

closing diminished the coolant flow in the primary loop and manifested as a critically low flow rate during each insertion. This can be seen in Figure 5.25.

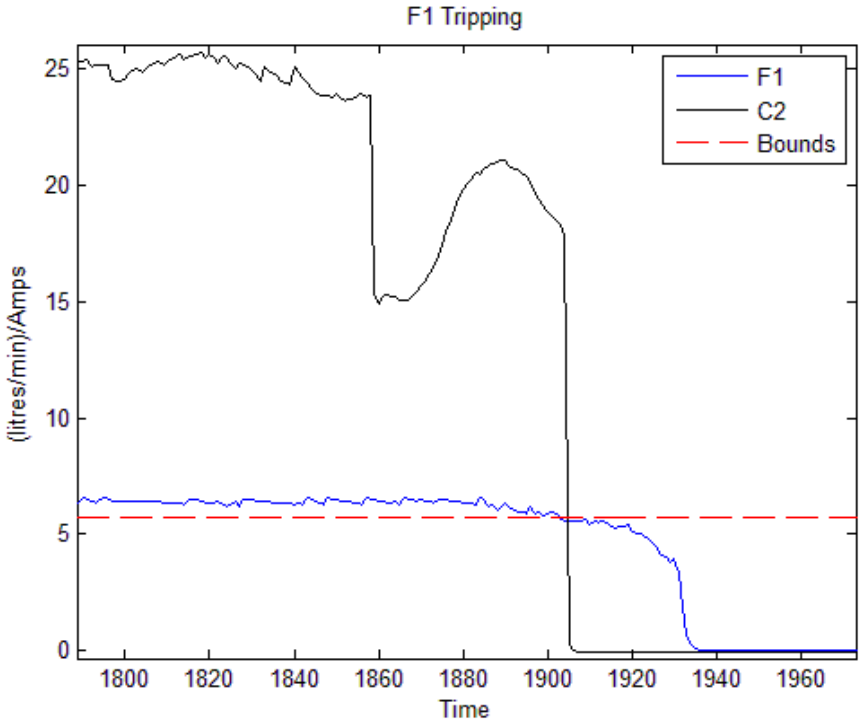

Figure 5.25: Result of Fault H when inserted during 30^0C→25^0C Transition.

With the closure of the two main flow controlling valves, the flow in the primary loop steadily diminishes. Though the parameter is noisy, it never returned back into safe operating regions to reset the counter. Thus, the safety system was forced to shut down the NPCTF.

5.6.9 Fault I: CV-9 Open/CV-10 Force Close

Fault I is the simultaneous opening of CV-9 and closure of CV-10. It is again part of the 14th item on the AECB list, representing the 'any other' requirement. This was inserted into the 35^0C, 35^0C → 30^0C, and 30^0C → 25^0C set points. Fault I tripped on a different parameter in each trial. The first, second, and third trials tripped on L3, F1, and P1 respectively.

When Fault I began to overpressure the pressurizer by closing the air outlet and opening the pressurized air inlet, the water level dropped, as shown in Figure 5.26. Pressure in the pressurizer is not a tripping parameter in CANDU or the safety algorithm, but as pressure increased the water level (L3) fell, causing the safety system to trip.

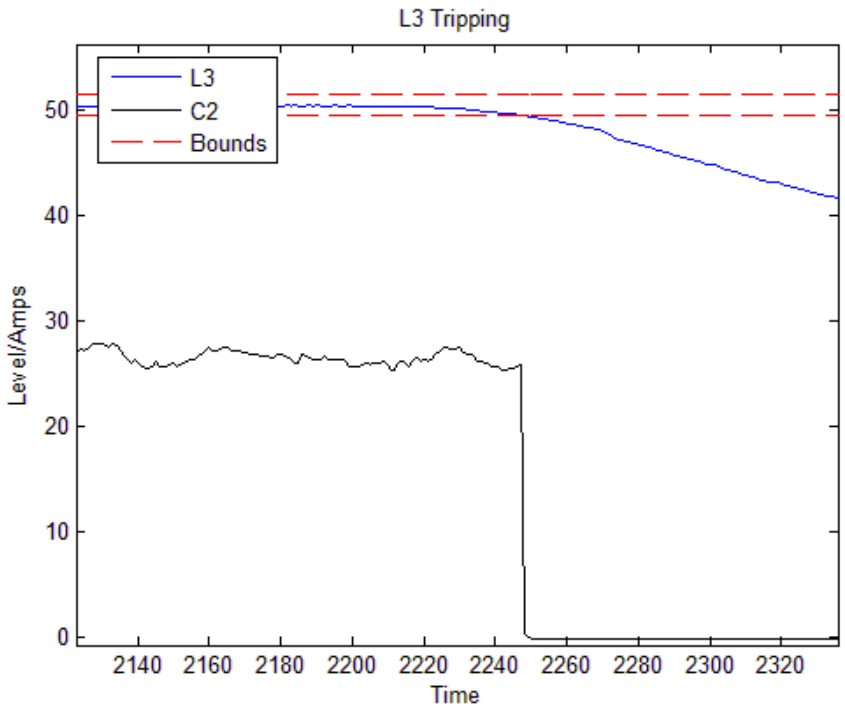

Figure 5.26: Result of Fault I when inserted during 35^0C Operating Point.

5.7 Chapter Summary

The V&V process utilized has demonstrated the successful implementation of the RPS. This implementation is compared against the initial design criteria, as presented in the introduction. The evaluation is as follows:

1. The system must be capable of detecting all faults inserted without exception. Specifically, these faults will be those outlined in CNSC regulatory document R-8

- 9 faults from the CNSC document were inserted: Heater Current Failure, Pump 1 Failure, CV-3 Open, LOCA, CV-20 Open, CV-18 Open, Pump3 Failure, CV-1/CV-2 Close, CV-9/CV-10 Open
- Every fault was examined 3 times, in 3 different situations, with the exception of the heater-current failure which had mistrial twice. This created 25 total test trials
- There were no faults missed, granting the implementation a 25/25 record, and meeting the set criteria

2. The system must not be the cause of spurious trips. The NPCTF, as the system under test, must be able to perform all permissible operations without interference from the RPS
    - The system was tested through two trials where every possible step change was performed. In total, this provided 10+ hours of fault free operation in which to test the design's discretion
    - The system once again achieved a perfect record. No spurious trips were caused, allowing operations to carry-out smoothly
3. All trips must occur within 1s. This will be measured by the NPCTF's internal log and defined as occurring from the recorded bypass to the recorded moment of complete cessation of heater operations
    - The 25 recorded faults each showed the breach and absolute shutdown of heater operations within a single sample of one another
    - Though the fidelity of the recording makes high accuracy readings possible, this implies that each shutdown was completed within 1s of the trip signal

- This meets the performance criteria for speed, once again demonstrating a perfect record for this criteria

6 Conclusions

6.1 Summary

An investigation of the operating characteristics of the NPCTF with the HFC6000 are carried out first. This is accomplishes through nearly 50 hours of non-continuous operation. The findings can be summarized as follows:

1. The NPCTF is chosen to have three discrete operating states: 25°C, 30°C, and 35°C
2. The critical parameters of CANDU, as short-formed to T2, P1, P2, L3, L4, and F1, are shown to fall into two categories: heater-dependent (T2, L4) and heater-independent (P1, P2, L3, and F1)
3. These parameters can be characterized by maximums, minimums, transition times, and other relevant characteristics as explained.
4. The HX tank level, L4, is found to have large inverse response characteristics

These conclusions led to the foundation of the reactor protection system. This implementation has been carried out on a USNRC certified PLC unit, the HFC6000. The implementation is first coded into Matlab, then translated into STL. The summary of the implementation are as follows:

1. Three of the heater independent parameters (F1, P1, and L3) benefitted from the use of soft boundaries. These boundaries used 3s timers (F1 lower, L3 upper and lower), and 2s timers (P1 upper and lower)
2. The software could be written into a single loop and a start-up routine. The single loop is able to make calls to subroutines used calculate transient boundaries when necessary
3. The current to the heater is measured by a single subroutine. It makes use of spikes in current to identify forthcoming transients and characterise them as much as necessary

4. The transitions by heater-dependent parameters are handled by the called subroutines. The heater temperature was handled by a single subroutine, while the HX tank level was handled by two due to inverse response characteristics and overshoot
5. The total time of shutdown is calculated to be 489ms in worst case scenario. This is beyond the resolution of the NPCTF recording devices, but sufficient for the implementation

Finally, the validation process tested the implementation on the NPCTF using regular operations and fault insertion scenarios. The simulated faults comply with CNSC standard scenarios. The following findings have been made:

1. The system demonstrates appropriate judgement, as demonstrated through the normal operations testing, producing no spurious trips in 10+ hours of operation
2. The system demonstrates high accuracy, detecting 25 of 25 faults, a perfect record against the CNSC design basis accidents
3. The system has achieved the desired speed, and is able to shut down the NPCTF within 1s of the theoretical trip signal for each design basis accident

6.2 Conclusions

This thesis started with the objective of designing, implementing, and testing a reactor protection system. Based on the discussed summaries, all of the research objectives have been met. The systematic approach discussed in the V&V process has provided the following conclusions:

1. A relationship between a CANDU NPP and the NPCTF has been established

2. A protection scheme has been designed based on the critical parameter parallels between a CANDU NPP and the NPCTF
3. An RPS has been implemented using industrial grade safety PLC to operate on the NPCTF
4. The designed RPS has been properly implemented and meets all necessary design criteria though validation and verification process.

6.3 Future Work

The subsequent work will progress with the design and implementation of two additional safety systems on the NPCTF. This permits the following advancements:

- Creates comparisons for the HFC implemented safety system. Direct performance comparisons in speed, accuracy, and discretion can only be made against systems likewise designed for the NPCTF.
- Permits use of 2oo3 voting logic. This both improves the overall safety design of the NPCTF and increases fidelity to CANDU systems.
- Improves the system through the use of redundancy and diversity, especially if additional systems utilize different safety controllers.

Further, as the NPCTF is capable of being configured to mimic the I&C processes of different NPPs, safety logic for each type of NPP can be different. Even though this thesis concentrates on CANDU type of NPP, the similar work can also be done for other types of NPPs.

7 References

[1] AECL, "CANDU Fundamentals - Section 9: Nuclear Safety," Ottawa, Canada, CNSC, 2004

[2] J. Ma, “PCTF and Control”, UWO- CIES Research Group, London, ON, 2013

[3] G. Pon. Nuclear Power Symposium, Topic: “Lecture No. 1: Introduction.” Sheridan Park, CAN, 1972.

[4] C. Beck. “Concepts of Reactor Physics, Without the Mathematics.” IEEE Transactions on Nuclear Science, vol. 39, pp. 461-463, June 1992

[5] CANDU. EC6: Enhanced CANDU 6 Technical Summary. Mississauga, CAN.: CANDU, 2013, pp. 1-42.

[6] R. Steed. Nuclear Power in Canada and Beyond. Renfrew, CAN: General Store Publishing House, 2007.

[7] J. Cai, S. Sen, and N. Barkman, "Safety Systems and Safety Analysis of the Qinshan Phase III CANDU Nuclear Power Plant," Nuclear Power Engineering, vol. 20, pp. 519-525, 1999.

[8] Case study on the use of PSA methods: Assessment of technical specifications for the reactor protection System Instrumentation, ser. TECDOC, no. 669, IAEA, Oct. 1992.

[9] IAEA. The Statute of the IAEA. New York, USA: The United Nations, 1956.

[10] IAEA. “The IAEA Mission Statement.” Internet: https://www.iaea.org/about/mission, Nov 2, 2014 [August 2, 2015].

[11] IEEE-SA NPEC. “Policies and Procedures for Standard Development” New York, USA. December 2012.

[12] IEEE, IEEE 383 – 2003: IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations, IEEE, 2008.

[13] IEEE, IEEE 603 – 2009: IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE, 2009.

[14] IEEE Power and Energy Society. “IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations” U.S. IEEE Std. 308-2012, 16 Jan. 2013.

[15] IEC. “IEC Partners.” Internet: http://www.iec.ch/dyn/www/f?p=103:218:0, 2015* [June 22, 2015].

[16] IEC and IEEE. “Guide to IEC/IEEE Cooperation” Geneva, Switzerland. 2012-08. August, 2012.

[17] IEC, "IEC-62340: Nuclear power plants - Instrumentation and control important for safety - Requirements for Coping with Common Cause Failures" 2007.

[18] IEC, "IEC-61513: Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems," 2001.

[19] IEC, "IEC-60880: Nuclear power plants - Instrumentation and control important for safety - Software aspects for computer-based systems performing category A functions," 2006

[20] Ministry of Justice. "Nuclear Safety and Control Act." SC 1997, C.9, 1997.

[21] Ministry of Justice. "General Nuclear Safety and Control Regulations." Canada. SOR/2000-202, April 17, 2008.

[22] Atomic Control Board Canada, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants," Atomic Control Board Canada, Regulatory Documentation R-8, 1991.

[23] A. Viktorov. "Development of Best Estimate Analysis Methods in Canada to Allow Quantification of Safety Margins" IAEA-TECDOC-1332, 2003, pp. 127-142

[24] R Nevalainen, J Halaminen, H Harju, M Johansson, Certification of Software in Safety-Critical I&C Systems of Nuclear Power Plants, InTech Europe, Rijeka Croatia (2010)

[25] CAE. "About Us." Internet: http://www.cae.com. 2010. [Nov. 12, 2014]

[26] WSC, "About Us." Internet: https://www.ws-corp.com. 2010. [Nov. 12, 2014]

[27] L-3 Communications MAPPS Inc., "About Us." Internet: http://www.mapps.l-3com.com. 2010. [Nov. 12, 2014]

[28] D. Rankin, J. Jiang, "A Hardware-In-The-Loop Simulation Platform for the Verification and Validation of Safety Control Systems" IEEE Transactions on Nuclear Science, VOL. 58, NO. 2, pp 468-478 (2011)

[29] M Lin et al. "Main control system verification and validation of NPP digital I&C System based on engineering simulator". Nuclear Engineering and Design, vol. 240, pp. 1887-1896, Mar. 2010.

[30] Solutions for Cost Effective Assessment of Software Based Instrumentation and Control Systems in Nuclear Power Plants, ser. TECDOC, no. 1328, IAEA, Dec. 2002.

[31] IEEE Computer Society. "IEEE Standard for System and Software Verification and Validation" U. S. . IEEE Std. 1012, 25 May 2012.

[32] L. Xia. Development of 3-D Neutronic Kinetic Model and Control for CANDU Reactors. London CAN., School of Graduate and Postdoctoral Studies, The University of Western Ontario, 2012

[33] E. Critoph. Nuclear Power Symposium, Topic: “Lecture No. 4: Reactor Physics.” Sheridan Park, CAN, 1972.

[34] M. MacBeth. IAEA - CANDU I&C, Topic: “Lesson 7: Reactor Control and Protection - Module 3: Reactor Regulating System” Shanghai, China, Jun. 2004.

[35] D. Meneley. A Reactor Cannot Explode Like a Nuclear Bomb. Ottawa, Canada: Canteach Initiative, Dec 2002

[36] V. Snell. AECL Safety Lecture Series, Topic: “CANDU Safety #5- Safety Functions-Shutdown Systems.” Ottawa, CAN., May 2001.

[37] M. MacBeth. IAEA - CANDU I&C, Topic: “Lesson 9: Reactor Protection, Module 1: Reactor Protection Systems” Shanghai, China, Jun. 2004.

[38] G. Kessler et al. The Risks of Nuclear Energy Technology, Science Policy Reports, Berlin, Germany: Springer, 2014, pp 11-30.

[39] R. Gilbert. “Digital Computers in CANDU Safety Systems: Part II- Implementation and Experience”. IEEE Transactions on Nuclear Science, vol.NS-25, No. 3, pp 1912-1916, June 1983.

[40] M. MacBeth. IAEA - CANDU I&C, Topic: “Lesson 9: Reactor Protection, Module 2: Trip Computer Systems and Safety Critical Software” Shanghai, China., Jun. 2004

[41] USNRC. “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants.” USA. NUREG 0800, June 1987.

[42] D. Meneley. Nuclear Safety and Reliability. Ottawa, Canada: Canteach Initiative, Oct 2003.

[43] P. Winokur et Al. “Use of COTS Microelectronics in Radiation Environments”. IEEE Transactions on Nuclear Science, vol.25, No. 6, pp 1494-1503, Dec 1999.

[44] IEC, "IEC-61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety Related Systems" 2010.

[45] "Software for Computer Based Systems Important to Safety in Nuclear Power Plants," IAEA NS-G-1.1, 2000.

[46] "Instrumentation and Control Systems Important to Safety in Nuclear Power Plants," IAEA NS-G-1.3, 2002.

[47] USNRC. “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.” USA. NUREG 7007, December 2008.

[48] IAEA. “Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants.” Austria. No. NP-T-1.5, 2009.

[49] V. Karchenko et al. ICONE 22, Topic: “Standard Analysis and Tool-Based Assessment Technique of NPP I&C Systems Diversity.” Prague, CZR, July 2014.

[50] G. Cowper. Nuclear Power Symposium, Topic: “Lecture No. 2: Power Reactor Types.” Sheridan Park, CAN, 1972.

[51] J. Hortal, "Safety Margins: Deterministic and Probabilistic Views" in Implications of Power Uprates on Safety Margins of Nuclear Power Plants, 2004.

[52] "Safety Margins of Operating Reactors—Analysis of Uncertainties and Implications for Decision Making," IAEA, IAEA-TECDOC-1332, 2003.

[53] C. R. Tuley and R. B. Miller, “Westinghouse set point methodology for control and protection systems,” IEEE Trans. Nucl. Sci., vol. NS-33, no. 1, pp. 684–687, Feb. 1986.

[54] R. J. Dodson and M. A. Feltus, “Low temperature overpressurization protection system set point analysis using RETRAN for Salem,” Ann. Nucl. Energy, vol. 23, no. 6, pp. 487–498, Apr. 1996.

[55] S. H. Yang, S. H. Kim, Y. J. Chung, and S. Q. Zee, “Trip set point analysis for the reactor protection system of an advanced integral reactor,” Ann. Nucl. Energy, vol. 34, no. 4, pp. 319–325, Apr. 2007.

[56] M. Mladin, D. Dupleac, and I. Prisecaru, "SCDAP/RELAP5 application to CANDU6 fuel channel analysis under postulated LLOCA/LOECC conditions," Nuclear Engineering and Design, vol. 239, pp. 353-364, 2009.

[57] J.C. Luxat, R.G. Huget, D.K. Lau, F. Tran, "Development and Application of Ontario Power Generation's Best Estimate Nuclear Safety Analysis Methodology", in Proceedings of ANS International Meeting on Best Estimate Methods in Nuclear Installations Safety Analysis, Washington, DC, November 2000.

[58] Technical Program Group, “Quantifying reactor safety margins: application of CSAU methodology to a LBLOCA,” EG&G Idaho, Inc., NUREG/CR-5249, December 1989.

[59] A. Kaliatka, R. Urbonas, and M. Vaisnoras, "Evaluation of uncertainties for safety margins determination at the analysis of maximum design basis accident in RBMK-1500," in Implications of Power Uprates on Safety Margins of Nuclear Power Plants, pp. 109-117, 2004.

[60] C. Jae Lee et al. "Set point Methodology Improvement Considering Beyond Design Basis Events for Safety-Related Instrumentation." IEEE Transaction on Nuclear Science, vol. 61 issue-4, pp. 2120-2130, Aug. 2014

[61] D Novog and P Sermer. “A Startisitical Methodology for Determination of Safety Systems Actuation Setpoints Based on Extreme Value Statistics”. Science and Technology of Nuclear Installations, vol. 2008, pp 1-10, Feb. 2008.

[62] P. Sermer, G. Balog, D. R. Novog, E. A. Attia, and M. Levine, “Monte Carlo computation of neutron overpower protection trip set-points using extreme value statistics,” in Proceedings of the 24th Annual CNS Conference, Toronto, Ontario, Canada, June 2003.

[63] ISA Recommended Practice RP67.04.02-2000, “Methodologies for the determination of set points for nuclear safety related instrumentation,” January 2000.

[64] YVL 5.5, Instrumentation systems and components at nuclear facilities. STUK 2002.

[65] IEC, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems. Ed 2.0., IEC, April 2010.

[66] IEC, IEC 15504, Information Technology - Process Assessment. Ed 1.0., IEC, November 2004.

[67] R. Uhrig, R. Carter. Instrumentation, Control and Safety Systems of Canadian Nuclear Facilities. Baltimore, USA: International Technology Research Institute- JTEC/WTEC Program, 1993.

[68] IEC, "IEC-61131-1: Programmable Controllers - Part 1: General Information" 2003.

[69] IEC, "IEC-61131-3: Programmable Controllers - Part 3: Programming Languages" 2013.

[70] "The Programmable Logic Controller and Its Application in Nuclear Reactor Systems," U.S. NRC, NUREG/CR-6090, UCRL-ID-112900, 1993.

[71] Invensys. “Triconex Approved Topical Report.” USA. 7285-545-1-A, Rev. 4, May 2012.

[72] J. Ma, PCTF Subsystems, London, CAN: UWO- CIES Research Group, 2013.

[73] ABB. “The Controller AC 700F.” Switzerland. 38DD015188 Rev A.

[74] American Sensor Technologies. “AST4100 Compact Stainless Steel Media Isolated Pressure Sensor.” USA. AST4100, July 2007.

[75] American Sensor Technologies. “AST5100 Wet/Wet- Low Differential Pressure Transmitter.” USA. AST5100, 2009.

[76] Lake Monitors. “FlowStat-Turbine Flow Sensor.” USA. FSDS-1106, 2006.

[77] Belimo. “LF24-SR Actuators, Proportional.” USA. K20903, March 2008.

[78] ISO. “Quality Management Systems.” United Kingdom. ISO 9001:2008, 2008.

[79] IEC, "IEC-61131-2: Programmable Controllers - Part 2: Equipment Requirements and Tests" 2008.

[80] Laing Thermotech. “ecocirc D5 Solar DC Pump.” USA. BR-20, 2009.

[81] Brazetek Heat Exchangers. “Brazed Plat Heat Exchangers.” USA. BT3x8-16, 2012.

[82] J. She. Investigation on the Benefits of Safety Margin Improvement in CANDU Nuclear Power Plant Using an FPGA-Based Shutdown System. London CAN., School of Graduate and Postdoctoral Studies, The University of Western Ontario, 2012.

[83] intempc. “MIST03 Temperature Sensor w/ Programmable 4-20mA Output.” USA. US 7,223,014 B2, 2012.

[84] Gaumer Process. “C15P3N18T2.” USA. C15P3N18T2, 2012.

[85] V. Istvan-Szilard. "Steam Generator Water Level Control of a Nuclear Power Plant." Proc. Interdisciplinarity in Engineering Scientific International Conference, 2007, pp. V-12-1 V-12-6.

[86] HF Controls Corporate Profile http://www.hfcontrols.com/corporate.htm (Retrieved Nov 2014)

[87] Doosan HF Controls Corporation, "Technical Notes TN008-001-09, HFC-6000," Doosan Group, Seoul South Korea (2013)

[88] Doosan HF Controls Corporation, "HFC-SBC06-DPM06 Boards Module Design Specification, Rev C”, Doosan Group, Seoul South Korea (2007)

[89] Intel. “Intel386 EX Embedded Microprocessor.” USA. 272420-007, Oct 1999.

[90] Doosan HF Controls Corporation. “HFC-6000 I/O Board Module Design Specification, MS901-000-02, Rev A” Seoul South Korea. Nov 2003.

[91] Doosan HF Controls Corporation. “EWS User's Guide. Software Revision 2.00, UG04-000-01, Rev E” Seoul South Korea. 2007.

[92] Q. Chou, P. Achhion, and P. Kar. “Safety Considerations in Design of a Unique Nuclear Steam Generator Feed water Control System.” Proc. American Control Conference. June 1985. pp 1451-1456.

[93] G. Hepburn. “Instrumentation and Control” in The Essential CANDU, Canada: UNENE Network, Sept 2014.

[94] Canteach. "Couse 223-Boiler and Auxiliary". Ottawa, Canada: Canteach Initiative, June 1992.

[95] CNSC. “Licensing Process for New Nuclear Power Plants in Canada.” Canada. INFO-0756 R-1, May 2008.

[96] F.J. Doria, "CANDU Safety Course #12: Large Loss of Coolant Accident," AECL, 1999.

[97] V. Snell. AECL Safety Lecture Series, Topic: “CANDU Safety #14- Loss of Heat Sink.” Ottawa, CAN., May 2001.

[98] IAEA. INES: The International Nuclear and Radiological Event Scale- User's Manual, 2008 Edition. Vienna: IAEA, 2008.

[99] Y. Khalil. “Risk Assessment and Safety Analysis for Commercial Nuclear Reactors” in Nuclear Engineering Handbook, K.D. Kok, Boca Raton, USA: CRC Press, Taylor and Francis Group, 2009, pp 525-541.

[100] W Garland. Core Composition Changes. Ottawa, Canada: Canteach Initiative, July 2005.

[101] G. Kessler et al. “Some Facts about Neutron and Reactor Physics” in Risks of Nuclear Energy Technology - Safety Concepts of Light Water Reactors. G. Kessler. New York, USA: Springer, 2014, pp 11-30.

[102] International Nuclear Safety Advisory Group. Safety Series No. 75: INSAG-7, The Chernobyl Accident: Updating of INSAG-1. Vienna, AUS: IAEA, 1992.

[103] ANS. “Fukushima Daiichi: ANS Committee Report.” Internet: http://fukushima.ans.org/report/accident-analysis, June 2012, [Feb 24, 2015].

Appendix A: Matlab Code

This appendix presents the simulated coding as written into Matlab. This coding is a functional imitation of the HFC6000 code as discussed in Section 4.3: Description of Implemented Monitoring Software and presented in Appendix B. For aid in referencing what each memory item is used for, refer to Appendix C: HFC Items List

```
%A full simulation of the code as run on NPCTF recorded data
clean

%Open the files
experiment = 'experiment1.mat';
StartUp

%Extra Things
t=0;
tmax=length(C2);

%%%%%%%%%%%%%%%%%%%%%%%%%Initialization%%%%%%%%%%%%%%%%%%%%%%%%%
while 1==1
    %Start of the program

    %Initialize Inputs/Outputs
    BL=zeros(length(C2),26);
    FL=zeros(length(C2),31);
    CO=zeros(length(C2),14);
    TI=zeros(length(C2),12);
    DO=zeros(length(C2),16);

    BL(:,9)=31.5; %T2max
    BL(:,10)=28.5; %T2min
    BL(:,14)=80; %L4max
    BL(:,15)=60; %L4min
    BL(:,25)= 5.65;%P2maX
    BL(:,26)= 3.2;%P2miN
    BL(:,12)= 51.5;%L3maX
    BL(:,13)= 49.5;%L3miN
    BL(:,16)= 5.75;%F1miN
    BL(:,22)= 10.5;%P1maX
    BL(:,23)= 7.25;%P1miN
    BL(:,17)=C2(1); %C2n-1
    BL(:,18)=0; %C2n-2
    BL(:,19)=0; %C2n-3
    BL(:,20)=0; %C2n-4
    BL(:,21)=0; %C2n-5
    break
end

%%%%%%%%%%%%%%%%%%%%%%%%%StartUpLoop%%%%%%%%%%%%%%%%%%%%%%%%%
while t<tmax

    %Read the AI
    t=t+1;
    AIRead
```

```
    %Test for start up count
    if CO(t,4)>=120; %20
        break
    end

    %If C2>25%, increment, else set count to 0
    if BL(t,1)>12.5
        CO(t+1,4)=CO(t,4)+1;
    else
        CO(t+1,4)=CO(t,4);
    end

    %If any of the absolute trips (T2 and C2) have defied their max
    %FL(t,9)=(BL(t,1)>(BL(t,17)+3))||(BL(t,1)<BL(t,17)-3);
    DO(t,1)=(BL(t,1)>45)||(BL(t,2)>BL(t,9)); %45 Amps or 36'C

end

%%%%%%%%%%%%%%%%%%%%%%%%%Operations%%%%%%%%%%%%%%%%%%%%%%%%%
while t<tmax

    %Start of Loop2
    t=t+1;
    Carry
    AIRead
    DO(t,10)=1;

%%%%%%%%%%%%%%%%%%%%%%%%%C2Tracker%%%%%%%%%%%%%%%%%%%%%%%%%
    while 1==1

        %Do a long list of hand-me-downs
        BL(t,21)=BL(t-1,20);
        BL(t,20)=BL(t-1,19);
        BL(t,19)=BL(t-1,18);
        BL(t,18)=BL(t-1,17);
        BL(t,17)=BL(t-1,1);

        %Determine the spike direction
        if BL(t,17)>BL(t,1)&&not(FL(t-1,9))
            FL(t,10)=0; %So the direction will keep getting set until
FL(t,9 is set
        else if BL(t,17)<BL(t,1)&&not(FL(t-1,9))
                FL(t,10)=1;
            end
        end

        %Is there a jump?
        FL(t,9) = (((BL(t,17)-
2.5)>BL(t,1))||((BL(t,17)+2.5)<BL(t,1)))||FL(t,9);

        %Is there drift?

FL(t,15)=(FL(t,12)&&(BL(t,17)<21)||BL(t,17)>23.5)||(FL(t,13)&&(BL(t,17)<24)
||(BL(t,17)>22.5))||(FL(t,14)&&(BL(t,17)<27)||(BL(t,17)>30.5))||not(FL(t,19
));
        %ie. We're not escaping if we're in transit
```

```
        %if we drift, allow it only twice in a row
        if FL(t,15)
            CO(t,1)=CO(t-1,1)+1;
        else
            CO(t,1)=0;
        end
        if CO(t,1)>2
            DO(t,1)=1;
            break
        end

        %if you've drifted, you're not going to get a good settle reading,
        %so bypass it
        if FL(t,15)
            FL(t,12)=FL(t-1,12);
            FL(t,13)=FL(t-1,13);
            FL(t,14)=FL(t-1,14);
            break
        end

        %Increment the counters according to where settling is occuring
        %25'C = 21<x<23.5
        if
(BL(t,17)>21)&&(BL(t,17)<23.5)&&(BL(t,18)>21)&&(BL(t,18)<23.5)&&(BL(t,19)>2
1)&&(BL(t,19)<23.5)&&(BL(t,20)>21)&&(BL(t,20)<23.5)&&(BL(t,21)>21)&&(BL(t,2
1)<23.5);
            CO(t,7)=CO(t,7)+1;
            if CO(t,7) > 90
                CO(t,7)=90;
            end
        else CO(t,7)=CO(t,7)-5;
        end
        %30'C = 24<x<27.5
        if
(BL(t,17)>24)&&(BL(t,17)<27.5)&&(BL(t,18)>24)&&(BL(t,18)<27.5)&&(BL(t,19)>2
4)&&(BL(t,19)<27.5)&&(BL(t,20)>24)&&(BL(t,20)<27.5)&&(BL(t,21)>24)&&(BL(t,2
1)<27.5);
            CO(t,8)=CO(t,8)+1;
            if CO(t,8) > 90
                CO(t,8)=90;
            end
        else CO(t,8)=CO(t,8)-5;
        end
        %35'C = 27<x<30.5
        if
(BL(t,17)>27)&&(BL(t,17)<30.5)&&(BL(t,18)>27)&&(BL(t,18)<30.5)&&(BL(t,19)>2
7)&&(BL(t,19)<30.5)&&(BL(t,20)>27)&&(BL(t,20)<30.5)&&(BL(t,21)>27)&&(BL(t,2
1)<30.5);
            CO(t,9)=CO(t,9)+1;
            if CO(t,9) > 90
                CO(t,9)=90;
            end
        else CO(t,9)=CO(t,9)-5;
        end

        %25'C Settling
        if CO(t,7)>60
```

```
            FL(t,12)=1;
        else
            FL(t,12)=0;
        end
        %30'C Settling
        if CO(t,8)>60
            FL(t,13)=1;
        else
            FL(t,13)=0;
        end
        %35'C Settling
        if CO(t,9)>60
            FL(t,14)=1;
        else
            FL(t,14)=0;
        end

        %Exit the current tracker
        break

    end

%%%%%%%%%%%%%%%%%%%%%%%%%Boundaries%%%%%%%%%%%%%%%%%%%%%%%%%
    while 1==1
        %The Non-Transitive Limits
        BL(t,25)= 5.65;%P2maX
        BL(t,26)= 3.2;%P2miN
        BL(t,12)= 51.5;%L3maX
        BL(t,13)= 49.5;%L3miN
        BL(t,16)= 5.75;%F1miN
        BL(t,22)= 10.5;%P1maX
        BL(t,23)= 7.25;%P1miN

        %Check for Spike Flag. If active, jump to HeatX
        while FL(t,9)==1

%%%%%%%%%%%%%%%%%%%%%%%%%Start of Heat Transition%%%%%%%%%%%%%%%%%%%%%%%%%
            while 1==1
                %Receive the jump
                DO(t,12) = 1;

                %Stage 1
                %First visit?
                %Assume a step using direction flag
                %25-30 if: Up, @25
                FL(t,16) = (FL(t,10)&&FL(t,12)&&not(FL(t,19)))||FL(t,16);
                %30-35 if: Up, @30
                FL(t,17) = (FL(t,10)&&FL(t,13)&&not(FL(t,19)))||FL(t,17);
                %35-30 if: Down, @35
                FL(t,23) =
(not(FL(t,10))&&FL(t,14)&&not(FL(t,19)))||FL(t,23);
                %30-25 if: Down, @30
                FL(t,24) = (not(FL(t,10))&&
FL(t,13)&&not(FL(t,19)))||FL(t,24);
                %Trip if up at 35, or down at 25
                %JUMP L0011 IF ((FL(t,10 && FL(t,14) || (not(FL(t,10 &&
FL(t,12))&&not(FL(t,19
```

```
%Set timers-even the big ones if they applied
if (FL(t,16) && not(FL(t,19)))%T2 25-30
    TI(t,02)= 240.0;
end
if (FL(t,17)&&not(FL(t,19)))%T2 30-35
    TI(t,03)= 1500.0;
end
if (FL(t,18)||FL(t,16))&&not(FL(t,19));%T2 25-35
    TI(t,04)= 1800.0;
end
if (FL(t,23) && not(FL(t,19))) ;%T2 35-30
    TI(t,05)= 90.0;
end
if (FL(t,24) && not(FL(t,19))) ;%T2 30-25
    TI(t,06)= 150.0;
end
if (FL(t,25) || FL(t,23)) && not(FL(t,19)) ;%T2 35-25
    TI(t,07)= 240.0;
end
if (FL(t,16) && not(FL(t,19))) ;%L4 25-30
    TI(t,08)= 300.0;
end
if (FL(t,17) && not(FL(t,19))) ;%L4 30-35
    TI(t,09)= 240.0;
end
if (FL(t,18)||FL(t,16))&&not(FL(t,19)) ;%L4 25-35
    TI(t,10)= 420.0;
end
if (not(FL(t,10))&&not(FL(t,19))) %L4 IRC Delay
    TI(t,12)=300;
end

%Set stage 1 flag
if not(FL(t,19))
    FL(t,19)=1;
    FL(t,12)=0;
    FL(t,13)=0;
    FL(t,14)=0;
    FL(t,22)=0;
    CO(t,7)=0;
    CO(t,8)=0;
    CO(t,9)=0;
end

%Build new bounds
%25-30
if FL(t,16)
    BL(t,9) = 31.5 - (5/240/240)*(TI(t,02))*(TI(t,02))/3;
    BL(t,10) = 28.5 - (4.5/240/240)*(TI(t,02))*(TI(t,02));
end

%30-35
if FL(t,17)
    BL(t,9) = 35.5 - (4/1500/1500)*(TI(t,03))*(TI(t,03))/3;
    BL(t,10) = 33.5 - (5/1500/1500)*(TI(t,03))*(TI(t,03));
end
```

```
                %25-35
                if FL(t,18)
                    BL(t,9) = 35.5 - (9/1800/1800)*(TI(t,04))*(TI(t,04))/3;
                    BL(t,10) = 33.5 -
(9.5/1800/1800)*(TI(t,04))*(TI(t,04));
                end

                %Split Bounds Up: 25-30 + 25-35
                if FL(t,16)&&not(FL(t,20))
                    BL(t,9) = 35.5 - (9/1800/1800)*(TI(t,04))*(TI(t,04))/3;
                    BL(t,10) = 28.5 - (4.5/240/240)*(TI(t,02))*(TI(t,02));
                end

                %35-30
                if FL(t,23)
                    BL(t,9) = 31.5 + (4/90/90)*(TI(t,05))*(TI(t,05));
                    BL(t,10) = 28.5 + (5/90/90)*(TI(t,06))*(TI(t,05))/3;
                end

                %30-25
                if FL(t,24)
                    BL(t,9) = 26.5 + (5/150/150)*(TI(t,06))*(TI(t,06));
                    BL(t,10) = 24 + (4.5/150/150)*(TI(t,06))*(TI(t,06))/3;
                end

                %35-25
                if FL(t,25)
                    BL(t,9) = 26.5 + (9/240/240)*(TI(t,07))*(TI(t,07));
                    BL(t,10) = 24 + (9.5/240/240)*(TI(t,07))*(TI(t,07))/3;
                end

                %Split Bounds Down: 35-30 + 35-25
                if FL(t,23)&&not(FL(t,20))
                    BL(t,9) = 31.5 + (4/90/90)*(TI(t,05))*(TI(t,05));
                    BL(t,10) = 24 + (9.5/240/240)*(TI(t,07))*(TI(t,07))/3;
                end


                %Test for settled C2
                FL(t,20) = FL(t,12) || FL(t,13) || FL(t,14) || FL(t,20);

%%%%%%%%%%%%%%%%%%%%%%%%%Stage 2%%%%%%%%%%%%%%%%%%%%%%%%
                %First visit?
                %25-35 if: C2 Settles on 35, previously 25-30
                FL(t,18) = (FL(t,14) && FL(t,16) && FL(t,20))||FL(t,18);
                if FL(t,18)
                    FL(t,16)=0;
                end
                %35-25 if: C2 Settles on 25, previously 35-30
                FL(t,25) = (FL(t,12) && FL(t,23) && FL(t,20))||FL(t,25);
                if FL(t,25)
                    FL(t,23)=0;
                end

                %Test for settled T2
```

```
                %Increment if within final bounds
                if (BL(t,2) < 26.5)&&(BL(t,2) > 24) && FL(t,12) &&FL(t,20)
                    CO(t,5)=CO(t-1,5)+1;
                end
                if (BL(t,2) < 31.5)&&(BL(t,2) > 28.5) && FL(t,13)
&&FL(t,20)
                    CO(t,5)=CO(t-1,5)+1;
                end
                if (BL(t,2) < 35.5)&&(BL(t,2) > 33.5) && FL(t,14)
&&FL(t,20)
                    CO(t,5)=CO(t-1,5)+1;
                end

                %Set Settled Flag if count higher than 50
                FL(t,29) = (CO(t,05) > 50) && FL(t,9) && FL(t,20);

                %Values at 25'C
                if FL(t,12) && FL(t,29)
                    BL(t,9)=26.5;
                    BL(t,10)=24;
                end

                %Values at 30'C
                if FL(t,13) && FL(t,29)
                    BL(t,9)=31.5;
                    BL(t,10)=28.5;
                end

                %Values at 35'C
                if FL(t,14) && FL(t,29)
                    BL(t,9)=35.5;
                    BL(t,10)=33.5;
                end
                break
            end

%%%%%%%%%%%%%%%%%%%%%%%%%Start of Level Transition%%%%%%%%%%%%%%%%%%%%%%%%%
            while 1==1
                if not(DO(t,15))
                    DO(t,15)=1;
                end

                %If Transition Down, go to level transition down
                if FL(t,10)

%%%%%%%%%%%%%%%%%%%%%%%%%Stage 1%%%%%%%%%%%%%%%%%%%%%%%%%

                    %If settled C2, flag stage 2
                    FL(t,22) = FL(t,12)||FL(t,13)||FL(t,14)||FL(t,22);
                    if FL(t,22)
                        FL(t,21)=0;
                    end

                    %Build new bounds:
                    %Give room for 10% Overshoot on up
```

```
                    %25-30
                    if FL(t,16)
                        BL(t,14) = 88;
                        if not(FL(t,22))
                            BL(t,15) = 60;
                        end
                    end
                    %30-35
                    if FL(t,17)
                        BL(t,14) = 94;
                        if not(FL(t,22))
                            BL(t,15) = 70;
                        end
                    end
                    %25-35
                    if FL(t,18)
                        BL(t,14) = 94;
                        if not(FL(t,22))
                            BL(t,15) = 60;
                        end
                    end

%%%%%%%%%%%%%%%%%%%%%%%%Stage 2%%%%%%%%%%%%%%%%%%%%%%%%
                    %Build new bounds

                    %25-30
                    if FL(t,16)&&FL(t,22)
                        BL(t,15) = (0070)-(10/300)*(TI(t,08));
                    end

                    %30-35
                    if FL(t,17)&&FL(t,22)
                        BL(t,15) = (0075)-(5/240)*(TI(t,09));
                    end

                    %25-35
                    if FL(t,18)&&FL(t,22)
                        BL(t,15) = (0075)-(15/420)*(TI(t,10));
                    end

                    %%Test for Settled L4
                    %Increment if within final bounds
                    %25-30
                    if (BL(t,5) > 70)&&(BL(t,5) <
80)&&FL(t,16)&&FL(t,22)%&&(TI(t,10)>(TI(t,8)/2))
                        CO(t,06)=CO(t,06)+1;
                    end
                    %30-35
                    if (BL(t,5) > 75)&&(BL(t,5) <
85)&&FL(t,17)&&FL(t,22)%&&(TI(t,10)>(TI(t,9)/2))
                        CO(t,06)=CO(t,06)+1;
                    end
                    %25-35
                    if (BL(t,5) > 75)&&(BL(t,5) <
85)&&FL(t,18)&&FL(t,22)%&&(TI(t,10)>(TI(t,10)/2))
                        CO(t,06)=CO(t,06)+1;
                    end
```

```
                %Set Flags if counter greater than 30
                FL(t,30) = CO(t,06) > 30;

                %%%Finished Stage
                %25'C Setpoint
                if FL(t,30)&&FL(t,12)
                    BL(t,14) = 75;
                    BL(t,15) = 60;
                end

                %30'C Setpoint
                if FL(t,30)&&FL(t,13)
                    BL(t,14) = 80;
                    BL(t,15) = 70;
                end

                %35'C Setpoint
                if FL(t,30)&&FL(t,14)
                    BL(t,14) = 85;
                    BL(t,15) = 75;
                end

                %Test that both are finished
                %Clear Spike Flags
                if FL(t,29)&&FL(t,30)
                    FL(t,9) = 0;
                    FL(t,10) = 0;
                    %Clear Stage Flags
                    FL(t,19) = 0;
                    FL(t,20) = 0;
                    FL(t,21) = 0;
                    FL(t,22) = 0;
                    %Clear Trans Type Flags
                    FL(t,16) = 0;
                    FL(t,17) = 0;
                    FL(t,18) = 0;
                    FL(t,23) = 0;
                    FL(t,24) = 0;
                    FL(t,25) = 0;
                    %Clear the settled counters
                    CO(t,5) = 0;
                    CO(t,6) = 0;
                    %CLear the settled flags
                    FL(t,29) = 0;
                    FL(t,30) = 0;

                end

                %Return to variable testing

            else

%%%%%%%%%%%%%%%%%%%%%%%%%%Level Transition Down%%%%%%%%%%%%%%%%%%%%%%%%%%
                if not(DO(t,16))
                    DO(t,16)=1;
                end
```

```
                    %X Down Flag, NOT Stage 2 Flag, NOT Finished Flag
                    %%%Stage 1
                    %If First visit
                    %Record current L4 and start timer
                    if not(FL(t,21))
                        BL(t,7)=BL(t,5);
                    end

                    %Flag stage 1
                    if not(FL(t,21))
                        FL(t,21)=1;
                    end

                    %If time has passed, test if a cross has happened, flag
stage 2 if yes
                    if not(FL(t,22)) %Timer keeps resetting until it is
used
                        TI(t,11) = 600.0;
                    end

                    %Test for start of stage 2
                    FL(t,22) = ((TI(t,12)==0)&&(BL(t,5) <
BL(t,7)))||FL(t,22);

                    %Build New Limits
                    %35-30
                    if FL(t,23)&&FL(t,21)
                        BL(t,14) = 93;
                        BL(t,15) = 75;
                    end

                    %30-25
                    if FL(t,24)&&FL(t,21)
                        BL(t,14) = 88;
                        BL(t,15) = 70;
                    end

                    %35-25
                    if FL(t,25)&&FL(t,21)
                        BL(t,14) = 93;
                        BL(t,15) = 75;
                    end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%Stage 2%%%%%%%%%%%%%%%%%%%%%%%%%

                    %%Test for Settled L4
                    %Increment if within final bounds
                    if (BL(t,5) > 60)&&(BL(t,5) < 75)&&FL(t,12)
                        CO(t,6)=CO(t,6)+1;
                    end
                    if (BL(t,5) > 70)&&(BL(t,5) < 80)&&FL(t,13)
                        CO(t,6)=CO(t,6)+1;
                    end
                    if (BL(t,5) > 75)&&(BL(t,5) < 85)&&FL(t,14)
                        CO(t,6)=CO(t,6)+1;
                    end
```

```
%Set Flags if counter greater than xx
FL(t,30) = CO(t,06) > 300;

%Build New Bounds, with 20% Undershoot
%35-30
if (FL(t,23)&&FL(t,22))
    BL(t,14) =  (80)+(5/600)*(TI(t,11));
    BL(t,15) =  63;
end

%30-25
if (FL(t,24)&&FL(t,22))
    BL(t,14) = (70)+(10/600)*(TI(t,11));
    BL(t,15) =  52;
end

%35-25
if (FL(t,25)&&FL(t,22))
    BL(t,14) = (70)+(15/600)*(TI(t,11));
    BL(t,15) =  52;
end

%If Finished With Transition
%25'C Setpoint
if FL(t,30)&&FL(t,12)
    BL(t,14) = 75;
    BL(t,15) = 60;
end

%30'C Setpoint
if FL(t,30)&&FL(t,13)
    BL(t,14) = 80;
    BL(t,15) = 70;
end

%35'C Setpoint
if FL(t,30)&&FL(t,14)
    BL(t,14) = 85;
    BL(t,15) = 75;
end

%Test that both are finished
%Clear Spike Flags
if FL(t,29)&&FL(t,30)
    FL(t,9) = 0;
    FL(t,10) = 0;
    %Clear Stage Flags
    FL(t,19) = 0;
    FL(t,20) = 0;
    FL(t,21) = 0;
    FL(t,22) = 0;
    %Clear Trans Type Flags
    FL(t,16) = 0;
    FL(t,17) = 0;
    FL(t,18) = 0;
    FL(t,23) = 0;
```

```
                        FL(t,24) = 0;
                        FL(t,25) = 0;
                        %Clear the settled counters
                        CO(t,5) = 0;
                        CO(t,6) = 0;
                        %Clear the settled flags
                        FL(t,29) = 0;
                        FL(t,30) = 0;
                    end

%%%%%%%%%%%%%%%%%%%%%%%%%Return to variable testing%%%%%%%%%%%%%%%%%%%%%%%%%

                end

                break
            end

            break
        end

        %Values at 25'C
        if FL(t,12)&&not(FL(t,9))
            BL(t,09)=26.5;%T2maX
            BL(t,10)=24;%T2miN
            BL(t,14)=75;%L4maX
            BL(t,15)=60;%L4miN
        end

        %Values at 30'C
        if FL(t,13)&&not(FL(t,9))
            BL(t,09)=31.5;%T2maX
            BL(t,10)=28.5;%T2miN
            BL(t,14)=80;%L4maX
            BL(t,15)=70;%L4miN
        end

        %Values at 35'C
        if FL(t,14)&&not(FL(t,9))
            BL(t,09)=35.5;%T2maX
            BL(t,10)=33.5;%T2miN
            BL(t,14)=85;%L4maX
            BL(t,15)=75;%L4miN
        end

        break
    end

%%%%%%%%%%%%%%%%%%%%%%%%%The test and break%%%%%%%%%%%%%%%%%%%%%%%%%
    while 1==1

        %First, all of the soft boundary counters
        %F1miN Soft
        if BL(t,6)<BL(t,16)
            CO(t,3)=CO(t,3)+1;
        else if BL(t,6)>BL(t,16)
                CO(t,3)=0;
```

```
            end
        end

         %P1maX Soft
        if BL(t,8)>BL(t,22)
            CO(t,10)=CO(t,10)+1;
        else if BL(t,8)<BL(t,22)
                CO(t,10)=0;
            end
        end

         %P1miN Soft
        if BL(t,8)<BL(t,23)
                CO(t,12)=CO(t,12)+1;
        else if BL(t,8)>BL(t,23)
                CO(t,11)=0;
            end
        end

        %L3maX Soft
        if BL(t,4)>BL(t,12)
                CO(t,13)=CO(t,13)+1;
        else if BL(t,4)<BL(t,12)
                CO(t,13)=0;
            end
        end

        %L3miN Soft
        if BL(t,4)<BL(t,13)
                CO(t,14)=CO(t,14)+1;
        else if BL(t,4)>BL(t,13)
                CO(t,14)=0;
            end
        end

        %Flagging for timed or absolute breaches
        FL(t,1)=BL(t,2)>BL(t,9); %T2maX
        FL(t,2)=BL(t,2)<BL(t,10); %T2miN
        FL(t,3)=BL(t,3)>BL(t,25); %P2maX
        FL(t,3)=BL(t,3)<BL(t,26); %P2miN
        FL(t,4)=CO(t,13)>3; %L3maX
        FL(t,5)=CO(t,14)>3; %L3miN
        FL(t,6)=BL(t,5)>BL(t,14); %L4maX
        FL(t,7)=BL(t,5)<BL(t,15); %L4miN
        FL(t,8)=CO(t,3)>3; %F1miN
        FL(t,27)=CO(t,10)>2; %P1maX
        FL(t,28)=CO(t,11)>3; %P1miN


DO(t,1)=FL(t,1)||FL(t,2)||FL(t,3)||FL(t,4)||FL(t,5)||FL(t,6)||FL(t,7)||FL(t
,8)||FL(t,27)||FL(t,28);
    break
    end
end

LevelTimer %Show how long the level transitions required
Diagnose %Display the states of flags for personal reference
```

```
TransitionTimer %Show how long the temperature transitions required
ShowTrips %Show which parameteres (if any) initiated the trip
```

Appendix B: HFC Code

This code has been discussed in detail in Section 4.3: Description of Implemented Monitoring Software. This appendix presents the actual coding as written to the HFC. For reference of what each memory item is used for, refer to Appendix C: HFC Items List

```
;;Start of program
;Initialize Inputs/Outputs
AIC(BL,1,50); Input 1=C2
AIC(BL,2,100); Input 2=T2
AIC(BL,3,100); Input 3=P2
AIC(BL,4,100); Input 4=L3
AIC(BL,5,100); Input 5=L4
AIC(BL,6,100); Input 6=F1
AIC(BL,8,100); Input 8=P1

;The Shutdown
DO,01 R= DO,01 ;

;Reset Flags
FL,01 R= /FL,01;
FL,02 R= /FL,02;
FL,03 R= /FL,03;
FL,04 R= /FL,04;
FL,05 R= /FL,05;
FL,06 R= /FL,06;
FL,07 R= /FL,07;
FL,08 R= /FL,08;
FL,09 R= /FL,09;
FL,10 R= /FL,10;
FL,11 R= /FL,11;
FL,12 R= /FL,12;
FL,13 R= /FL,13;
FL,14 R= /FL,14;
FL,15 R= /FL,15;
FL,16 R= /FL,16;
FL,17 R= /FL,17;
FL,18 R= /FL,18;
FL,19 R= /FL,19;
FL,20 R= /FL,20;
FL,21 R= /FL,21;
FL,22 R= /FL,22;
FL,23 R= /FL,23;
FL,24 R= /FL,24;
FL,25 R= /FL,25;
FL,26 R= /FL,26;
FL,27 R= /FL,27;
FL,28 R= /FL,28;
FL,29 R= /FL,29;
FL,30 R= /FL,30;

;The Limits (ie. 'G')
BL,9= VA,63;T2maX
BL,10= VA,57;T2miN
BL,11= VA,22;P2maX
BL,12= VA,51;L3maX
BL,13= VA,49;L3miN
BL,14= VA,80;L4maX
BL,15= VA,60;L4miN
BL,16= VA,55;F1miN
BL,22= VA,38;P1maX
BL,23= VA,29;P1miN
BL,17= BL,1;C2n-1
BL,18= VA,00;C2n-2
BL,19= VA,00;C2n-3
BL,20= VA,00;C2n-4
BL,21= VA,00;C2n-5

;Declare all counters
CO,01=VA,00 ;C2 Counter for Wandering
CO,02=VA,00 ;P2 Soft Trip Counter
CO,03=VA,00 ;F1 Soft Trip Counter
CO,04=VA,00 ;C2 Counter for Start Up
CO,05=VA,00 ;T2 Settled Counter
CO,06=VA,00 ;L4 Settled
CO,07=VA,00 ;25C Settle
CO,08=VA,00 ;30C Settle
CO,09=VA,00 ;35C Settle

;Preset all Timers
TISC,02 = VATP,240.0
TISC,03 = VATP,1500.0
TISC,04 = VATP,1800.0
TISC,05 = VATP,90.0
TISC,06 = VATP,150.0
TISC,07 = VATP,240.0
TISC,08 = VATP,300.0
TISC,09 = VATP,240.0
TISC,10 = VATP,420.0
TISC,11 = VATP,600.0
TISC,12 = VATP,30.0

;;;;;;;;;;;;;;;;;Wait for Start- Up;;;;;;;;;;;;;;;;;;;

;Start of Loop 1
L0001: DO,09 S= /DO,09

;Test for Start Up Count
JUMP L0002 IF CO,04 => VA,4800; approximating a 40Hz Refresh Rate

;If C2>25%, increase its counter, else set the count to 0
INC CO,04 IF BL,1 > BL,50

;Jump to trip if absolute bounds are tripped
```

```
JUMP L0011 IF ((BL,1 > VA,90) OR (BL,2 >BL,9))

;Return to top of loop
JUMP L0001

;;;;;;;;;;;;; Operations;;;;;;;;;;;;;;
;Start of Loop 2
L0002: DO,10 S= /DO,10

;;;Counter's Don't Go Below 0
CO,01 = VA,00 IF CO,01 < VA,00
CO,02 = VA,00 IF CO,02 < VA,00
CO,03 = VA,00 IF CO,03 < VA,00
CO,04 = VA,00 IF CO,04 < VA,00
CO,05 = VA,00 IF CO,05 < VA,00
CO,06 = VA,00 IF CO,06 < VA,00
CO,07 = VA,00 IF CO,07 < VA,00
CO,08 = VA,00 IF CO,08 < VA,00
CO,09 = VA,00 IF CO,09 < VA,00

;Nice Outsource to C2 Tracker
JUMP L0020
L0021: FL,31 S= /FL,31

;Outsource to Bounds Builder
JUMP L0006
L0012: FL,31 S= /FL,31

;Increment (or decrement) the soft bounds
INC CO,3 IF BL,6 < BL,16; F1<MIN
DEC CO,3 IF BL,6 > BL,16
INC CO,10 IF BL,8 > BL,22; P1>MAX
DEC CO,10 IF BL,8 < BL,22
INC CO,12 IF BL,8 < BL,23; P1<MIN
DEC CO,12 IF BL,8 > BL,23
INC CO,13 IF BL,4 < BL,12; L3>MAX
DEC CO,13 IF BL,4 > BL,12
INC CO,14 IF BL,4 < BL,13; L3<MIN
DEC CO,14 IF BL,4 > BL,13

;Check the formed bounds
FL,01=BL,02 > BL,09; T2>MAX
FL,02=BL,02 < BL,10; T2<MIN
FL,06=BL,05 > BL,14; L4>MAX
FL,07=BL,05 < BL,15; L4<MIN
FL,27=BL,03 > BL,25; P2>MAX
FL,28=BL,03 < BL,26; P2<MIN

;Check the Soft Bounds
FL,04= CO,13> VA,100; L3 COUNT MAX
FL,05= CO,14 > VA,100; L3 COUNT MIN
FL,08= CO,3 > V1,100; F1 COUNT MIN
FL,27= CO,10 > VA,70; P1 COUNT MAX
FL,28= CO,12 > VA,100; P1 COUNT MIN

;Trip under the extrardinary circumstances
JUMP L0011 IF FL,01 OR FL,02 OR FL,03 OR FL,04 OR FL,05 OR FL,06 OR FL,07 OR FL,08 OR FL,27 OR FL,28

;Back to the start of Operations Loop
JUMP L0002

;;;;;;;;;;;;C2 TRACKER;;;;;;;;;;;;;;;;;;;
;Do at least one hand me down
L0020: BL,21 = BL,20
BL,20 = BL,19
BL,19 = BL,18
BL,18 = BL,17
BL,17 = BL,1

;Determine spike direction
FL,10 R= (BL,17 > BL,1) AND /FL,9
FL,10 S= (BL,17 < BL,1) AND /FL,9

;Is there a jump?
FL,9 = ((BL,17 - VA,5) > BL,1) OR ((BL,17 + VA,5) < BL,1) OR FL,9

;Is there a drift?
FL,15 S= (BL,1 > VA,47) OR (BL,1 < VA,42) AND /FL,9 AND FL,12
FL,15 S= (BL,1 > VA,55) OR (BL,1 < VA,48) AND /FL,9 AND FL,13
FL,15 S= (BL,1 > VA,61) OR (BL,1 < VA,54) AND /FL,9 AND FL,14

;If drift, allow it only for 2s (Assuming 35Hz) (70 Samples)
;Do the increment/ decrement thing
INC CO,1 IF FL,15
DEC CO,1 IF /FL,15
JUMP L0011 IF CO,1 > VA,1=70

;While there is drift, ignore the settle reading
INC CO,7 IF (BL,17 > VA,42) AND (BL,17 < VA,47) AND (BL,18 > VA,42) AND (BL,18 < VA,47) AND (BL,19 > VA,42) AND (BL,19 < VA,47) AND (BL,20 > VA,42) AND (BL,20 < VA,47) AND (BL,21 > VA,42) AND (BL,21 < VA,47) AND /FL,15
CO,7 = CO,7 - VA,5 IF (BL,17 < VA,42) OR (BL,17 > VA,47) OR (BL,18 < VA,42) OR (BL,18 > VA,47) OR (BL,19 < VA,42) OR (BL,19 > VA,47) OR (BL,20 < VA,42) OR (BL,20 > VA,47) OR (BL,21 < VA,42) OR (BL,21 > VA,47) AND /FL,15

INC CO,8 IF (BL,17 > VA,48) AND (BL,17 < VA,55) AND (BL,18 > VA,48) AND (BL,18 < VA,55) AND (BL,19 > VA,48) AND (BL,19 < VA,55) AND (BL,20 > VA,48) AND (BL,20 <
```

```
VA,55) AND (BL,21 > VA,48) AND (BL,21 < VA,55) AND /FL,15
CO,8 = CO,8 - VA,5 IF (BL,17 < VA,48) OR (BL,17 > VA,55) OR (BL,18 < VA,48) OR (BL,18 > VA,55) OR (BL,19 < VA,48) OR (BL,19 > VA,55) OR (BL,20 < VA,48) OR (BL,20 > VA,55) OR (BL,21 < VA,48) OR (BL,21 > VA,55) AND /FL,15

INC CO,9 IF (BL,17 > VA,54) AND (BL,17 < VA,61) AND (BL,18 > VA,54) AND (BL,18 < VA,61) AND (BL,19 > VA,54) AND (BL,19 < VA,61)AND (BL,20 > VA,54) AND (BL,20 < VA,61)AND (BL,21 > VA,54) AND (BL,21 < VA,61) AND /FL,15
CO,9 = CO,9 - VA,5  IF (BL,17 < VA,54) OR (BL,17 > VA,61) OR (BL,18 < VA,54) OR (BL,18 > VA,61) OR (BL,19 < VA,54) OR (BL,19 > VA,61) OR (BL,20 < VA,54) OR (BL,20 > VA,61) OR (BL,21 < VA,54) OR (BL,21 > VA,61) AND /FL,15

;Declare the settle point
FL,12 = CO,7 > VA,120
FL,13 = CO,8 > VA,120
FL,14 = CO,9 > VA,120
FL,15 R= /FL,15

;Don't let the counters get too high
CO,7 = VA,180 IF CO,7 > VA,180
CO,8 = VA,180 IF CO,8 > VA,180
CO,9 = VA,180 IF CO,9 > VA,180

;Return from the subroutine
JUMP L0021

;;;;;;;;;;;;;;;BOUNDARIES;;;;;;;;;;;;;;;;;;;
;Start of Loop 6
;The Non-Transitive Limits
L0006: BL,25= VA,23;P2maX
BL,26=VA,13;P2miN
BL,12= VA,51;L3maX
BL,13= VA,49;L3miN
BL,16= VA,57;F1miN
BL,22= VA,42;P1maX
BL,23= VA,29;P1miN

;Check for Spike Flag. If active, jump to HeatX
JUMP L0003 IF FL,09

;Values at 25'C
BL,09=VA,53 IF FL,12;T2maX
BL,10=VA,48 IF FL,12;T2miN
BL,14=VA,75 IF FL,12;L4maX
BL,15=VA,60 IF FL,12;L4miN

;Values at 30'C
BL,09=VA,63 IF FL,13;T2maX
BL,10=VA,57 IF FL,13;T2miN
BL,14=VA,80 IF FL,13;L4maX
BL,15=VA,70 IF FL,13;L4miN

;Values at 35'C
BL,09=VA,71 IF FL,14;T2maX
BL,10=VA,67 IF FL,14;T2miN
BL,14=VA,85 IF FL,14;L4maX
BL,15=VA,75 IF FL,14;L4miN

;Return to operations
JUMP L0012

;;;;;;;Heat Stage 1;;;;;;;;;;;;;;;
;Receive the jump
L0003: FL,31 S= /FL,31

;First Visit? Make a preliminary direction flag
;;25-30 if: Up, @25
FL,16 = FL,10 AND FL,12 AND /FL,19
;30-35 if: Up, @30
FL,17 = FL,10 AND FL,13 AND /FL,19
;35-30 if: Down, @35
FL,23 = /FL,10 AND FL,14 AND /FL,19
;30-25 if: Down, @30
FL,24 = /FL,10 AND FL,13 AND /FL,19
;Trip if up at 35, or down at 25
JUMP L0011 IF ((FL,10 AND FL,14) OR (/FL,10 AND FL,12)) AND /FL,19

;Set all timers that apply
TISC,02 = VATP,240.0 IF (FL,16 AND /FL,19) ;T2 25-30
TISC,03 = VATP,1500.0 IF (FL,17 AND /FL,19) ;T2 30-35
TISC,04 = VATP,1800.0 IF (FL,18 OR Fl,16 AND /FL,19) ;T2 25-35
TISC,05 = VATP,90.0 IF (FL,23 AND /FL,19) ;T2 35-30
TISC,06 = VATP,150.0 IF (FL,24 AND /FL,19) ;T2 30-25
TISC,07 = VATP,240.0 IF (FL,25 OR FL,23 AND /FL,19) ;T2 35-25
TISC,08 = VATP,300.0 IF (FL,16 AND /FL,19) ;L4 25-30
TISC,09 = VATP,240.0 IF (FL,17 AND /FL,19) ;L4 30-35
TISC,10 = VATP,420.0 IF ((FL,18 OR FL,16) AND /FL,19) ;L4 25-35
TISC,12 = VATP,300.0 IF (/FL,10 AND /FL,19)

;Set the stage flags
FL,12 R= /FL,19
FL,13 R= /FL,19
FL,14 R= /FL,19
FL,22 R= /FL,19
```

```
CO,7 = VA,00 IF /FL,19
CO,8 = VA,00 IF /FL,19
CO,9 = VA,00 IF /FL,19
FL,19 S= /FL,19

;Build the new bounds
;Up Bounds
;25-30
BL,9 = VA,0063 -
(VA,0010/VA,2400/VA,2400)*(VA,2400-
TI,02)*(VA,2400-TI,03)*VA,7/VA,2 IF FL,16
BL,10 = VA,0057 -
(VA,0009/VA,2400/VA,2400)*(VA,2400-
TI,02)*(VA,2400-TI,03) IF FL,16

;30-35
BL,9 = VA,0071 -
(VA,0008/VA,15000/VA,15000)*(VA,15000-
TI,03)*(VA,15000-TI,03)*VA,7/VA,2 IF FL,17
BL,10 = VA,0067 -
(VA,0010/VA,15000/VA,15000)*(VA,15000-
TI,03)*(VA,15000-TI,03) IF FL,17

;25-35
BL,9 = VA,0071 -
(VA,0018/VA,18000/VA,18000)*(VA,18000-
TI,04)*(VA,18000-TI,04)*VA,7/VA,2 IF FL,18
BL,10 = VA,0067 -
(VA,0019/VA,18000/VA,18000)*(VA,18000-
TI,04)*(VA,18000-TI,04) IF FL,18

;Split Bounds Up
BL,9 = VA,0071 -
(VA,0018/VA,18000/VA,18000)*(VA,18000-
TI,04)*(VA,18000-TI,04)*VA,7/VA,2 IF FL,16
AND /FL,20
BL,10 = VA,0067 -
(VA,0010/VA,15000/VA,15000)*(VA,15000-
TI,03)*(VA,15000-TI,03) IF FL,16 AND /FL,20

;Down Bounds
;35-30
BL,9 = VA,0063 +
(VA,0008/VA,0900/VA,0900)*(VA,0900-
TI,05)*(VA,0900-TI,05) IF FL,23
BL,10 = VA,0057 +
(VA,0010/VA,0900/VA,0900)*(VA,0900-
TI,05)*(VA,0900-TI,05)*VA,7/VA,2 IF FL,23

;30-25
BL,9 = VA,0053 +
(VA,0010/VA,1500/VA,1500)*(VA,1500-
TI,06)*(VA,1500-TI,06) IF FL,24
BL,10 = VA,0048 +
(VA,0009/VA,1500/VA,1500)*(VA,1500-
TI,06)*(VA,1500-TI,06)*VA,7/VA,2 IF FL,24

;35-25
BL,9 = VA,0053 +
(VA,0018/VA,2400/VA,2400)*(VA,2400-
TI,07)*(VA,2400-TI,07) IF FL,25
BL,10 = VA,0048 +
(VA,0019/VA,2400/VA,2400)*(VA,2400-
TI,07)*(VA,2400-TI,07)*VA,7/VA,2 IF FL,25

;Split Bounds Down
BL,9 = VA,0063 +
(VA,0008/VA,0900/VA,0900)*(VA,0900-
TI,05)*(VA,0900-TI,05) IF FL,23 AND /FL,20
BL,10 = VA,0048 +
(VA,0019/VA,2400/VA,2400)*(VA,2400-
TI,07)*(VA,2400-TI,07)*VA,7/VA,2 IF FL,23
AND /FL,20

;Test for settled C2
FL,20 S= FL,12 OR FL,13 OR FL,14

;;;;;;;;;;;;;;;;;;Heat Stage 2;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;If first visit, check for innaccurately chosen steps
;25-35 if: C2 Settles on 35, previously 25-30
FL,18 S= FL,12 AND FL,16 AND FL,20
FL,16 R= FL,18
;35-25 if: C2 Settles on 25, previously 35-30
FL,25 S= FL,14 AND FL,23 AND FL,20
FL,23 R= FL,25

;Test for settled T2
;Increment if within final bounds
INC CO,05 IF (BL,2 < VA,52) AND (BL,2 >
VA,49) AND FL,12
INC CO,05 IF (BL,2 < VA,62) AND (BL,2 >
VA,58) AND FL,13
INC CO,05 IF (BL,2 < VA,70) AND (BL,2 >
VA,68) AND FL,14
;Decrement if within final bounds
DEC CO,05 IF ((BL,2 > VA,52) OR (BL,2 <
VA,49)) AND FL,12
DEC CO,05 IF ((BL,2 > VA,62) OR (BL,2 <
VA,58)) AND FL,13
DEC CO,05 IF ((BL,2 > VA,70) OR (BL,2 <
VA,68)) AND FL,14

;Set Settled flag if count is greater than xx
FL,29 = (CO,05 > VA,400) AND FL,9 AND FL,20

;Static bounds if settled
;Values at 25'C
BL,09=VA,53 IF FL,12 AND FL,29;T2maX
BL,10=VA,48 IF FL,12 AND FL,29;T2miN

;Values at 30'C
BL,09=VA,63 IF FL,13 AND FL,29;T2maX
BL,10=VA,57 IF FL,13 AND FL,29;T2miN
```

```
;Values at 35'C
BL,09=VA,71 IF FL,14 AND FL,29;T2maX
BL,10=VA,67 IF FL,14 AND FL,29;T2miN

;Continue to level transition

;;;;;;;;;;;;;;;;;;Level Up;;;;;;;;;;;;;;;;;;;;;;;;;;
;Jump to Level Down if it is a down spike
JUMP L0004 IF /FL,10

;Check for the settled current
FL,22 S= FL,12 OR FL,13 OR FL,14

;Build new bounds
;25-30
BL,14 = VA,88 IF FL,16
BL,15 = VA,60 IF FL,16 AND /FL,22

;30-35
BL,14 = VA,94 IF FL,17
BL,15 = VA,70 IF FL,17 AND /FL,22

;25-35
BL,14 = VA,98 IF FL,18
BL,15 = VA,70 IF FL,18 AND /FL,22

;;;;Stage 2 for Level Up
;Do the timing bounds
;25-30
BL,15 = (VA,0070)-(VA,0010/VA,3000);*(VA,3000-TITM,08) IF (FL,16 AND FL,22)

;30-35
BL,15 = (VA,0075)-(VA,0005/VA,2400)*(VA,2400-TITM,08) IF (FL,17 AND FL,22)

;25-35
BL,15 = (VA,0075)-(VA,0015/VA,3000)*(VA,4200-TITM,08) IF (FL,18 AND FL,22)

;Test for Settled L4
INC CO,06 IF ((BL,5 > VA,60) AND (BL,5 < VA,75) AND FL,12 AND FL,22)
INC CO,06 IF ((BL,5 > VA,70) AND (BL,5 < VA,80) AND FL,13 AND FL,22)
INC CO,06 IF ((BL,5 > VA,75) AND (BL,5 < VA,85) AND FL,14 AND FL,22)

;Set flag if counter higher than 600 (30s)
FL,30 = CO,06 > VA,600

;Static Bounds
;25'C Setpoint
BL,14 = VA,75 IF FL,30 AND FL,12
BL,15 = VA,60 IF FL,30 AND FL,12

;30'C Setpoint
BL,14 = VA,80 IF FL,30 AND FL,13
BL,15 = VA,70 IF FL,30 AND FL,13

;35'C Setpoint
BL,14 = VA,85 IF FL,30 AND FL,14
BL,15 = VA,75 IF FL,30 AND FL,14

;If both are done with, do a total reset of flags and timers
FL,9 R= FL,29 AND FL,30
FL,10 R= FL,29 AND FL,30
;Clear stage flags
FL,19 R= FL,29 AND FL,30
FL,20 R= FL,29 AND FL,30
FL,21 R= FL,29 AND FL,30
FL,22 R= FL,29 AND FL,30
;Clear Trans Type Flags
FL,16 R= FL,29 AND FL,30
FL,17 R= FL,29 AND FL,30
FL,18 R= FL,29 AND FL,30
FL,23 R= FL,29 AND FL,30
FL,24 R= FL,29 AND FL,30
FL,25 R= FL,29 AND FL,30
;Clear Settle Counters
CO,5 = VA,00 IF FL,29 AND FL,30
CO,6 = VA,00 IF FL,29 AND FL,30

;Jump out if the settling hasn't happened
JUMP L0012 IF /FL,29 OR /FL,30

;Else, reset these too
FL,29 R= FL,29
FL,30 R= FL,30

;Return to Operations
JUMP L0012

;;;;;;;;;;;;;;;;;;Level Down 1;;;;;;;;;;;;;;;;;;;;;
;Receive jump from level up
L0004: FL,31 S= /FL,31

;If the first visit
;Record the current L4 and start timer
BL,7 = BL,5 IF /FL,21

;Set stage 1 flag
FL,21 S= /FL,21

;If time has passed, test if a cross has happened, flag stage 2
TISC,11 = VATP,600.0 IF /FL,22
FL,22 S= (TITO,12 AND (BL,5 < BL,7))

;Build the new limits
```

```
;35-30
BL,14 = VA,95 IF FL,23 AND FL,21
BL,15 =  VA,75 IF FL,23 AND FL,21

;30-25
BL,14 = VA,95 IF FL,24 AND FL,21
BL,15 =  VA,70 IF FL,24 AND FL,21

;35-25
BL,14 = VA,95 IF FL,25 AND FL,21
BL,15 =  VA,75 IF FL,25 AND FL,21

;;;;;;;;;;;;;;;;Level Down 2;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

;Test for settled L4
INC CO,06 IF ((BL,5 > VA,60) AND (BL,5 < VA,75) AND FL,12 AND  FL,22)
INC CO,06 IF ((BL,5 > VA,70) AND (BL,5 < VA,80) AND FL,13 AND  FL,22)
INC CO,06 IF ((BL,5 > VA,75) AND (BL,5 < VA,85) AND FL,14 AND  FL,22)

;Set finished flag if counter greater than 10500 (5 minutes and 35Hz)
FL,30 = CO,6 > VA,10500

;Build new bounds, accounting for undershoot
;35-30
BL,14 = (VA,80)+(VA,0005/VA,6000)*(VA,6000-TITM,11) IF (FL,23 AND FL,22)
BL,15 =  VA,55 IF (FL,23 AND FL,30)

;30-25
BL,14 = (VA,70)+(VA,0010/VA,6000)*(VA,6000-TITM,11) IF (FL,24 AND FL,22)
BL,15 =  VA,45 IF (FL,24 AND FL,30)

;35-25
BL,14 = (VA,70)+(VA,0015/VA,6000)*(VA,6000-TITM,11) IF (FL,25 AND FL,22)
BL,15 =  VA,45 IF (FL,25 AND FL,30)

;Static Bounds
;25'C Setpoint
BL,14 = VA,75 IF FL,30 AND FL,12
BL,15 = VA,60 IF FL,30 AND FL,12

;30'C Setpoint
BL,14 = VA,80 IF FL,30 AND FL,13
BL,15 = VA,70 IF FL,30 AND FL,13

;35'C Setpoint
BL,14 = VA,85 IF FL,30 AND FL,14
BL,15 = VA,75 IF FL,30 AND FL,14

;If both are done with, do a total reset of flags and timers
FL,9 R= FL,29 AND FL,30
FL,10 R= FL,29 AND FL,30
;Clear stage flags
FL,19 R= FL,29 AND FL,30
FL,20 R= FL,29 AND FL,30
FL,21 R= FL,29 AND FL,30
FL,22 R= FL,29 AND FL,30
;Clear Trans Type Flags
FL,16 R= FL,29 AND FL,30
FL,17 R= FL,29 AND FL,30
FL,18 R= FL,29 AND FL,30
FL,23 R= FL,29 AND FL,30
FL,24 R= FL,29 AND FL,30
FL,25 R= FL,29 AND FL,30
;Clear Settle Counters
CO,5 = VA,00 IF FL,29 AND FL,30
CO,6 = VA,00 IF FL,29 AND FL,30

;Jump out if the settling hasn't happened
JUMP L0012 IF /FL,29 OR /FL,30

;Else, reset these too
FL,29 R= FL,29
FL,30 R= FL,30

;Return to Operations
JUMP L0012

;;;;;;;;;;;;;Tripped Loop;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;Start of Loop 11
L0011: DO,01 S= /DO,01;

;Display Error
DO,09= FL,01;
DO,10= FL,02;
DO,11= FL,03;
DO,12= FL,04;
DO,13= FL,05;
DO,14= FL,06;
DO,15= FL,07;
DO,16= FL,08;
JUMP L0011
```

Appendix C: HFC Items List

BLOCK	ITEM
1	C2
2	T2
3	P2
4	L3
5	L4
6	F1
7	L4 X Start
8	P1
9	T2 Max
10	T2 Min
11	--
12	L3 Max
13	L3 Min
14	L4 Max
15	L4 Min
16	F1 Min
17	C2 n-1
18	C2 n-2
19	C2 n-3
20	C2 n-4
21	C2 n-5
22	P1 Max
23	P1 Min
24	Holding
25	P2 Max
26	P2 Min

FLAG	ITEM
5	L3 Min
6	L4 Max
7	L4 Min
8	F1 Min
9	Spike
10	Spike Up
11	L4 Trans
12	Set point 25
13	Set point 30
14	Set point 35
15	C2 Drifting
16	X 25->30
17	X 30->35
18	X 25->35
19	X Stage 1 (Heat)
20	X Stage 2 (Heat)
21	X Stage 1 (Level)
22	X Stage 2 (Level)
23	X 35->30
24	X 30->25
25	X 35->25
27	P1 Max
28	P1 Min
29	T2 Settled
30	L4 Settled
31	Loop Catch

FLAG	ITEM
1	T2 Max
2	T2 Min
3	P2 Max
4	L3 Max

COUNT	ITEM
1	C2 Wander
2	--
3	F1 Soft Down
4	C2 Start Up

COUNT	ITEM
5	T2 Settled
6	L4 Settled
7	25'C Settle
8	30'C Settle
9	35'C Settle
10	P1 Soft Up
11	---
12	P1 Soft Down
13	L3 Soft Up
14	L3 Soft Down

TIMER	ITEM	Default Time
10	L4 Trans 25->35	420
11	L4 Trans Down	600
12	L4 Rebound Wait	300

LOOP	ITEM
0	Initialization
1	Start Up
2	Operations
3	Heat Transition
4	L4 Transition Down
6	Bounds Builder
11	Trip
12	Return from Bounds
19	Bypass C2 because of drift
20	C2 Tracker routine
21	Return from C2 Tracker

TIMER	ITEM	Default Time
1	---	
2	T2 Trans 25->30	240
3	T2 Trans 30->35	1500
4	T2 Trans 25->35	1800
5	T2 Trans 35->30	90
6	T2 Trans 30->25	150
7	T2 Trans 35->25	240
8	L4 Trans 25->30	300
9	L4 Trans 30->35	240

Curriculum Vitae

Name:	Michael V. Gverzdys
Post-secondary Education and Degrees:	University of Western Ontario London, Ontario, Canada 2008-2013, B.Sc. University of Western Ontario London, Ontario, Canada 2008-2013, B.E.Sc. University of Western Ontario London, Ontario, Canada 2013-2015, M.E.Sc.
Honours and Awards:	NSERC I-USRA Summer 2012
Related Work Experience:	Teaching Assistant The University of Western Ontario 2013-2015 Undergraduate Researcher NSERC I-USRA Program Summer 2012 Engineering Co-Op Exxon Mobil Summer 2011
Publications:	M. Gverzdys, J Jiang, T. Schaefer, S. Yang. "Design, Implementation, and Experimentation of a Reactor Shutdown System using HFC6000." *Proc. NPIC-HMIT,* 2015.