Title
Model Network Methodology for Experimental Development of Industrial Monitoring Systems

Author
Poresky, Christopher Morris

Publication Date
2019

Peer reviewed|Thesis/dissertation

Model Network Methodology for Experimental Development of Industrial Monitoring Systems

by

Christopher Poresky

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Nuclear Engineering

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Per F. Peterson, Chair
Assistant Professor Max Fratoni
Assistant Professor Scott Moura
Dr. Ronald Laurids Boring

Summer 2019

Model Network Methodology for Experimental Development of Industrial Monitoring Systems

Abstract

Model Network Methodology for Experimental Development of Industrial Monitoring Systems

by

Christopher Poresky

Doctor of Philosophy in Nuclear Engineering

University of California, Berkeley

Professor Per F. Peterson, Chair

Industrial systems enable modern life. They benefit tremendously by adapting digital communication technologies and leveraging automation algorithms and data availability. Their importance to basic human needs such as electricity, heating, food, transportation, clothing, and more also means that their constant availability and reliability is imperative in modern societies. Plant monitoring strategies that can collect information and use it to analyze and understand plant behavior is a key technology for optimizing industrial systems. Enabling plant monitoring insights to be communicated to human operators is essential to ensure the information can be used. While data-based methods continue to find new applications, model-based methods that incorporate unique plant characteristics and industry-specific considerations alone have the dual benefits of explainability and extrapolability. By developing plant monitoring systems that enable operators to understand plant state, quickly identify developing faults, and mitigate issues before they cause harm, designers can radically improve industrial system operations and management. Through thoughtful human-centered design of the interfaces between human and machine, they can elevate the role of industrial operators to orchestrate the plant monitoring system's set of autonomous routines.

This dissertation presents a methodology for the systematic design and implementation of a plant monitoring and operator support system running a fault diagnostic and decision support engine that can be adapted for a variety of industrial monitoring applications. It then demonstrates, by proof-of-concept application to an experimental thermal-hydraulic facility - the Compact Integral Effects Test (CIET) - and advanced control room testbed - the Advanced Reactor Control and Operations (ARCO) facility - the iterative plant monitoring system development process. The focus of this dissertation is the advanced nuclear power industry and the Fluoride salt-cooled High-temperature Reactor (FHR).

This dissertation is organized into eight sections. The first section introduces the background and motivation for model-based industrial monitoring systems before the second section provides an overview of the state-of-the-art for nuclear and other industry plant

monitoring systems before focusing on nuclear industry challenges and opportunities. The third section details the iterative fault diagnostic system development methodology and the fourth section describes one approach to decision support and fault mitigation algorithm design. These sections also walk the reader through an example application. The fifth section then introduces the ARCO-CIET facility used in the case study and the sixth section describes the operator support and human-machine interface design for ARCO. Finally, the seventh section presents the case study plant monitoring system design and results before the eighth section discusses promising applications of the overall design methodology.

This dissertation presents a methodology with the potential to guide the plant monitoring system development process across a variety of industries with the following original contributions: a methodology for iterative fault diagnostic system development using interdisciplinary information, recommendations for choosing plant models to build context between different monitoring objectives, a methodology for developing decision support routines, and guiding principles for plant monitoring system human-machine interface design and implementation in modern industrial control rooms.

To Mom and Dad,

Thank you for teaching me to be curious, to let my mind wander, to take nothing for granted, to challenge common knowledge, to be creative, to solve problems, to help others, and to do these things very stubbornly.

Contents

List of Figures

List of Tables

Acknowledgments

This dissertation ties together a variety of concepts and strategies from different disciplines. Fittingly, it results from the combined efforts of many wonderful people so that I can just barely claim it as my own. While the true number of contributors likely exceeds what I might record here, I will do my best to thank those who have made it possible.

Thank you to my close friends and fellow researchers outside of my lab: **Milos Atz**, **Joey Kabel**, **Sami Lewis**, and **Josh Rehak**. From the beginning, we have been in this together.

Prof. Peterson's Thermal-Hydraulics Laboratory is not just a windowless room with "sky"-blue walls where I go to stare at a computer screen. It is a place where I have developed bonds with friend after friend, where we debate back and forth modeling equations and coffee brewing techniques alike. We solve all problems as a team and I can think of no better team than the TH crew. Thank you to **Clara Alivisatos**, **Omar Alzaabi**, **Shane Gallagher**, **Ishak Johnson**, **James Kendrick**, **Theo Ong**, and **Dane de Wet** as well as honorary TH Lab grad students **Grey Batie** and **Vanessa Goss**. You are all brilliant and I owe some of my intelligence to osmosis. The best postdoc mentor award also goes to **Charalampos "Harry" Andreades** — both for research and for life advice.

The undergraduate students whom I've had the privilege to work with have inspired me through their enthusiasm. **Sala Tiemann** is my right-hand yeeter (is that how it works?) and contributed significantly to ARCO implementation and experimentation work. **Ian Kolaja** put together computer-based procedures and pseudo-analog shutdown controls with amazing speed and efficiency. **Eddie Bird** helped me to prototype fault detection algorithms and **Laura Shi** challenged me on the details of my work's explanations.

I've been lucky to have multiple faculty mentors throughout my time at Berkeley. **Max Fratoni**, whose office is right across the hall from the TH lab, never turned me away and welcomed me with warmth and wisdom from the first day I spoke with him. **Scott Moura's** course was invaluable but his excitement about energy systems and his contributions to literature permeate this work. I also owe my thanks to **Peter Hosemann** and **Rachel Slaybaugh**.

Thanks to the Nuclear Energy University Program, I interned at Idaho National Laboratory in Summer 2017 and gained a mentor in **R o n Boring**. Thank you, Ron, for your warm and personal style and for giving my work a human touch. Thanks also to **Roger Lew** and **Tom Ulrich**.

Thank you to my adviser, **Per Peterson**, for endlessly teaching, inspiring, and motivating me to contribute to the development of this necessary technology. You make me believe that it's possible and worth fighting for. You do the same for my ideas and I can never thank you enough for pushing me to keep my own promises.

Thank you to my friends for calling me and making me check in. Thank you to my family for always providing me perspective. Thank you to **Cullin** for providing likely the toughest peer review of my ability to explain myself.

Most importantly, thank you **Gabrielle Antoninni Caparimo**, the love of my life and, as of quite recently, my fiancée. Nobody has been more vital to this dissertation than you. Thank you for always pushing me, for always putting up with me (okay, maybe not always), and for always helping me be better. Thank you for giving so much.

Chapter 1

Introduction

1.1 Background and motivation

Today, automated and integrated processes provide essential services with greater efficiency, lower environmental impact, and reduced labor compared to the historical technologies they are replacing, including electricity, heating, food, clothing, and more. With modern round-the-clock supply and demand, interruptions to operation have substantial consequences. It is imperative to prevent these systems from failing and to keep them operating as efficiently as possible. Industrial monitoring systems can enable plant operators to anticipate problems, solve them before they become severe, and ensure safe and reliable operation. The most powerful monitoring systems incorporate the unique plant characteristics in their own design. This dissertation describes a methodology for using a network of system models to develop industrial monitoring systems alongside plant experimental development. While the implications of this work are broad, the specific application focus is on nuclear energy. But first, this dissertation will review broadly the opportunities for industrial monitoring lying in modern technological innovations.

Industry 4.0 Modern industrial processes grow increasingly complex and powerful with each new innovation. Industrial revolutions have come in multiple waves: the first via mechanization, the second via electrification, and the third via automation. The German government has heralded the fourth industrial revolution or Industry 4.0 — the infusion of data and machine learning into systems to make them smarter — and even autonomous [1].

Factors that have shaped industry's trajectory include demands for shorter development times, flexibility, resource efficiency, increased automation, and miniaturization [1]. Internet connectivity and data communication now permeates physical objects. Cyber-physical systems are commonplace. With connectivity comes a greater information variety and availability. We can gain powerful insights just by documenting and analyzing this new information abundance.

Information collection and distillation is only the first step. Researchers seek to solve

complex problems associated with healthcare, psychology, transportation, and more using the same principles that map clothing preferences to online behavior. Many industries, however, have not focused on the digital world and do not have the in-house expertise to develop their own tailored solutions. Most industries still stand to benefit from information-based efficiency gains but industrial systems have more technological inertia than consumer products. While some companies are actively developing domain-specific solutions to industrial problems through data science, there is increasing interest among industrial companies to cultivate expertise in-house. As data science grows in ubiquity, many professions are adopting it as a supplemental tool rather than a specialty. The most exciting solutions today are those that combine domain-specific expertise and insight with efficient and adaptable information management. How will we change our physical world and imbue industrial processes with communication-based "smartness"? What will long-established industries gain and how will they transform when every component can record and communicate with each other? How will the roles of humans evolve as systems can make decisions and adapt to new situations without supervision? Finally, we see the emergence and opportunity of Industry 4.0.

Automation and autonomy Most industrial processes incorporate some degree of automation. In currently-operating Generation II nuclear power plants in the United States, operators actuate mechanical systems by specifying their objective, e.g. by entering a desired level of movement for a component rather than directly controlling the force needed to obtain the movement. Automation is the operation of a predetermined routine without need for human intervention. Autonomous operation involves logic and decision-making in a simulation of intelligence. There is great economic potential in automating industrial processes to reduce operations costs. The incentives for autonomous operation are more diverse.

For the set of industrial processes in which human operators oversee and guide the system (the "plant"), we can define the operator as the manager of a plant's many automation routines. As the level of automation increases, the operator specifies control objectives in ways that are closer to the plant's overall purposes. As internal decision-making processes select between alternative automation routines to accomplish the operator's goal, the level of automation approximates autonomy. Autonomous operation would enable the plant to continuously adapt to conditions and meet objectives without operator intervention.

For many industries, this level of autonomous operation is not yet feasible. Human operators still sit at the fronts of most trains, in drivers' seats, in passenger airplane cockpits, in construction equipment, and in control rooms for chemical and power plants. We retain human operators even when their role is purely supervisory [2–4]. It is unlikely to be feasible or desirable to achieve full autonomy for all industrial processes, so we should not approach automation without designing for the human operators who supervise and use these processes. This dissertation will assert that the optimal partnership between human and machine can, with our current technological capabilities, exceed the value of either alone. The following sections will briefly detail some of the modern approaches to plant monitoring and the

existing challenges that they might address. The focus will be on the nuclear industry.

Focus on advanced nuclear energy Many industries stand to benefit from communication and data-enabled autonomous operation. Perhaps none has the potential to make both a larger singular leap and to more positively alter the world, however, than the nuclear industry. Among the myriad problems facing modern society, few bear so heavily on everything from public health to economic prosperity to productive development as does access to clean, reliable energy [5–8]. Due to its unparalleled energy density, minimal consumption of resources, and relative independence from environmental factors, nuclear energy represents one of the most significant tools we as a civilization have to mitigate both short- and long-term effects from energy-based pollution [9–11].

The imperative for adapting the nuclear industry to the modern age is twofold. First, we must give currently-operating reactors what they need to continue operating safely and reliably until the end of their operating lifetimes. Second, we must deploy a new generation of nuclear power plants that can optimize technological developments from the last half-century and operate in a variety of new ways. New capabilities, from variable generation to auxiliary services enabling deep decarbonization of our economy (e.g. energy storage, process heat production, and co-generation applications like alternative fuel production) support advanced nuclear energy as a unique and powerful asset.

Problem statement Revolutionizing industrial operations monitoring with modern data communication and autonomy will yield economic, reliability, and quality improvements for plants and the public. Researchers have developed myriad approaches to plant operations monitoring and fault mitigation but the existing set of approaches lacks cohesion, application flexibility, and human-system integration.

Research objective The objective of the research presented in this dissertation is to present and illustrate the application of a methodology for the systematic design and implementation of a fault diagnostic and mitigation engine via an operator support system that can be adapted for a variety of industrial monitoring applications.

Original contributions Many researchers have contributed to a rich and dense body of work on the subjects of fault diagnostics, industrial control systems, and human-machine interface design. This dissertation offers the following original contributions, in order of appearance:

- A methodology for an iterative fault diagnostic system development process that draws on the interdisciplinary expertise of an industrial system's design team
- Recommendations on fault diagnostic system model selection to build context between disparate objectives

- A methodology for a fault mitigation algorithm development process that supports plant autonomy through decision-making and self-correction
- Guiding principles for plant monitoring system human-machine interface implementation in modern industrial control rooms

To prove these contributions via application, this dissertation will present a proof-of-concept implementation in the ARCO-CIET (Advanced Reactor Control and Operations - Compact Integral Effects Test) facility at Berkeley. ARCO-CIET is a testbed to study the design and operation of a prototypical Fluoride-salt-cooled High-temperature Reactor (FHR). This dissertation will discuss ARCO-CIET and FHRs in Chapter 5.

Organization of this dissertation This dissertation leads the reader methodically, from idea to reality, starting with an overview of existing approaches and culminating with results from the approach described here.

- Chapter 2 briefly reviews the state-of-the-art for nuclear and other industry plant monitoring systems, broken up into system modeling, fault diagnostics and prognostics, and fault mitigation. It then focuses in on specific challenges and opportunities in the nuclear industry.
- Chapter 3 describes a methodology for building a fault diagnostic system and iteratively testing and improving it to obtain robust fault characterization signals. This chapter also provides a simple reference example.
- Chapter 4 describes a methodology for supporting operator decision-making through control planning and fault mitigation routines for the set of faults given by the diagnostic system. This chapter also considers disparate objectives for fault mitigation. This chapter applies the methodology to the example from Chapter 3.
- Chapter 5 briefly introduces the test facility, ARCO-CIET, that serves as the case study application.
- Chapter 6 describes the operator support system implementation for ARCO-CIET and provides guiding principles for plant monitoring system implementation and modern industrial control rooms.
- Chapter 7 presents a plant monitoring and operator support case study scenarios in ARCO-CIET including physical faults and digital control system faults.
- Chapter 8 presents a discussion of lessons learned and work path forward as well as considerations for applications to other systems. This chapter also presents some concepts for future development.

- Appendix A includes model derivations and other supplemental information to facilitate use and adaptation of the work described.
- Appendix B includes numerical parameter values and other data used in the case study.
- Appendix C includes the bibliography for this dissertation.

Chapter 2

State-of-the-Art

The research in this dissertation builds upon work across many different fields and industries. This chapter provides background on the applications and research that has supported industrial monitoring systems up to this point and the emerging concepts and opportunities for the future. It will begin by specifying the topics of primary interest and then give historical context before discussing the state-of-the-art for each step of the plant monitoring process. Finally, this chapter will zoom in on the state-of-the-art in the nuclear industry specifically before noting key concepts for improvement.

A word on terminology To discuss the state-of-the-art for plant monitoring systems, this dissertation first defines terms and limits scope. Plant monitoring goes by many names in literature such as health monitoring [12], fault diagnostics [13], digital twins [14], and operator support systems [15]. From the engineering point of view, this dissertation adopts the term *plant monitoring systems* to describe systems that support operational diagnostic, prognostic, and control capabilities in plants. Because the nuclear industry (and many others) still relies on human operators in the short term, this dissertation refers to the practical implementation of these systems for use as operator support systems as in [15]. The design problem then presents itself in two parts. The first is the design and implementation of algorithms and routines to facilitate autonomous plant analytics. The second is the design and implementation of human-machine interfaces (HMIs) to communicate actionable information to human operators. The focus of this dissertation is on a methodology for designing plant monitoring systems. It will then present a proof-of-concept operator support system built on this methodology.

Maintenance approaches Many researchers have proposed approaches that have shown promising results but require significant development work for each new fault considered [16–19] and must be later integrated into a complete system. Some systems have very specific faults (such as thermal faults in lithium-ion batteries and bearing defects in motors) and research is therefore targeted at these faults. With the ability to collect and organize plant information in a central location growing, more industries are seeking top-down ap-

proaches [20–22]. These approaches anticipate problems and lower risk from unexpected circumstances while also handling well-defined industry operational occurrences, or anticipated interruptions to the plant operation over its operating lifetime. This type of thinking is enabled by modern computation, communication, and data storage technologies.

Before plants relied on many interconnected processes with historic data on expected failure modes, the first maintenance practices in industrial processes focused on running until failure and fixing components as needed [23]. As machine complexity and demand grew in conjunction with leaps in instrumentation and control technology, plant owners sought more sophisticated practices [24]. The next maintenance strategy was time-based preventative maintenance. Industrial facilities could plan maintenance based on lessons learned and anticipated failure behavior. As in an auto owner's manual, planned maintenance is prescribed with certain frequencies and based on an initial plan. Planned maintenance may miss unanticipated operational occurrences or deviations from factory curves for component degradation. Additionally, planned maintenance may be overly conservative and lead to unnecessary and costly interruptions in plant operation. In an effort to address these shortcomings, modern research in industrial system health monitoring focuses on condition-based maintenance. Condition-based maintenance allows plants to optimize staffing and supplies by performing maintenance as needed only. It also has the potential to help plants run more efficiently if they are able to detect early signs of impending maintenance needs and address them before they occur.

The current nuclear industry standard is routine maintenance, with policies based on cumulative operating experience over the last 70 years. For the last few decades, there has been a push toward condition-based maintenance. While condition-based maintenance has not yet been fully adopted, the nuclear industry has adopted some practices and there is a wealth of academic literature on supporting tools and techniques. Coble et. al. published a thorough review on these contributions in 2012 [25] with some additional review in 2015 [26]. Some researchers focus on empirical solutions to specific problems like loose part monitoring while others attempt low-cost general approaches via machine learning-based methods. Some formulate first-principles models to ensure transparency in model behavior. Others even develop active interrogation methods for identifying plant performance issues. For those researchers who focus specifically on plant monitoring systems, the growing consensus, as described by Coble et. al. [26], is that these systems require summary and context. In other words, a holistic approach to systematically identifying monitoring needs and addressing them is necessary. There are two primary approaches: data-based models and physics-based models [27]. Contemporary literature overwhelmingly trends toward data-based models over physics-based models [16, 18, 28, 29] but this dissertation supports other researchers who argue that the two are complementary [14, 24, 25, 30, 31]. The priority, however, should be simple physics-based models that capture first-order effects of the system in explanatory and extrapolable ways. A brief discussion of modeling approaches follows.

2.1 Modeling

At its most basic form, plant monitoring is the collection of information from a plant as it operates. Instrumentation provides indications, measurements, and records of physical quantities that reveal plant status. The instrumentation for an entire plant consists of both direct measurements and methods of translating measurements into useful signals for operators to understand. Any definition of bounds on instrument readings relies on some form of a model. This is true even if the model is purely conceptual, such as an intuition that fluid temperatures should be limited to avoid boiling. Models are therefore attempts at characterizing a plant's behavior by describing relationships between inputs and outputs. A more sophisticated definition might be implemented as a plant operating envelope [32] or even as a digital twin [33].

In the context of plant monitoring systems, models serve as the basis for evaluating plant state both qualitatively and quantitatively. Depending on the model type and fidelity, model applications range from confirming expected operation to trajectory planning for control maneuvers. Models have long been used in industrial facilities to determine operating procedures and safety thresholds on system states. They are essential pieces of the plant design process that can also be used during operation. Modern contributions to fault diagnostics literature seek to leverage the plant information built into models to support plant monitoring systems. These models come in many forms but, for the discussion of plant monitoring, the two main types of models are data-based and physics-based.

Data-based models The defining characteristic of data-based models is that they are created and defined by data about plant behavior. Data-based models could also be called empirical models as in [24] because they are uniquely defined by a dataset from a given plant. They capitalize on the wealth of information recorded from an ever-growing array of sensors and digital processes in order to reveal performance patterns and trends. The nuclear industry has long used data-based models for applications including vibration monitoring, loose part monitoring, instrument response time inspection, reactor core monitoring, and more [24, 25]. Early versions of these models rely on experts to correlate signal features to physical behavior in order to develop libraries of identifiable behavior (signal-based methods). Current research seeks to eliminate the need for experts to perform this correlation. New approaches do not require humans to fully define the relationships between independent and dependent variables.

Because the amount of data available and the ability to efficiently capture it continues to grow, the potential of data-based methods to quickly generate powerful insights about system behavior continues to grow as well. For example, in the nuclear industry, researchers have developed data-based solutions for instrument calibration monitoring, reactor core monitoring, and transient identification [27]. Researchers in computer science and, recently, in many other fields are developing algorithms that imitate the human mind in their approach to pattern recognition or "learning". The allure of tools that can be systematically applied to a diverse variety of plant processes in order to characterize expected behavior at very low

cost is strong but comes with caveats. The most glaring drawback to data-based methods is their lack of physical explanatory information about the plant. Essentially, they are capable of taking in a set of inputs and returning a set of outputs. The internal process that results in these outputs, however, may be difficult to understand or correlate to physical mechanisms. Researchers build confidence in their algorithms by using "training" datasets — sets of existing or representative data so that the algorithm can demonstrate reliable prediction of accurate outputs. This leads to the common restriction on the application of data-based methods to situations and processes upon which the methods have already been trained. Furthermore, for a hypothetical situation in which the method predicts a value inconsistent with reality, it is difficult to perform a forensic investigation and determine its source of error. It is necessary to develop a robust understanding of potential false positive and false negative fault signals from data-based methods because the consequences of taking action on improper signals could be significant.

Despite these drawbacks, data-based methods continue to generate interest and likely have much to offer to the nuclear industry if applied appropriately. Examples of common data-based modeling strategies include artificial neural networks, multivariate state estimate techniques, principal component analysis, partial least squares regression, support vector machines, random forest techniques, and autoassociative kernel regression [27, 34]. Research and pilot studies have showed promise in using data-based methods for instrument calibration for on-line monitoring but have not been adopted in U.S. plants due to the need to obtain amendments to plant technical specifications [25]. New signal-based methods leveraging innovations in inspection technologies include empirical experience to develop signatures for faults. Some of these methods are neural networks for vibration monitoring fault characterization and linear relationships correlating valve degradation mechanisms to valve leak rate using frequency spectra profiles [25]. While researchers leverage their physical understanding of the plant in these cases, their models simply relate input and output data from a training data set.

Physics-based models In contrast to data-based models, physics-based models focus on the physical mechanisms that define the way a system receives a set of inputs and produces a set of outputs. Researchers who formulate these models must have access to domain expertise and attempt to incorporate all first-order effects at work while considering model uncertainty and error associated with lower-order effects. Ideally, the result is a model that can reproduce system behavior with physical consistency. This means that researchers can explore the resulting outputs and understand how and why the system behaves in a certain way. Model-based methods therefore have the potential to be explanatory, to be used diagnostically for new situations, and to be used for prognostic studies and predictive simulations.

Like data-based models, physics-based methods should be tested against representative plant data in order to support their accuracy and reliability. Unlike data-based models, physics-based methods can then be applied to other situations outside of operating expe-

rience. In fact, the U.S. Nuclear Regulatory Commission's website states that "...simple theoretical models are simply not capable of...full understanding of a system's response ... lessons learned from simulations carried out with these [advanced computational] tools help form the basis for decisions made concerning plant design, operation, and safety" [35]. Plant monitoring systems that may impact safety-critical plant systems must have a clear licensing basis that addresses algorithms, architectures, and applications [25].

The reason that physics-based models are not always preferred over data-based methods is simple: they require system-specific expertise and substantial engineering time investment to formulate and apply. High-fidelity models may provide very accurate results but may also be computationally very expensive to use in simulations. Low-fidelity models may sacrifice error and uncertainty margins for relative efficiency. Examples of physics-based models include state observers, parameter estimators, discretized system codes, and computational fluid dynamics.

More recently, some researchers are recommending hybrid methods that combine physics and data-based approaches [24, 25, 31]. These approaches seek to leverage extrapolability and physical consistency from the former while obtaining scalability and computational efficiency from the latter. The hybrid approach is likely the optimal path forward provided the strengths and weaknesses of the two methods are balanced through appropriately tailored applications. While academic researchers push the boundaries of plant monitoring systems from the theoretical and exploratory perspective, they must measure their impact first and foremost by the likelihood of practical adoption.

2.2 Fault diagnostics and prognostics

In [25], Coble et. al. describe a five-step monitoring system that starts with data acquisition and then proceeds to data manipulation, condition monitoring, health assessment, and finally prognostics. Additionally, a plant monitoring system may then generate an advisory message. Each of the steps in this process is a field in its own right and can be approached from many perspectives and in pursuit of different goals. This fact also represents the current state-of-the-art: only a few researchers tackle the issue of plant monitoring systematically. Plant owners may often go beyond vendor-recommended maintenance practices because they must identify shared vulnerabilities and conditions for the entire plant. Some systematic approaches include a strategy of using automatic control system actuations to reveal small faults [32] and deploying mass, momentum, and energy conservation equations in a generalized manner to detect leaks and other system changes [36].

Active and passive SSCs Nuclear plants are divided into structures, systems, and components (SSCs). Structures provide enclosure or support, systems include piping or cables, and components include mechanical and electrical equipment. SSCs can be further divided into two categories: active SSCs and passive SSCs. Active SSCs include moving parts like pumps and turbomachinery. Passive SSCs are parts that do not move, such as piping and

cables. Most fault diagnostic work has focused on active SSC monitoring due to active SSCs' vital role in plant operation and potential for damage in fault cases. Common subjects of active fault diagnostics include bearings, shafts, and rotors as well as valves and control components [37–39]. Passive SSC monitoring, including leak detection and cable health management, is a less mature field with newer focus on continuous and non-invasive monitoring [40–42].

Diagnostics The majority of fault diagnostics literature targets data manipulation and condition monitoring. The purpose of condition monitoring is generally to determine the state of a SSC. Health assessment then converts that state into actionable information for maintenance or operation planning. Coble et. al. point out that key technologies for condition-based maintenance in nuclear reactors include measurement methods, algorithms to characterize degradation state, and algorithms to use the degradation state to determine remaining useful life (RUL) and probability of failure (POF) of a SSC.

Diagnostics generally take the form of rule-based systems or classification systems. These systems either have logical checks to diagnose faults or classification algorithms to sort faults into "bins". It is very difficult to prescriptively define rules or classifications for all faults. The assumption that all faults have been modeled in a diagnostic system is referred to as the "closed-world assumption" [43] and is very difficult to support. Systems may adopt approaches that allow uncertainty in rules or classification. Probabilistic risk assessment (PRA) considers risks tied to plant operations and can benefit from plant monitoring systems if they provide on-line assessments of failure probabilities and incorporate passive SSCs into PRA analysis. [25]

Prognostics Compared to diagnostics, prognostics comprise a smaller body of literature [23]. Predictions of RUL and POF are widely-used goals. Coble et. al. define three classes of prognostic algorithms for time-to-failure [25]

- Type I : expected lifetime of average system in average environment
- Type II : expected lifetime of average system in specific environment
- Type III : expected lifetime of specific system in specific environment

All classes of prognostic algorithms have tradeoffs and limitations based on data quality and availability. Addressing these tradeoffs is the thrust of many current research efforts. In all cases, researchers must characterize uncertainties in their algorithms. Time-to-failure predictions that are too short or too long can have substantial economic and even safety consequences.

Other industries Outside of the nuclear industry, other fields have diagnostic and prognostic approaches. For example, electronics may have "canary", or built-in self-test (BIST), approaches that fail with some lead time compared to important components in order to give

users an early warning. In the defense sector, researchers have developed health management systems for vehicles such as the M1 Abrams main battle tank [44]. Nowadays, the push for efficient electric vehicles, autonomous cars, and energy storage has spurred a great deal of plant monitoring research in batteries and vehicles [45–48]. Many industries stand to benefit from each other's work as more common methods come to the foreground.

2.3 Fault mitigation

Fault mitigation is a subject area for which autonomy has the strongest potential. While fault diagnostics has some well-defined goal and a "true" answer, the goal of fault mitigation must be defined by the user. For example, if a fault occurs in an industrial facility, the safest option may be to shut the entire plant down. However, this may result in significant economic loss. For an even more difficult scenario, if the plant is delivering valuable electricity during an extreme weather event, there may be a public safety detriment if the plant stops operating. For these and other scenarios, there are a variety of objectives to optimize against one another.

The basic aim of fault mitigation is to achieve some safety or performance goal in spite of a given fault. For any physical faults that occur as a result of degradation or physical configuration change, it is unlikely that a control algorithm will be able to "fix" the fault and the goal is therefore to alert the operator and mitigate its detrimental effects until more permanent solutions are found. Fault mitigation is therefore a definition of system goals formulated as a control problem. The mathematical approach can take various forms, from reference tracking to emergency shutdown to optimal control.

To an extent, most industrial facilities that have some degree of control system autonomy already employ fault mitigation tools. If they have some capability for disturbance rejection, they may compensate for instrument noise and other Gaussian processes by adjusting to deliver certain outputs. The ability for control policies like this, especially in distributed control systems where different control tasks are separated, to inadvertently mask small-magnitude faults is the motivation behind the work of Cilliers et. al. in using control system actuations to reveal and characterize faults [32]. Control systems with fault mitigation capabilities built in are called fault tolerant control systems. Fault tolerant control systems use the results of fault diagnostics and prognostics to deliver an appropriate control signal.

Research in fault tolerant control systems often focuses on dynamic systems where control algorithms already need to account for changing plant environment. Active research areas include data-based plant process fault tolerant control and performance optimization [49], model-based fault-tolerant spacecraft dynamics control [50], and state observer-based adaptive vehicle management [51]. Some researchers are also developing generalized approaches for application to a variety of control systems [52, 53]. The literature for fault mitigation is rich. The most difficult goal to achieve for a given system is to deliver high-quality diagnostic and prognostic information and to choose appropriate objective functions for mitigation algorithms.

In the nuclear industry, systems have a relatively low degree of autonomy and operators generally follow prescribed written procedures. Fault mitigation research in nuclear often goes by the title of "resilient control systems". These resilient control systems must cooperate with the humans operating them. In other words, resilient control systems are designed to support operators' situational awareness and ability to respond to plant upsets [54–56] to maintain control systems' abilities to add value to plant fault tolerance.

2.4 Operator support systems

As researchers enrich the repertoire of fault diagnostics, prognostics, and mitigation tools available to industry, their implementation into control systems is critical. Human operators are still essential to many industries because no plant model is ideal and unexpected things will happen. Human operators continually learn and can react to surprises rather than inappropriately applying existing solutions. To quote Rochlin, "no learning can be taken to be exhaustive because the knowledge base for the complex and dangerous operations in question is inherently and permanently imperfect" [57]. Researchers have pointed out that fully automating industrial systems may take longer than envisioned; humans must be integral parts of control systems until then [58]. In autonomous systems, humans make decisions more than they crunch numbers. As long as human-machine interactions are important for operation, we will need to study and develop human-centered design approaches that optimize this partnership [59, 60]. We then arrive at the modern implementation of plant monitoring systems with human operators: operator support systems.

The most primitive operator support systems are any human-machine interfaces (HMIs) that facilitate communication and control between machines and their operators. This could be as simple as a button that an operator presses once to start a process and once to stop a process. If the button lights up when pressed, it communicates information to the operator that the system is activated. Due to the dizzying array of information and controls in modern industrial systems, operator support systems have a much more significant role than in the past. If human operators are not incorporated in the design process, results can be disastrous. In the case of the infamous Boeing 737 Max planes that have recently been grounded due to safety issues, engineers added automatic angle-of-attack adjustments to the aircraft control systems without properly training the pilots or communicating that information to them during flight. As a result, the pilots did not know how to respond or what the system status was as they flipped through paper manuals [61]. Operator training, instrumentation, and situational awareness all failed in this case. Many researchers are looking at how to best leverage modern technology for human-centered HMI design. Not only are researchers developing ways to accommodate human operators but they are also looking for unique benefits from human-machine collaboration over full automation.

Across disciplines, researchers envision the role of human operators in "smart" control rooms as decision-makers [62, 63]. Operator support systems collect, distill, and optimize information about plant systems to empower them to operate more effectively [55, 64]. In the

nuclear industry, researchers at Idaho National Laboratory have been working on designing operator support systems in a control room testbed [65–69]. The implementation of HMIs is plant-specific but guiding principles for human-centered design are inseparable from engineering challenges for plant monitoring. As Rochlin says, continued safe operation relies on "anticipation of events" [57]. We must adopt that philosophy in design, exercising humility and caution as appropriate to ensure we maximize benefits and minimize harm from these essential technologies.

2.5 Challenges for the nuclear industry and advanced reactors

This dissertation will use "advanced" to differentiate from current-generation, currently-operating nuclear power plants. Furthermore, it will focus on small modular reactors (SMRs). The U.S. Department of Energy (DOE) describes advanced SMRs as varying in size "from a couple megawatts up to hundreds of megawatts" [70]. SMRs also generally consist of modules — multiple similar units that, as a collective group, make up a single plant. The U.S. nuclear power industry has historically suffered from cost overruns and construction delays typically associated with massive civil engineering and infrastructure projects. SMRs seek to derive benefit from economies of scale not in size but in number. Advanced SMRs must adapt to compete in a modern energy market. Many are designed to operate at much lower pressures using molten salts, liquid metals, or even high-temperature gases. In fact, most advanced reactor designs will operate at higher temperatures than current reactors, in some cases enabling new and more efficient types of power conversion cycles [71]. Passive safety is also a central concept for advanced nuclear power plants. Some passive safety features minimize the need for electrical power and active operator intervention so that the plant can operate in both nominal and off-normal conditions with simplicity and robustness. Finally, one plant may consist of twelve individual SMRs made entirely from rail-transportable components. While these design features primarily improve upon those of more traditional designs, they may also make the application of traditional instrumentation, control, and plant monitoring systems difficult or even impossible. The following sub-sections examine each of the above-mentioned features for the unique considerations they demand from designers of advanced reactor systems and how those considerations might be made.

Higher operating temperatures Higher temperature operation not only exacerbates SSC degradation issues but also renders certain materials unusable. In regard to freezing concerns, higher operating temperatures could require special provisions for maintaining the system well above ambient conditions. Some instrumentation can be shielded from harsh chemical environments. However, reactor internals must still be kept above the fluid freezing temperature so high-temperature operation is the most pressing challenge for advanced reactor instrumentation.

Different working fluids Advanced reactor working fluids can be corrosive and their high temperature operation may restrict the lifetime of commercially available instrumentation. In addition to high temperature, these working fluids also challenge material compatibility for products from normal activation, radiolysis, and thermal decomposition. Molten salts, liquid metals, and high-temperature, high-pressure gases may necessitate specialized calibration and qualification testing, particularly for extreme in-reactor conditions [72]. These fluids may exhibit different flow and heat transfer behavior requiring new methods of monitoring. Some working fluids, such as liquid metals, even pose the issue of precluding visual inspection due to their opacity. They can also require new pump designs and methods of control [73]. For example, the possibility of freezing is an issue for molten salts and metals [74]. Different working fluids may also be toxic or otherwise hazardous to human health [74]. Innovative methods for sensor calibration, such as applying frequency response testing, may provide improved sensor calibration and data interpretation [75, 76].

Passive safety If a system heats and cools a fluid at different points in a flow path it can effectively drive the fluid with natural circulation instead of electrical or steam powered pumps. There are multiple new plant designs featuring natural circulation as a means of long-term heat removal in the case of unplanned shutdown. For these reactors, the rate of natural circulation and thus cooling relates to the magnitude of temperature excursion. Designers apply the principle of passive safety not only through physical design of the system via operating parameter selection and reactor neutronic feedback but also through the invention of specific passive safety devices, such as shutdown blades with magnetic latches that drop into the core and shut down the system following loss of electrical power [77, 78]. While many of these passive safety features forestall operational issues with elegance, they may not always represent the best option for reducing plant maintenance needs or ensuring profitable operation. There may be cases for which active control is actually preferable to passive mechanisms.

Small modular design In order to meet SMR design goals driven by economic and safety considerations, designers make sacrifices with respect to ease of access for maintenance and physical space used for instrumentation [79]. Tight spaces and sealed vessels obstruct routine inspection or intervention, posing an issue for existing solutions from light water reactors. Multi-modular configuration also poses a new class of operation and monitoring challenges [72]. The distribution of load across multiple reactors and power conversion systems all controlled from a central location ensures the needs of an advanced nuclear plant control room will be different from those of existing plants.

Potential solutions and approaches Approaching modern instrumentation and control challenges from a general perspective fosters the development of more robust solutions while also promoting industry-wide proficiency and best practices.

New designs need to consider the benefits of modernizing their concepts of operation. Most operation policies for nuclear power plants in the United States were designed decades ago and still rely significantly on analog systems and manual operator actions. Many of the digital components in existing nuclear power plant control rooms continue to emulate the appearance and functionality of their analog predecessors, and provide few additional functions [65, 80]. Digital control rooms promise many desirable improvements such as added autonomous control functionality; optimal information clustering, aggregation, and synthesis; control efficiency; and flexibility in operations.

Digitalization is also controversial from the perspective of cybersecurity, especially when considering the potential vulnerabilities associated with relying on discrete signals and data treatment that could be manipulated through malicious intent or accidental misuse. Passive safety systems can function without digital control and thus improve the resilience of nuclear power systems for cybersecurity. The attributes of digital control systems that can detect inadvertent faults may also be effective in detecting faults introduced by cyber threats [81].

One technology under active investigation is the implementation of virtual sensors [82]. Virtual sensors combine limited discrete data points (i.e. thermocouple readings or pressure measurements) in conjunction with a continuous physical model so that values are available outside of the physically instrumented locations. Virtual sensors therefore provide contextual data that maintains physical consistency with the rest of the instrumented domain. Not only could virtual sensors contribute to operators' understanding of system state, but they could also assist in online calibration or instrument evaluation efforts, mitigating the need both for extensive instrumentation and also for frequent in-vessel access [25, 82]. One early example of implemented virtual sensors is the pressurized water reactor subcooling margin monitor. This system, required in U.S. pressurized water reactors as of 1982, uses thermocouples at the reactor core exit and primary system pressure to determine the presence of subcooled water in the core [83].

Physical system models capable of running online (real-time or faster-than-real-time) and adjusting with system measurements empower operators with the ability to diagnose and prognosticate in the face of changing system conditions. For example, in the case of a transient in which passive safety systems might soon act, the operator could quickly simulate a few different potential courses of action in order to ascertain the best possible option for balancing safety, system stress, grid support, and profitability.

Finally, one physical technology poised to revolutionize nuclear plant instrumentation and control is the broader adoption of wireless sensing and actuation. Wired solutions not only require costly and inconvenient structural penetrations but also effectively add the entire length of wire to the set of monitored assets. Wireless sensors and actuators reduce the maintenance surface significantly and enable much simpler and less invasive instrumentation and control [25]. Wireless solutions may directly replace legacy wired functions or may lead to collection of new signals, such as wireless acoustics. With widespread adoption, industrial facilities can truly capitalize on new industrial trends and the advent of the Industrial Internet of Things. Designers should strive to overcome associated wireless networking and security challenges in favor of the myriad benefits.

Opportunities and outlook To summarize the state-of-the-art in the nuclear and other industries for plant monitoring and operator support systems, it is most practical to lay out some fundamental goals and obstacles. Industry would like to reduce operations and maintenance costs and to make them more predictable. This involves increasing productivity and operating time without maintenance while reducing downtime and the number and severity of failures. Furthermore, new policies should optimize operating performance and reduce overall life cycle cost for plant components. The nuclear industry is very risk-averse and that is particularly true when it comes to strategy changes that could affect licensing bases. The adoption of passive safety, which enables plants to be shut down into a safe state that does not rely on subsequent digital control or availability of electrical power, provides potential opportunities to increase the use of digital systems and wireless communication substantially. The primary opportunities for designers of plant monitoring and operator support systems are as follows:

- Improve data collection, record-keeping, analysis, and availability for reference
- Leverage both physics-based and data-based methods to monitor and optimize plant operation
- Integrate interdisciplinary work from designers of all plant systems without duplication
- Enable real-time, on-line maintenance and fault management
- Empower human operators with contextual top-down information to draw upon their strengths as critical-thinkers and decision-makers
- Attain cost and time reduction through the adoption and implementation of modern technology based on proven concepts

Chapter 3

Fault detection, isolation, and identification methodology

Plant monitoring system design is a task that requires modeling, analysis, testing, and iteration. This chapter guides the reader through the process from first specifying system goals through to experimentally verifying performance. Each section first introduces the relevant concepts in fault diagnostics and then applies them to an example system. This chapter refers throughout to structural analysis methods developed by many authors in the late 1990s and early 2000s for application to fault detection system design [84–87]. Specifically, researchers at Linköping University in Sweden have published a series of articles from the early 2000s and through today on the formulation of these methods into efficient algorithms implemented in MATLAB. They have written the Fault Diagnostics Toolbox in MATLAB [13] and demonstrated the application of structural analysis techniques for fault diagnostic signal generation to various simulated mechanical systems [53, 88–90]. Details on toolbox syntax and numerical methods can be found in their work. This chapter builds on their work by placing it into an iterative plant design context to enable its application to rapid prototyping studies.

3.1 Fault diagnostics background

Before outlining the fault diagnostics system design process, we define our goals. The purpose of fault diagnostics systems is to check plant process data for physical consistency with normal operation and to detect deviations from expected normal operation as clearly and early as possible. Once this is accomplished, the system can then communicate the information to the operator and give them the ability to understand the plant state. It can then solve the problem automatically or help the operator plan a course of action. With that context in mind, it is impossible to design for an unknown plant with complete generality. Plant specifics and purpose shape every step of the design process from modeling choices to performance metrics.

This chapter refers to expected, as-designed plant behavior as "normal operation". Normal operation corresponds not only to steady-state operation (e.g. full power operation for a nuclear power plant) but also to transient control maneuvers such as power level change. As long as these operation modes have been designed and engineered for the plant, the expected behavior during their execution is considered normal operation.

If the plant operates outside of expected behavior or deviates from conventional reading values (e.g. abnormally high temperatures or pressures in a nuclear reactor), this is called "off-normal" behavior. Off-normal behavior may occur as a result of many factors. If the causal factors are external (e.g. extreme weather events for a system with outside air intake) the system should have the capability to adjust to these dynamic conditions through its control system design. If the causal factors are internal and change the system as-designed, such as broken components or leaky pipes, these factors are "faults". Off-normal behavior caused by faults is "faulted" behavior. The complementary set of behavior is then "fault-free" behavior. The goal of our design problem is to diagnose these faults if they occur.

The focus of this dissertation is on plant monitoring approaches that incorporate physical information about the plant. For that reason, descriptions of the plant during fault-free operation have faults with magnitude zero. Faulted behavior affects the same equations by changing fault magnitude to nonzero. As a simple example, this chapter introduces the system shown in Figure 3.1.

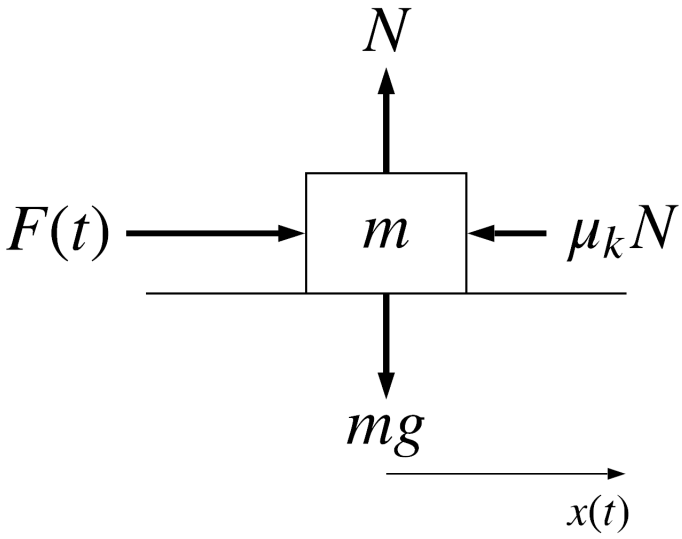

Figure 3.1: Block on flat surface

Figure 3.1 shows a block of mass m that is pushed by unknown force $F(t)$ on a flat surface. As it slides along the surface, it experiences sliding friction force $K = \mu_k N$. We

measure its position x at a given point in time t as $y = x(t)$. Our model of the system is then:

$$y(t) = x(t) \tag{3.1}$$

$$\frac{d^2x}{dt^2} = \frac{F(t) - \mu_k N}{m} \tag{3.2}$$

where $\frac{d^2x}{dt^2}$ is the second time derivative of position, or the block's acceleration. We can calculate $\frac{d^2x}{dt^2}$ from time series position data. The model parameters are μ_k, m, and N. The variables are $y(t)$, $x(t)$, and $F(t)$. Because the measurement $y(t)$ yields a numerical value, it is a known variable while $x(t)$ and $F(t)$ are unknown. There are two equations and two unknowns. This is a system that we can solve for both unknown variables given time series data.

If we observe that our model seems incorrect or that the modeled system has changed in some way, there is currently no way of confirming our suspicions. If we make a measurement of $y(t)$ and calculate an $F(t)$ that seems nonsensical, we cannot determine the source of this inconsistency. It then becomes useful to introduce a fault term into equation (3.2).

$$\frac{d^2x}{dt^2} = \frac{F(t) - \mu_k N}{m} + f \tag{3.3}$$

This is a general fault term that does not specify a form or cause of the fault. It provides a useful convention for defining the difference between fault-free and faulted behavior. During fault-free operation, $f = 0$. During faulted operation, $f \neq 0$. This fault term corresponds to faults directly related to the physics of the equation in which it is described. Therefore, this term does not cover potential sensor faults that would cause $y(t) \neq x(t)$, but only faults in the physical system described by equation (3.2). To include potential sensor faults, we would need to add a fault term to equation (3.1).

$$y(t) = x(t) + f_y \tag{3.4}$$

If we knew the forms of expected faults, we could formulate our fault terms accordingly to render the expected faults immediately identifiable. For example, to include a sudden change in surface roughness, we could add the term f_{μ_k} and to include an unexpected force we could add the term f_F as follows:

$$\frac{d^2x}{dt^2} = \frac{F(t)(1 + f_F) - \mu_k N(1 + f_{\mu_k})}{m} + f \tag{3.5}$$

However, each additional fault term f is another variable. Therefore, it would only be useful to add the two specific fault terms f_F and f_{μ_k} if we had at least two more equations with sufficient variable relationships that would allow us to solve for all terms algebraically. We are now approaching an important point that motivates our strategy for choosing fault detection system equations. We need at least one diverse method of determining our variable

quantities if we want to be able to determine the fault term f. The relationship between number of equations and number of variables and their corresponding applications follows these rules:

$$no.\ of\ equations\ <\ no.\ of\ variables$$

Under-determined system

$$no.\ of\ equations\ =\ no.\ of\ variables$$

Just-determined system: algebra

$$no.\ of\ equations\ >\ no.\ of\ variables$$

Over-determined system: fault detection

Without additional model equations, our block system is just-determined rather than over-determined. We will adopt a systematic method to ensure we are applying the third rule for all fault diagnosis scenarios of primary interest. First, however, this chapter suggests collecting all models already available and determining their utility for diagnosing faults. Rosich et. al. discuss the model selection process to ensure suitability for fault diagnosis and note that disparate model types may be used if they are computationally tractable in [90]. This chapter leverages their work to derive benefit from diverse model types. Combinations of physics-based and data-based approaches have also been proposed by other researchers seeking to capitalize on new data availability and physical system descriptions [14, 24, 31].

3.2 Setup and interdisciplinary approach

Compile models used for design and planning Plant monitoring systems seek to measure, describe, and analyze a plant designed and constructed by an interdisciplinary team. There can be substantial additional benefits if one draws on their hard work and expertise at the beginning of the system design process to generate models for the expected plant behavior. The benefits of a well-designed plant monitoring system are multi-faceted. It can improve plant performance, reduce maintenance concerns, and support goals in addition to those of the system's engineers. The first step, then, is not to begin modeling the plant from scratch but to take the existing models developed throughout the design process and compile them in one place.

The two most likely types of plant descriptions that are available before any experimental data has been collected are

- Physics-based models
- Measurement equations

The physics-based models likely come from engineering designs and should describe the primary physics of interest in an experimental or prototypical system. Simple models are a good starting point to facilitate rapid prototyping. The most important models to incorporate are those describing the most unique or vital aspects of the plant — first-order energy transfer mechanisms or actuation points.

Measurement equations depend on experimental designers' choices and the goals of the facility but provide very simple equations like equation (3.1) in the form of $y = x$. They play an essential role in plant monitoring. After all, without them, there is nothing to ground the models in reality.

Other model types may be available and should be incorporated if so. This chapter includes a discussion of additional model types and their strengths and weaknesses in its final section.

Example 3.2 For this chapter, we will follow along with an example plant to illustrate each concept. Our example is a simple experiment representing a bulk handling nuclear processing facility — a facility for separating plutonium and uranium from spent nuclear fuel for the purpose of making new fuel and minimizing raw material consumption. While bulk handling facilities are highly-engineered and feature both nuclear and chemical interactions, researchers at Berkeley have designed a simple experiment using water and medical radiotracers to simulate movement of nuclear material and to test methods of detecting material holdup and diversion. Material holdup and diversion may correspond to plant inefficiences or faults such as blockages and leaks. They may also lead to unknown nuclear material streams and it is therefore very important to understand if the plant is operating in a faulted regime.

The facility, shown schematically in Figure 3.2, consists of four tanks to represent different stages of a chemical process. Each successive tank is situated progressively lower than the last to facilitate gravity-driven flow between them. Researchers pump water containing a radiotracer into the first tank and it then flows from tank to tank, ultimately collecting in the final drain tank.

Because we are observing a flow process and are concerned with tank inventory, our model relates flow and inventory. The flow from one tank to another is driven by a pressure differential that can be described by the density of the fluid, the acceleration due to gravity, and the difference in fluid height. Some flow resistance also impedes this driving force. The height in each tank also depends on tank area. We will refer to the tanks by numbering them, from left to right, Tank 1 through Tank 4. We will refer to the source as Tank 0. We then have a very simple model to describe the dynamics of the tank inventories:

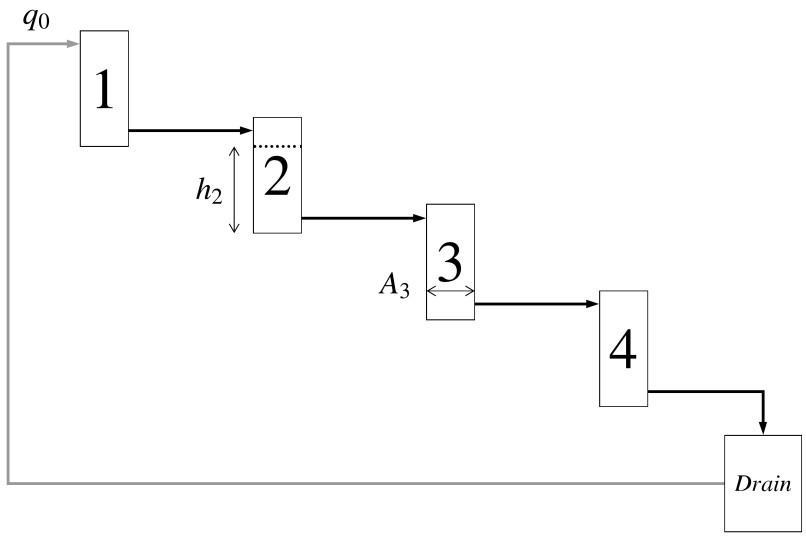

Figure 3.2: Bulk handling nuclear processing facility schematic

$$q_1 = \frac{\rho g(h_1 - h_2)}{R_1} \qquad \dot{h_4} = \frac{1}{A_4}(q_3 - q_4)$$
$$q_2 = \frac{\rho g(h_2 - h_3)}{R_2} \qquad \frac{dh_1}{dt} = \dot{h_1}$$
$$q_3 = \frac{\rho g(h_3 - h_4)}{R_3} \qquad \frac{dh_2}{dt} = \dot{h_2}$$
$$q_4 = \frac{\rho g h_4}{R_4} \qquad \frac{dh_3}{dt} = \dot{h_3}$$
$$\dot{h_1} = \frac{1}{A_1}(q_0 - q_1) \qquad \frac{dh_4}{dt} = \dot{h_4}$$
$$\dot{h_2} = \frac{1}{A_2}(q_1 - q_2) \qquad y_1 = q_0$$
$$\dot{h_3} = \frac{1}{A_3}(q_2 - q_3) \qquad y_2 = q_4$$

where q_N is the volumetric flow rate out of, h_N height of fluid, R_N flow resistance, and A_N cross-sectional area of tank N, respectively. ρ is the density of the fluid and g acceleration due to gravity. Additionally, $\dot{h_N}$ and $\frac{dh_N}{dt}$ are each the derivative of h_N with respect to time, where the $\frac{dh_N}{dt}$ equations are included for the purpose of showing that $\dot{h_N}$ can be calculated as the slope between two different data points for h_N in time. y_1 and y_2 represent measurements of the first tank inlet flow (where "Tank 0" is simply the flow source) and the Tank 4 outlet, respectively. This means that, for this example, we assume that we are

able to obtain data for flow into the process and flow out of the process. Because owners of reprocessing facilities will not typically share information about their facilities readily, this may already be an excessive amount of information to expect.

Once we have compiled system models and instrument relations, we can begin to assess the utility of our models for designing a fault detection system.

3.3 Structural representation

We can now describe our models via structural representation. To do so, we will not include actual model form or coefficients [91]. Instead, structural representation requires only two pieces of information: the number of equations in our model and the plant variables described by each equation. By building a matrix of all equations and their corresponding variables, we can quickly determine, by inspection, for which variables we have an under-determined set, for which variables we have a just-determined set, and for which variables we have an over-determined set. This allows us to assess whether our model is suitable for detecting faults in given parts of the plant. This chapter will continue referring back to structural representation throughout the plant monitoring system design process. It is very powerful as a universal language for interdisciplinary communication among team members with the appropriate level of detail for fault diagnostics. Note that the Fault Diagnostics Toolbox still requires the designer to adequately model the target plant and only facilitates best-case conclusions — it cannot fix measurement, model, or programming errors and should be filtered and thresholded for proper application [90].

Building the representation Before we construct our structural representation, we need to break our model into a few pieces. We refer to all values that change throughout operation and that we do not directly control as *unknown variables*. Inputs and measurements are our *known variables*. Finally, we have our *fault variables*, which play a role as in Section 3.1.

Faults may have cascading effects on multiple equations but these should be captured in the interdependence of the model. Therefore, we should only include each fault variable in one equation. This ensures future separability of fault signals from one another. For example, a fault in bearing alignment should only be included in an equation specifically describing the physical meaning of bearing alignment. It should not also be included in another equation describing variables that are indirectly affected by bearing alignment. If there are multiple model equations with direct effects from a single fault, we can introduce an additional equation $x_f = f$ and then replace f with x_f in each relevant equation. That way, we maintain one unique equation per fault to facilitate isolability as recommended by Krysander and Frisk in [92].

To construct the structural representation of our system, we follow this step-by-step process:

1. List each unknown variable across the x-axis of the matrix.
2. List each control input and sensor measurement across the x-axis of the matrix. Each typically corresponds to one or more unknown variables.
3. List each fault to be included in the analysis across the x-axis of the matrix.
4. Number all model equations and list them along the y-axis of the matrix.
5. Going one equation at a time, place a mark at the point for each unknown variable, known variable, and fault variable described by the equation in the corresponding (x,y) position.
6. For variables that are differentiated values of another variable, place a "D".
7. For variables that are integrated values of another variable, place an "I".

This process is relatively quick for a model with few equations but it can become untenable for models of hundreds or thousands of equations. The Fault Diagnostics Toolbox facilitates structural representation with flexibility for the user to enter model equations either with algebraic relationships or as lists of included variables. As a demonstration, we develop our structural representation in a continuation of the example from Section 3.2.

Example 3.3 Before building our structural representation, we should separate our model into its unknown, known, and fault variables. We begin by selecting fault variables. Our primary consideration is faults related to nuclear material diversion and holdup. The basic faults we consider for this system, then, are represented by fQ_N and fH_N, which correspond to faults affecting flow out of each tank and affecting the height of fluid in each tank, respectively. Our updated model, with numbered equations, is now:

$$e_1 : q_1 = \frac{\rho g(h_1 - h_2)}{R_1} + fQ_1 \qquad e_8 : \dot{h_4} = \frac{1}{A_4}(q_3 - q_4) + fH_4$$
$$e_2 : q_2 = \frac{\rho g(h_2 - h_3)}{R_2} + fQ_2 \qquad e_9 : \frac{dh_1}{dt} = \dot{h_1}$$
$$e_3 : q_3 = \frac{\rho g(h_3 - h_4)}{R_3} + fQ_3 \qquad e_{10} : \frac{dh_2}{dt} = \dot{h_2}$$
$$e_4 : q_4 = \frac{\rho g h_4}{R_4} + fQ_4 \qquad e_{11} : \frac{dh_3}{dt} = \dot{h_3}$$
$$e_5 : \dot{h_1} = \frac{1}{A_1}(q_0 - q_1) + fH_1 \qquad e_{12} : \frac{dh_4}{dt} = \dot{h_4}$$
$$e_6 : \dot{h_2} = \frac{1}{A_2}(q_1 - q_2) + fH_2 \qquad e_{13} : y_1 = q_0$$
$$e_7 : \dot{h_3} = \frac{1}{A_3}(q_2 - q_3) + fH_3 \qquad e_{14} : y_2 = q_4$$

Our unknown variables are q, h, and $\frac{dh}{dt}$ for each tank and q_0 for the source. Our known variables are y_1 and y_2. Our fault variables are fQ and fH for each tank. Everything else is a parameter: ρ, g, R, and A for each tank. Once we enter the equations into MATLAB, we get the plot shown in Figure 3.3.

The Fault Diagnostics Toolbox lists the model equations along the y-axis and the variables along the x-axis. Blue dots in the left-most section indicate the unknown variables while red dots in the middle section indicate the fault variables. Black dots in the right-most section indicate the measurements each equation describes (and inputs, when they are part of the model). Blue D's and blue I's correspond to differential and integral relations, respectively. When concluding that a variable is structurally over-determined in the model, consider that if one of the equations is a differential or integral relation, multiple data points in time will be needed to solve for all variables.

Figure 3.3 shows that we have some structural over-determination in our model: we have multiple relations for every variable. However, we must examine the level of information available from our model more closely to determine its suitability for fault diagnostics.

Building a structural representation of a model is already a helpful method of organizing information to understand what is and is not monitored with the formulated equations. It would not be inappropriate at this step, if the plant monitoring system designer notes gaps in the model, to seek further modeling equations before proceeding to evaluating the model's suitability as a plant monitoring system. However, as shown in the next section, the process for evaluating a model's ability to generate fault signatures is straightforward and can help guide additional model selection.

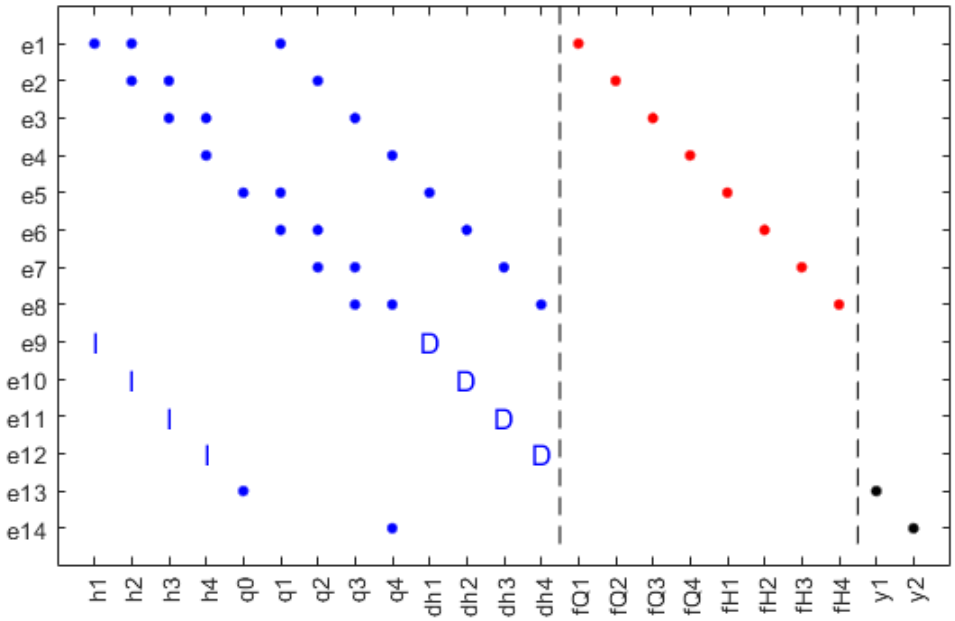

Figure 3.3: Structural representation of bulk material processing facility model using Fault Diagnostics Toolbox

3.4 Fault detectability and isolability

Fault diagnosis has distinct phases. Fault *detectability* is the ability to distinguish faulty behavior caused by a specific fault. Fault *isolability* is a property of detectable faults meaning the ability to distinguish a detected fault from any other specific fault [91]. Whether it is necessary to satisfy both detectability and isolability for a given fault is consequential of the plant monitoring system goals. We will define detectability and isolability in further detail below.

Detectability Fault detectability means that the plant monitoring system can generate a signal for faulted operation when a fault affects the plant. Detectability does not imply that the specific fault causing faulted operation is known. Detectability only implies that one or more faults is active. Structural detectability is a feature of model form described by model structural representation — it includes no information about model uncertainties, measurement error, or sensitivity deadband. Therefore, the plant monitoring system designer should factor uncertainty and error terms into model equations in later iterations. Modeling and experimental exercises can be applied to isolate detection sensitivity to these confounding

factors. Khorasgani et. al. provide one method and examples for this in [93]. The condition for fault structural detectability, in plain language, is:

A fault is structurally detectable in a model if it is part of a structurally over-determined set of equations.

Isolability Guaranteed fault detectability is certainly a positive characteristic of a plant monitoring system but fault isolability — the ability to distinguish fault signatures from one another — is a higher level of sophistication that facilitates further action. Fault isolability means that the plant monitoring system can generate a specific fault signal unique to a specific fault if the fault affects the system. Isolability of a fault only exists in relation to other faults — faults are isolable from one another. A fault may be isolable from some faults but not others. Full isolability for a specific fault is achieved if that fault can always be identified when it occurs. If the effects of a fault cannot be distinguished from the effects of a subset of other faults, then it only has partial isolability. The criterion for fault isolability follows directly from that for fault detectability:

If the set of equations for which a fault is structurally detectable does not include other faults, that fault is then structurally isolable from those faults. If the equation set can exclude all other model faults, that fault then has full structural isolability [92].

Valuable tools that can facilitate visual analysis of a model's structural representation include isolability matrices and Dulmage-Mendelsohn decompositions. It may be most helpful to illustrate these concepts as applied to our example.

Example 3.4 The Fault Diagnostics Toolbox includes an algorithm for performing detectability and isolability analysis. We can already assess detectability visually from Figure 3.3 but can look at detectability and isolability together using an isolability test. The results of the isolability test are shown in Figure 3.4.

We read the isolability matrix as follows: each fault is listed along both the y-axis and the x-axis. Starting with each fault on the y-axis, the model supports structural detectability of the fault if it has any blue dots for each entry on the x-axis. If the fault occurs, the model allows it to be identified as *any of* the corresponding fault(s) on the x-axis for which it has a blue dot filled in. We see from Figure 3.4 that, while all eight faults are detectable, none are isolable from any others. That means that we only know if a fault occurs but not which fault(s) are occurring.

We can further understand this result by plotting the Dulmage-Mendelsohn (DM) decomposition [91, 94]. This is a way of rearranging the equations so that we have, at the top, our structurally under-determined part (no. of equations $<$ no. of variables), in the middle our structurally just-determined part (no. of equations $=$ no. of variables), and at the bottom our structurally over-determined part (no. of equations $>$ no. of variables). The DM decomposition for our current model is shown in Figure 3.5.

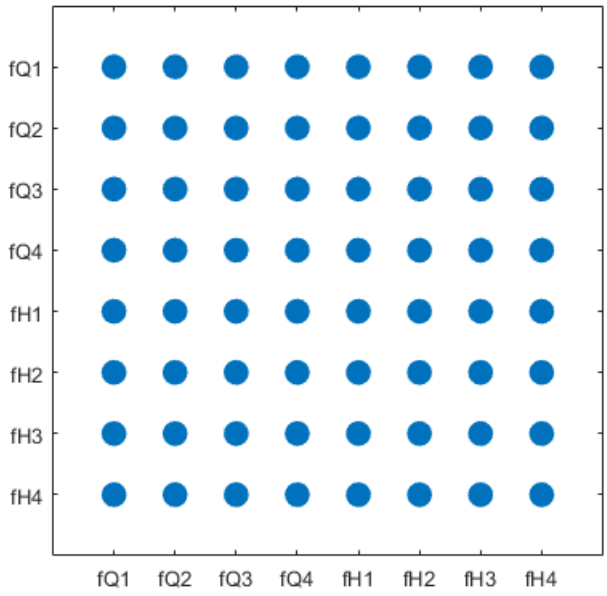

Figure 3.4: Isolability matrix of model using Fault Diagnostics Toolbox

For our current model, we only have a structurally over-determined part, meaning that we have no just-determined or under-determined equations or variables. Furthermore, our entire model exists within one equivalence class, denoted by the gray rectangle. Equivalence classes can be thought of as sets of equations for which every constituent equation is necessary to make the entire set over-determined. Practically, this means that no faults within the gray rectangle are structurally isolable from each other. Our modeled faults are shown on the right side of the DM decomposition with red dotted lines to show the equations they affect. We can understand the DM decomposition conceptually by imagining that each red dotted line "activates" the gray rectangle. If multiple red dotted lines run through the same gray square, their effects are structurally indistinguishable from one another. Figure 3.5 provides the information necessary to establish a path forward for improvement to our plant monitoring system. We must add additional equations that separate our model into more than one equivalence class and, ideally, into an equivalence class for each fault.

Our response to different types of faults affecting each tank will be different. We therefore want to be able to distinguish fault types from one other, at the very least, and would ideally like to be able to isolate faults to their specific tank locations. For this reason, we already recommend a design change to our plant monitoring system before going on to develop the application of our model. This helps illustrate the power of the structural approach and the Fault Diagnostic Toolbox.

We can improve our model by adding a single measurement. The authors of the Fault Diagnostics Toolbox have previously published articles on the application of structural analysis

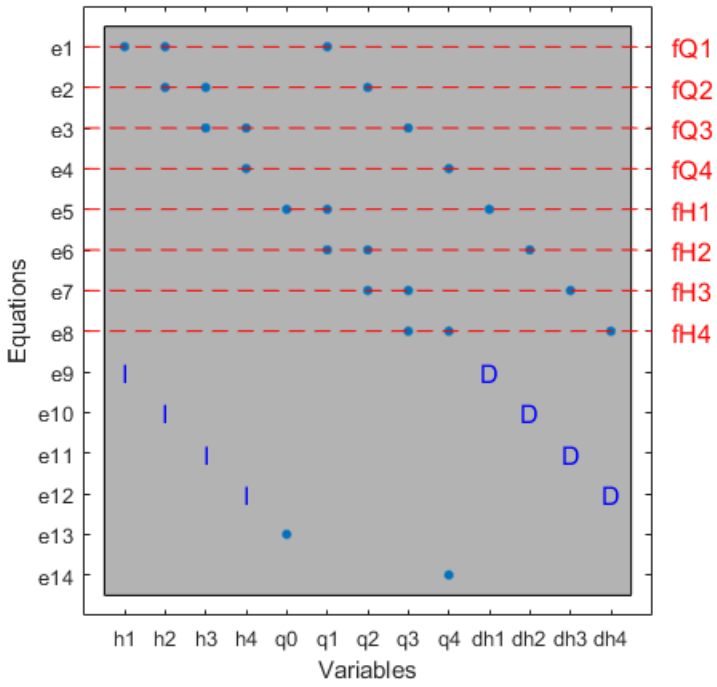

Figure 3.5: Dulmage-Mendelsohn decomposition of model using Fault Diagnostics Toolbox

to sensor placement [88, 92] and placing sensors to facilitate fault isolability is a reasonable next step. If we add an additional measurement equation,

$$e_{15} : y_3 = h_1 \tag{3.6}$$

to measure the height of Tank 1, we obtain the new DM decomposition shown in Figure 3.6.

We see from this Figure 3.6 that, through the addition of one measurement alone, we have separated all fH_N into their own equivalence classes and all fQ_N into equations with isolable faults. In fact, the simple addition of one measurement has pushed six equations into equivalence classes of their own, as indicated by the lower-right section of the figure bounded by the black dotted line. Faults in equations 14 and 15 could also be structurally isolable if we chose to model them. It's also useful to note that all of our faults affecting tank fluid height rely on integral and differential relationships for their structural over-determination. We may later find that these signatures for these faults are computationally more difficult to obtain than for faults with simpler relationships.

To double-check the effect of adding equation 15 on isolability only, we can perform an isolability analysis on our new model, as in Figure 3.7.

The isolability matrix now shows us that, for each of the eight hypothetical faults that occurs, we can generate a signature for that unique fault. This diagonal isolability matrix has the ideal shape — every fault is uniquely identifiable as itself. One important caveat

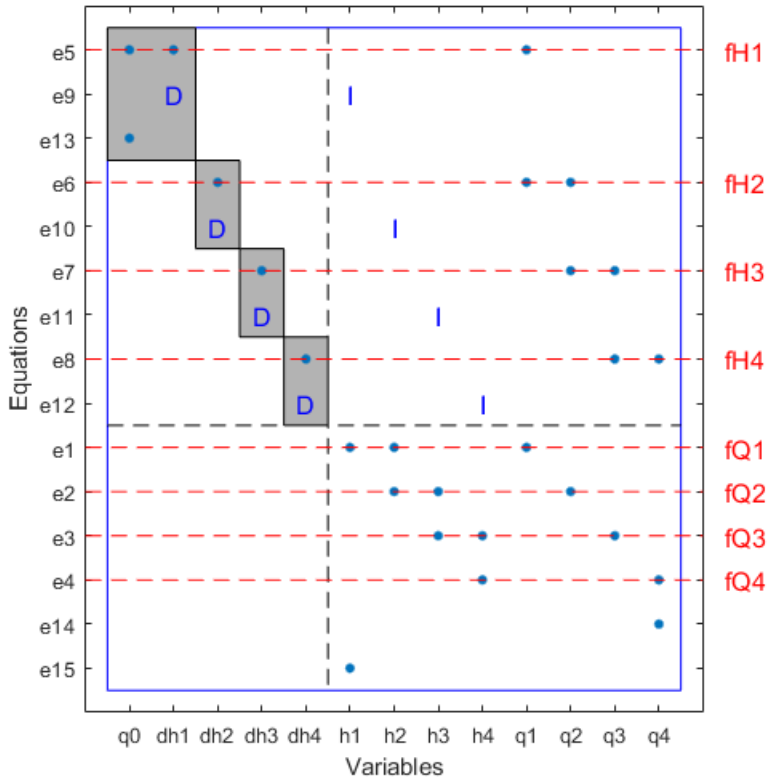

Figure 3.6: Dulmage-Mendelsohn decomposition of model with Tank 1 height measurement using Fault Diagnostics Toolbox

of this example is that the measurement of h_1 must be collected over at least two points in time in order to facilitate the use of the integral and differential relations. Our conclusion from this exercise is that the additional measurement of the height of Tank 1 over time gives us a method for developing signatures for each and every fault. This height measurement may not be a realistic piece of information from a nuclear material bulk handling facility in the real world. Redundant and diverse methods of measuring this height may be desirable to allow detectability of measurement faults. Designers will need to consider the unique considerations of their target plant.

The ease and practicality for implementation of fault signatures is not guaranteed. For example, they may require iterative numerical methods to produce, where an algorithm uses an initial guess and multiple iterations before converging at a solution [89]. Fault detection system designers must explore their options. Ideally, sequential residual generators, which solve equation sets by plugging values in systematically, are the most computationally efficient and transparent ways to obtain fault signatures. This chapter discusses residual

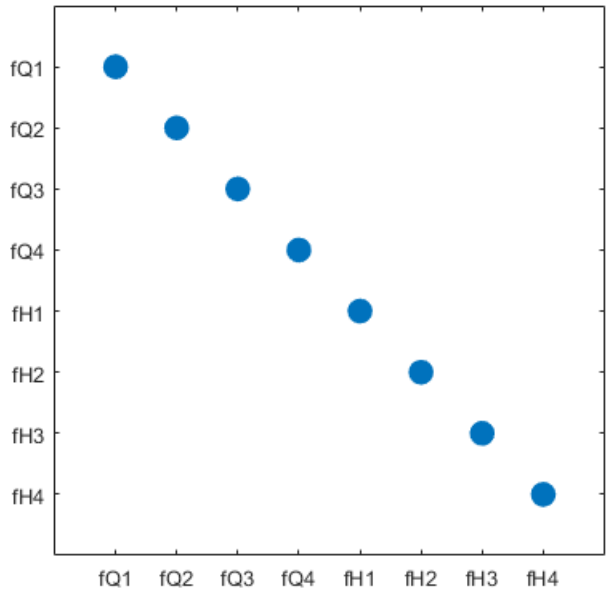

Figure 3.7: Isolability matrix of model with Tank 1 height measurement using Fault Diagnostics Toolbox

generator design in the next section.

3.5 Rapid prototyping

Determine testable set of equations and possible residual generators After assessing the suitability of a model for use in generating fault signatures from plant monitoring data, we must determine the relevant equations and methods for doing so. The general approach for fault signature generation is through the use of analytical redundancy relations or *residual generators* [93]. If an equation set can be solved to obtain values of unknown variables in multiple ways, their values are confirmed when the solutions agree. If the solutions do not match, the discrepancy is a residual signal r. Residual generators are equations that compare multiple solutions for a variable and reveal the role of faults in the equations. They generate a value of $r = 0$ when no fault is present and $r \neq 0$ when fault magnitude is nonzero.

The simplest and most computationally efficient type of residual generator is a sequential residual generator [90]. They programmatically plug in values to equations in a just-determined system, one at a time, until they have solved for every unknown variable. After they obtain the value of the final variable, at the last step, they compare the result with the output of a redundant equation in the form $r = |x - \hat{x}|$ where $x = \hat{x}$ for a fault-free case. As

an illustration, take the model

$$\begin{aligned} e_1 &: y = x_1 \\ e_2 &: x_2 = c_1 x_1 - c_2 \\ e_3 &: x_2 = c_3 e^{-c_4} \end{aligned} \tag{3.7}$$

where y is a known measurement, x_1 and x_2 unknown variables, and c_1, c_2, c_3, and c_4 known parameters. Figure 3.8 shows the sequential solution path and redundant equation for x diagrammatically with r as the resulting residual generator:

$$r = |e_3 - e_2| \tag{3.8}$$

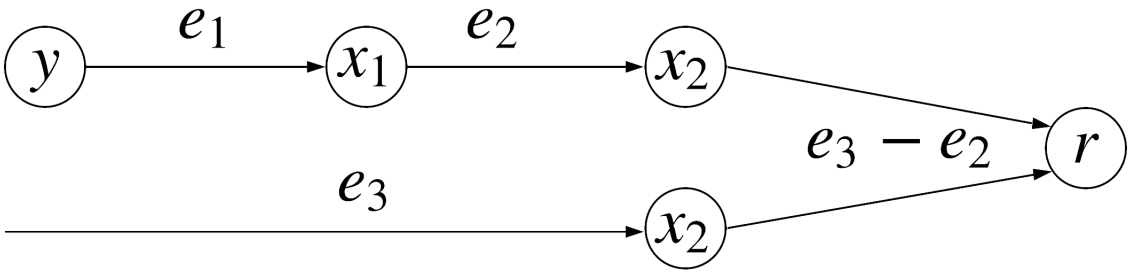

Figure 3.8: Diagram of residual generator for example system

Sequential residual generators are also advantageous because they can be used with models that incorporate a variety of equation types from first-principles equations to lookup tables. The only requirement is that they take inputs and compute outputs. We now need guidance on how to select the appropriate model equations to design residual generators and generate fault signals.

Determine test equation sets Models of real-life systems tend to have multiple candidate equation sets suitable for formulating residual generators. These equation sets should be structurally over-determined by having more equations than unknowns excluding fault variables. If every variable in the set is over-determined, it is then a *Proper Structurally Over-determined (PSO)* set [91]. Krysander et. al. [95] define a *Test Equation Support (TES)* as a set of equations that is PSO and contains some, but not all model fault variables.

Going one step further, an equation set is a *Minimum Test Equation Support (MTES)* if no subset is also a TES. To find all model MTESs is therefore to find all candidate PSO equation sets that can be used to formulate residual generators for the model. Ideally, the MTESs will cover all model faults.

For our final down-selection of equations, we should pick out the subsets in our MTESs that are minimally structurally over-determined (MSO) sets. These have no subset of equations that is structurally over-determined. If the structure of any of these MSO sets allows us to remove one equation and leave a just-determined set, we can then use the redundant equation as a residual generator.

Residual generator selection criteria When sequential residual generators like the one in Figure 3.8 can simply plug one value after another into each equation, computation is inexpensive. However, operations such as differentiation and integration requiring numerical methods can become expensive [89, 96]. Computational cost is a primary criterion for residual generator selection. Plant monitoring systems ideally use only residual generators requiring minimal differentiation or integration with respect to time.

The other criterion for sequential residual generator selection is coverage of system faults. We can investigate this using isolability analysis on our new model subset MSOs in the same fashion as for the full model. If we find that we don't have full fault isolability for our model, this may be a point to seek further modeling equations. Iterative model development is an essential component of this methodology that both relies on and benefits experimental trials.

Design experiments and simulations Once the designer selects equation subsets to use for residual generators, they can plan experimental and simulation studies to test fault diagnostic capabilities. These subsets contain the formula for experimental procedures by providing the list of measurements, inputs, and fault signals in focus. To best demonstrate, we will continue with our example system.

Example 3.5 For our example system, we have eight faults to study. We hope to achieve full fault isolability from our given model. We begin by determining our MTESs and corresponding MSOs. For this system, we obtain eight separate MTESs with each MTES containing one MSO able to detect every fault except one but with no fault isolability. The fault signature matrix in Figure 3.9 shows which MTES is capable of generating fault signatures for which faults.

We could endeavor to design a fault detection system with this set of MTESs that would enable full fault isolability as promised by the DM decomposition in Figure 3.6. Instead of each residual generator yielding a positive fault signature for an individual fault, we expect to see one residual generator alone that is *not* sensitive to that fault. Furthermore, our ability to isolate faults in this manner would be compromised if multiple faults occurred simultaneously. Finally, we have not yet down-selected to the MTESs that are computationally efficient. If we do this, we see in Figure 3.10 that only three of our possible residual generators are left.

Unfortunately, this leaves us with only three isolable faults: fQ_4, fH_1, and fH_4. It is likely that we would want to improve this fault detection system. However, we could design experiments for these three faults. The equations in $MTES_4$, $MTES_5$, and $MTES_8$ are

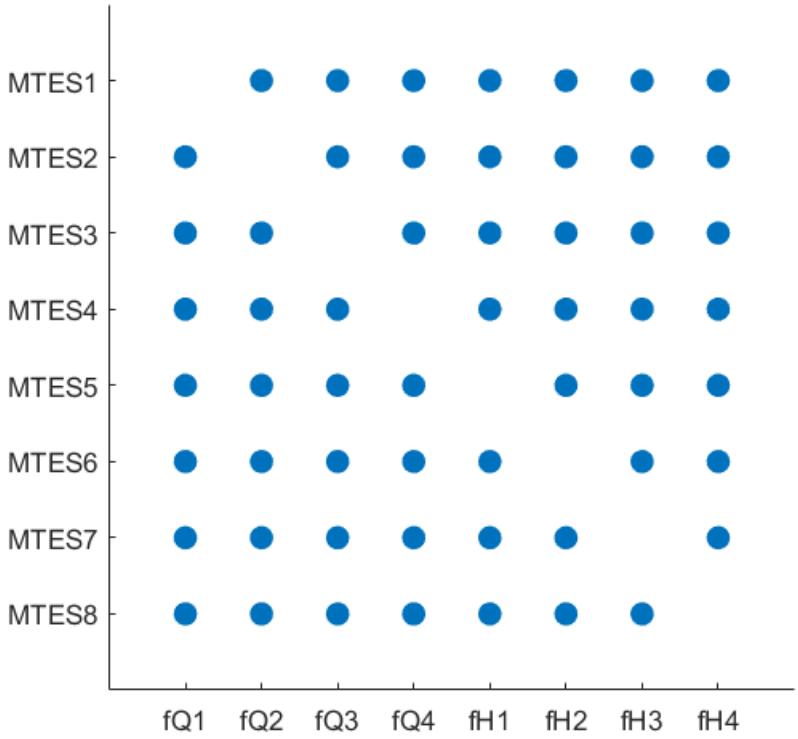

Figure 3.9: Fault signature matrix for Minimum Test Equation Supports in the nuclear bulk material handling system model

almost the same. The only difference between them is that each leaves out one equation. $MTES_4$ is incapable of detecting fQ_4 and it accomplishes this by excluding e_4, the equation containing fQ_4.

Our preparation of experimental procedures is then straightforward. By preparing three experiments in which each experiment perturbs a different fault, we can test the three residual generators' abilities to detect faults affecting flow out of Tank 4 and faults affecting the heights of Tank 1 and Tank 4. The set of plant monitoring data to collect is our residual generators' required inputs. The relevant system parameters are also clearly described by the model.

We can also conduct experiments in which we perturb the other five modeled faults and should see that all three of our residual generators respond. We will not be able to separate those faults from one another, though. Finally, it is important to test residual generators to obtain their fault-free response. Residuals will typically have some nonzero value due to the fact that they are based on models and are consequently not perfect copies of the physical system.

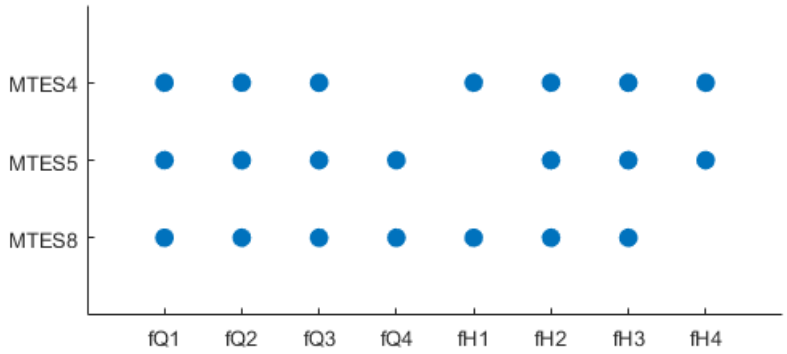

Figure 3.10: Fault signature matrix for computationally efficient MTES in the nuclear bulk material handling system model

3.6 Iterative development

Use results to iterate on system design If a model is unable to isolate certain faults, as in the example above, it may need supplementary equations or relationships. Furthermore, experimental tests of residual generators may expose unexpected residual behavior. So far, the example model contains simplifying assumptions and does not include any terms to accommodate uncertainty or noise. Consistent high-magnitude nonzero residuals may indicate that the model lacks fidelity. If the uncertainty or noise has an expected average value, the designer could simply choose alarm thresholds above that value. It will be important, however, to make sure that the residual value in the presence of faults is significantly different than its noise level.

Add diverse models as appropriate If the model lacks equations sufficient to pick computationally efficient MTESs for residual generator design, the system designer can seek additional equations. There are a variety of model options with their own unique benefits and drawbacks. These should be selected judiciously and are discussed briefly here:

- **First-principles relationships** that have not yet been considered may be available if the fault diagnostic system designers have not yet extensively modeled the plant. Per the discussion in Chapter 2, these models are useful because they capture the first-order effects of the plant and are extrapolable outside of training data. An example first-principles model that is often used in plant monitoring systems is a state observer such as a Kalman Filter. There are, however, limited choices if the system has already been modeled. These models also may require access to system expertise.
- **Alternative formulations** that describe the physics of the system in different ways may be available. For example, frequency domain models may help to isolate input-output relationships and reduce signal-to-noise ratio [76]. Discretization of the plant

domain might capture spatial resolution for fault detectability that is missing from the model. Alternative formulations are good for increasing the degree of over-determination for variables with existing descriptions. However, they have the same drawbacks as first-principles relationships with respect to limited choice and requirements for system expertise. (i.e. frequency domain, discretization, etc.)

- **Active control algorithms** such as reference trajectories and perturbation signals are another form of physics-based model. They rely on active interrogation and therefore require the operator to "ping" the status of the system but they can supplement understanding of the system and can even be designed to highlight potential faults [53]. They may also leverage methods of filtering confounding sources of error to isolate fault effects. They have the same time and effort investment drawbacks as other physics-based models.

- **Data-driven models** such as empirical correlations derived from experimental data or machine-learning applications may be particularly useful when no obvious first-principles model is available. For example, data-driven models may provide redundant input-output relationships to compare to first-principles models and capture predictable noise and uncertainty. Diverse models may provide relationships between variables for which no other model is obvious, such as for the likelihood of faults occurring based on operational data. As discussed in Chapter 2, data-driven models suffer from their lack of trustworthiness and extrapolability outside of their training data set. They may still provide useful supplementary information as part of the overall structural context but their use in residual generators needs to be demonstrated thoroughly before employing in any safety-related systems.

- **Instrument relations** are the most fundamental tools for supplementing the plant model. They yield near-direct variable measurements and can convert known values to unknown with associated precision and uncertainty constraints. Instrument relations, however, require physical system modifications and can be limited in feasibility due to cost or physical obstacles. Furthermore, each additional instrument is another potential fault source.

There are many models to choose from and the balance appropriate for a given plant will depend on the designer's goals. To complete this chapter, we iterate on our example plant monitoring system by weighing our modeling options in the example below.

Example 3.7 We will go through the model types listed above and determine which are appropriate and feasible for our system. Based on our investigation in Example 3.6, our goal is to obtain isolability for fQ_1, fQ_2, fQ_3, fH_2, and fH_3 with simple equations. Looking at Figure 3.6, we hypothesize that this might be achieved by reducing our reliance on differential and integral solution pathways.

In terms of first-principles models, we have already modeled our plant significantly. It is difficult to consider additional relationships that do not introduce new variables and cause new issues of under-determined equation sets.

Alternative formulations may be available but to use them for a system that we do not operate ourselves would be difficult. These models would likely require further plant information that we do not have available.

Active control algorithms are unavailable because we do not have access to this plant's control system. This means that any kind of inspection signal is not a likely candidate for improving our plant model.

We could potentially develop data-driven models if we had access to a set of training data but the likelihood of that data being available is low and the likelihood it is the data we are interested in is even lower. The type of data available would likely be the same data we already measure, q_0, q_4, and h_1. If we were able to use this data to develop direct relationships between values and their rate of change characteristic of common operation regimes, we could circumvent the need for time-series data in the future. If we develop a relationship between dh_2 and h_2, for example, our new fault signature matrix would be given by Figure 3.11.

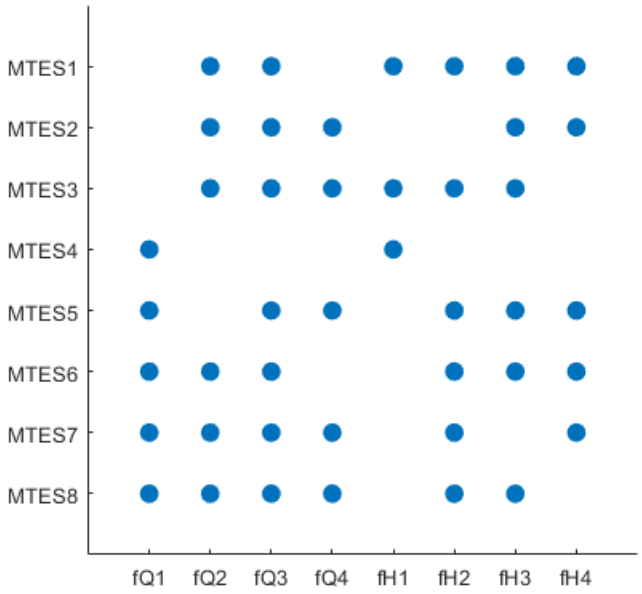

Figure 3.11: Fault signature matrix for computationally efficient MTES in the nuclear bulk material handling system model with supplemental data-driven model

We see now that we have eight unique computationally-efficient residual generators. Some combination of each of these eight residual generators can not only be used to isolate an individual fault, but also to detect multiple simultaneous faults. Research into data-based

models for this plant might be useful in this case, but are likely inappropriate for a class of plants with characteristically small sets of available data.

Most promising and realistic, then, are new instrument relations. Radiation detection may provide us measurements of values we have not yet considered. For example, we may be able to relate new proxy values for flow rate balance into and out of a tank if the change in tank activity is a function of this balance. Figure 3.12 is the fault signature matrix obtained by introducing a measurement that relates to an expression for the flow difference $q_2 - q_3$.

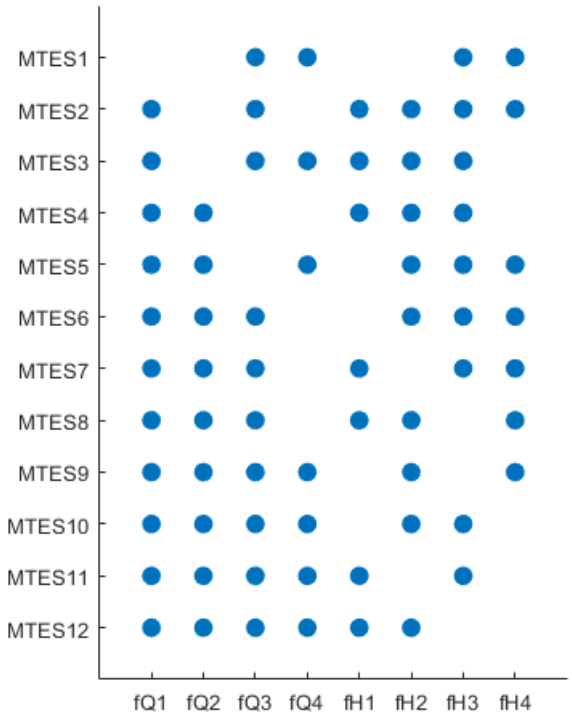

Figure 3.12: Fault signature matrix for computationally efficient MTES in the nuclear bulk material handling system model with supplemental instrumentation model

This additional relation should give our plant monitoring system full fault isolability with some multiple fault isolability (ability to distinguish different combinations of simultaneous faults from one another) as well. The system designer could run studies to determine optimal measurements which is closely related to the sensor placement problem as discussed in [88, 92]. Structural analysis then proves a powerful tool when chances for inspection are limited and optimization is valuable.

This chapter guides the reader through the development stages and considerations key to fault diagnostic system design. Once a plant monitoring system delivers accurate fault diagnostics, it can then empower operators to assess system state and respond accordingly. Fault prognostics and mitigation are the topics of the next chapter.

Chapter 4

Decision support

This chapter builds on Chapter 3's fault diagnostic system design methodology to describe operator decision support via control planning and fault mitigation. It begins with some background and definition of prognostics goals and existing approaches before narrowing scope to short-term plant behavior prognostics due to control actions. The chapter then demonstrates these concepts through application to the bulk material handling facility. Following the discussion on prognostics and decision support, this chapter describes the steps for formulating fault mitigation maneuvers as optimization problems. Finally, it demonstrates a fault mitigation policy applied to the example facility.

4.1 Fault prognostics

As introduced in Chapter 1, the function of prognostics is to predict plant behavior. Fault prognostics, then, is the prediction of plant behavior in the presence of a fault and its consequences. Diagnostics are concerned with assessing plant health at a given time while prognostics are concerned with projecting plant health assessments into the future. Diagnostic tools seek to identify the true state of a plant while prognostic tools seek to predict likely plant trajectories. The field of fault prognostics inherently relies on data for understanding failure mechanisms and generating failure probabilities. The modern revolution in data accessibility and collection has spurred increasing interest in new prognostics research [97]. The goals, however, largely remain the same.

Goals The goals of fault prognostics research are typically to determine remaining useful life (RUL) and probability of failure (POF) for the component, system, or plant of interest. These metrics essentially serve the same purpose except that RUL estimates remaining operation time for a target component and POF provides an instantaneous metric for risk assessment. Both RUL and POF support operations strategies that incorporate expected failure rate and behavior into inspection and maintenance practices. This information is the

focus of reliability engineering. If plant owners and operators have reliability estimates for their components, they can plan for failures and even avoid them altogether.

Anticipating component degradation and failure supports a variety of management goals including those related to safety, plant performance, and component maintainability. Once the reliability of individual components has been characterized, the impact of their reliability on the overall system reliability can also be studied. This system-level thinking began in the 1960s and grew in application to larger, more complex systems in the 1970s [98]. Reliability in the commercial sector led to businesses defining tangible relationships between prognostics and profits.

As techniques for reliability have matured, the range of reliability goals has expanded. Modern reliability studies question *why* things fail and aim to identify the interdependent consequences of their failure. Decades of study have informed reliability-based design practices. Engineers now measure and test reliability in design, operation, and management. Finally, fault diagnosis and prognosis facilitates reliability management throughout operation [98]. As the quantity and diversity of goals and applications for prognostics has grown, so too have the approaches.

Approaches Historically, prognostics has been based on collections of population time-to-failure data from representative components to generate standard failure rates and probabilities [98]. For units that are well-represented in historic data, this approach may work very well. Research in this area has been primarily focused on sophisticated data analysis techniques. Plants today continue to collect historic reliability data and have the tools to do so with higher detail and fidelity than ever before [99]. Moving forward, researchers are seeking methods for improving the practice to better accommodate failure cause identification, reliability-based design, and unique plant-to-plant and component-to-component variability.

Approaches to modern prognostics, as in diagnostics, can be separated into data-based and physics-based methods [100]. For both approaches, the goal is to reduce the need for historic information by developing degradation predictions while relaxing input data quantity and depth requirements. One way this can be accomplished is by simulating population data for degradation and failure used in model formulation [99]. Another way is by simulating environment or component-specific failure to develop unique reliability prognostics [97]. Of course, researchers may even attempt to do both at the same time [101].

Rather than relying on historic datasets, this dissertation focuses on physics-based models and design-phase plant monitoring system development. For advanced nuclear power plants and other first-of-a-kind plants, there may be components with degradation and failure modes that have not yet been characterized. For these reasons, the prognostics focus of this chapter is on what information is built into fault diagnostics models and how they can be applied to prognostics tools in the plant design phase.

Design phase One strength of structural fault diagnostics models is that faults can be detected, isolated, and characterized simultaneously. Residuals yield signals not only that

faults are active, but also that indicate their magnitudes. Furthermore, because fault variables have descriptions inside the plant model itself, the prognostics questions of current degradation extent and impact on system level operation can be readily addressed. If residual generators have well-characterized uncertainty and error, once a fault occurs, the fault's value can be incorporated into the plant model for plant trajectory predictions.

Lithium ion battery health researchers have focused significantly on physics-based models to formulate observers that estimate prognostic parameters like state of charge and, consequently, remaining useful life [102]. This chapter, however, targets simple simulation of existing model equations, formulated during the fault diagnostics design process, to obtain reliability-relevant outputs. Unlike fault diagnostics, design-phase fault prognostics requires careful consideration of representative degradation states and behavior of interest on a case-by-case basis. A rigorous standard approach to this is to conduct a Failure Mode and Effects Analysis (FMEA). In this exercise, an expert panel brainstorms the different ways in which a component, system, or plant might fail and the corresponding effects. FMEAs are structured exercises using worksheets and can be used to determine risk priority numbers (RPNs) based on the occurrence, severity, and detection probability of each failure mode. It is important to note widely-discussed shortcomings of FMEAs such as the difficulty accounting for qualitative differences between failure modes with the same mathematical RPNs and the best treatment of interdependencies between failure modes [103]. FMEAs provide a very good starting point before experimental data has been collected.

Without well-characterized degradation models, it is difficult to select plant state trajectories to estimate long-term future behavior. Decision support systems go one step further — they seek to leverage predictions of future plant behavior to inform current operator actions. Approaches to decision support rely heavily on expert knowledge and probabilistic models to make informed projections of plant state evolution. Decision support system approaches can be found in the information technology [104], naval [105], and aviation [106] industries among others. In the nuclear industry, probabilistic risk assessment leads to event tree or fault tree analyses that prescribe probabilities for pre-determined progressions of events. However, due to the fact that it is difficult to convert historic failure data into failure probabilities relevant to the specific plant and environment of interest, researchers are currently developing a variety of dynamic probabilistic risk assessment approaches [107–109].

In the absence of degradation models such as those given by historical data or otherwise empirically formulated as for battery capacity in [102], definition of degradation variables and their thresholds will be a focus of the design problem. In short, fault prognostics requires definition of dependent and independent variables. Prognostics variables may not be the same as fault variables. For example, the operator may be most concerned with maximum core outlet temperature even though it is useful to also understand the trajectory of a fault affecting the core. Once the designer has specified prognostics variables of interest, the preceding fault diagnostics work provides the essential information required to estimate their trajectories. To provide decision support to operators in the face of faults, the equations used to sequentially generate residual values can also be used to estimate state trajectories. The equation can take possible control inputs that the operator would like to test and simulate

corresponding projected outputs. In real-time applications, the equation set takes in real-time data and projects some time horizon into the future. This type of decision support tool can then be used by the operator to predict plant behavior in response to planned control routines, even if the presence of faults makes them question their conceptual model of the plant's response. As the development process continues through experimental iterations, a new set of historic data will be produced that not only facilitates statistical analysis for application to prototypical systems, but also that tests the accuracy of plant models. By injecting fault prognostics and decision support design strategies into the plant monitoring system development during the design phase, tailor-made RUL and dynamic fault threshold definitions will become available.

To summarize the decision support strategy:

1. Identify failure modes and effects using a structured study such as an FMEA
2. Use identified failure modes and effects to select primary prognostics variables of interest
3. Relate the variables of interest and possible operator control actions to states in the fault diagnostic models
4. Choose operator input trajectories and simulate using sequential model calculations to obtain unknown variables and fault variables due to operator input
5. Determine impact of predicted trajectory on plant state and failure probabilities

For illustration, this chapter presents a case of operator decision support strategy design in the bulk material handling facility. The following example picks up where Example 3.7 left off.

Example 4.1 The first step in formulating a decision support approach for our bulk material handling facility example is to identify a specific failure mode and corresponding effect that we would like to understand and predict. Because we already identified eight possible failure signals in Example 3.3, we can select a failure mode that might be detected by one of those signals. So far, we have not talked about operating the facility. For the sake of demonstrating operator decision support, take e_{13} to be an input rather than a measurement:

$$e_{13} : u = q_0 \tag{4.1}$$

We consider the case of a leak in Tank 1 that we can detect and isolate as a fault in the height dynamics of Tank 1, fH_1. From our work in Example 3.5, we have three computationally-efficient residual generators, r_4, r_5, and r_8, corresponding to MTES4, 5, and 8, respectively. We detect fH_1 when r_4 and r_8 yield similar values but r_5 does not, as

shown in Figure 3.10. If we choose the redundant equation in our residual generator to be e_5, we have

$$r_5 = r_8 = fH_1 \tag{4.2}$$

in an ideal case with zero uncertainty, noise, and/or model error. In the event that we have well-characterized uncertainty, noise, or model error in r_5 and r_8, we can add additional terms to (4.2) to separate the true value of fH_1 from confounding effects. The more signals we have for a fault, the better we can build confidence in our calculated value.

Now, imagine that the facility's plant monitoring system notifies the facility operator of the fault fH_1. Assuming the fault is relatively small and the operator is allowed to continue operating in this case, the operator may still wish to maintain a constant outlet flow of q_4. This is therefore our primary prognostic variable of interest. Intuitively, reduced height in Tank 1 will slow the pressure-driven flow throughout the rest of the facility and ultimately reduce q_4. If the operator's only control is inlet flow q_0, they will then want to compensate accordingly. However, the relationship between q_0 and q_4 is not immediately obvious. Therefore, a decision support tool could allow the operator to "test drive" a control action before taking it to confirm the desired outcome. The equation set used by the other residual generator, r_5, sequentially computes many unknown variable values each time step. It takes control input q_0, measurement h_1, and previous estimates of the heights of Tanks 1-3, $h_1(t-1)$; $h_2(t-1)$; and $h_3(t-1)$, and calculates an expected value for q_4. By modifying e_5 with the known value of fH_1, the resulting calculation should incorporate the faulted plant state into the projected plant behavior. The flow diagram for estimating the resulting q_4 for control input u in this way is shown in Figure 4.1.

Note that this control response estimation algorithm relies on previous time step estimates for the heights of Tanks 1-3 in order to calculate the derivatives of each, $\dot{h}_1$, $\dot{h}_2$, and $\dot{h}_3$, during each iteration. The algorithm then uses these derivative estimates to project next-time-step values of other variables as shown in Figure 4.1. The error introduced by this algorithm, assuming that residual generators come from a reasonable plant model, should be small for the calculation of response to an instantaneous control input. If the decision support tool designer wishes to allow the operator to project several time steps into the future, however, this error will grow and propagate with each additional projected step into the future. In future work, guidelines for estimated state trajectories to guide the simulation would facilitate reliable estimates but would necessarily incorporate probabilistic models to show the operator a projected operating envelope rather than a specific value for the output variable.

Providing operators with a decision support tool that allows them to check the impact of their control actions before taking them, especially during a transient or faulted situation, may prove invaluable for avoiding operation mistakes related to a misunderstanding of plant state. The operator may rely on different indications to assess plant state than those used in the internal calculation of control response. Furthermore, a model-based algorithm like

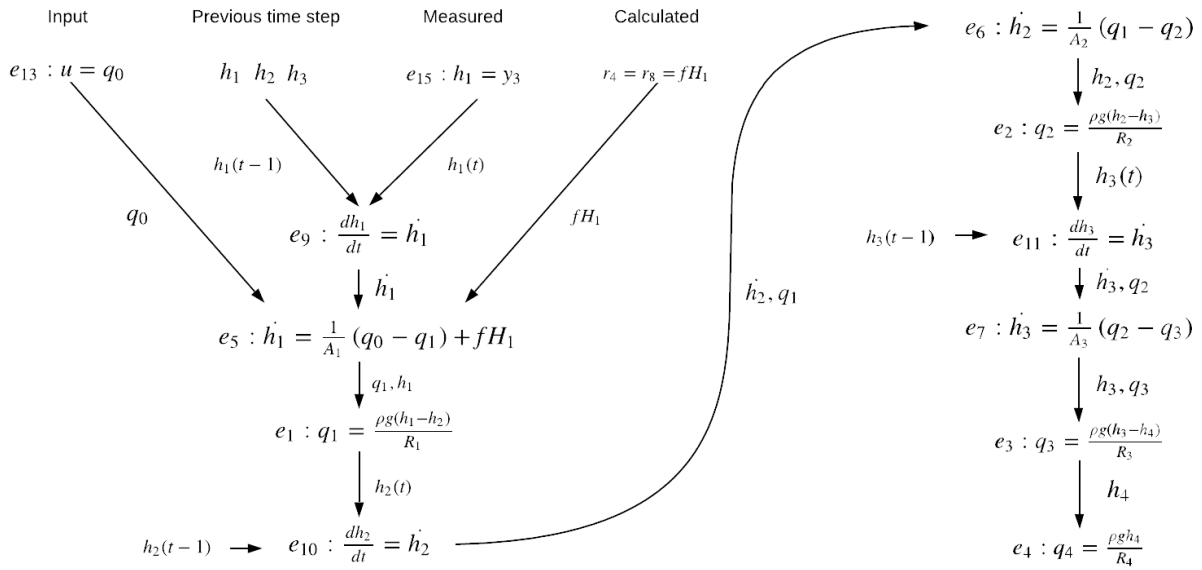

Figure 4.1: Decision support calculation flow diagram for Example 4.1

the one shown in Figure 4.1 reflects the current plant state rather than one predetermined in written procedures, meaning that it provides the operator a vital ally in unexpected situations. Projected values of different plant variables in response to control inputs could be checked against operating thresholds before they would actually be exceeded. After the Tohuku earthquake and resulting tsunami struck Japan in 2011, operators at the Fukushima Daiichi nuclear power plant took many control actions in an attempt to maintain reactor core cooling. They operated safety relief valves and isolation condensers and rerouted flow to manipulate temperatures, water inventories, and pressures. In some cases, the post-accident analysis shows that operators may have misunderstood the plant situation or left the plant in a compromised state due to controls becoming stuck in disadvantageous positions when the plant lost power [110]. In the crucial moments before losing power, a decision support system might have assisted them in confirming their conceptual model of the impact of their control actions before taking them.

4.2 Mitigation

Fault mitigation is the action, if necessary, that should be taken to compensate for the impact of diagnosed faults while optimizing plant operation for performance goals. Fault mitigation is therefore a balancing act between maintaining plant reliability, delivering performance outputs, and adhering to safety constraints. If the control maneuvers needed during fault-free operation are well-defined, the problem of fault mitigation is then concerned with informing

control maneuvers specific to the impact of faults. This section describes the logical way that fault diagnostics and prognostics results can be incorporated into fault mitigation strategies. Specifically, this section focuses on mitigating actions to be taken in the form of optimal control, or input, actuations.

Objective function To formulate an optimal control problem, the first step is to define an objective function. Optimization algorithms seek to minimize objective functions and the designer must therefore choose an objective function that can be calculated and minimized subject to plant constraints.

The objective function actually serves as a "loose constraint". This means that it does not need to be strictly satisfied, but that its minimum can be approached by the optimal input. The constraints of the optimization problem, however, must be preserved. For a plant monitoring system, this chapter asserts that fault mitigation should optimize an objective function describing performance metrics while preserving constraints for safety and reliability. Because the fault diagnostics and prognostics design process provides real-time descriptions of plant dynamics and identified faults, the optimization problem solved in real-time can ensure both safer and better-performing control inputs than through pre-determined operating policies.

The objective function should target a specific design goal or plant issue such as the primary prognostics variables of interest determined in an FMEA. If the decision support tool already describes the plant trajectory and allows it to be compared to defined failure thresholds, fault mitigation should correct the plant trajectory to ensure it does not reach those thresholds. Model-based mitigation routines are therefore fault-specific and rely on formulated plant models just like the control decision support algorithm in Figure 4.1. For example, mitigation of a fault affecting control algorithms may involve compensatory control actuation. Mitigation of a fault affecting instrument readings may involve pre-conditioning readings with correction factors. Sometimes, mitigation may not be possible and it is important to recognize that a safety constraint will be violated without emergency action. Practically speaking, the fault mitigation objective function and set of constraints can follow directly from previous sections and draw on available information.

Optimization problem The optimization problem for minimizing the value of objective function $f(x)$ is

$$\begin{aligned} \min_{u \in U} \quad & f(x) \\ \text{s.t.} \quad & g_i(x) \leq 0, \;\; i = 1,...,m \\ & h_j(x) = 0, \;\; j = 1,...,p \\ & x \in X, \, u \in U \end{aligned} \tag{4.3}$$

where the objective function $f(x)$ should have a lower bound and the constraint sets $g(x) \leq 0$ and $h(x) = 0$ represent inequality and equality constraints, respectively. As described above,

the objective function should describe some performance goal with a value defined by state x dynamics in the set of states X and control inputs u in the set of controls U while the constraints represent limits on safety, reliability, state dynamics, and available control actions. Objective function and constraint definition relies on the plant goals and operating regime and are an important design-phase exercise. The following example can illustrate the methodology through an example fault mitigation case.

Example 4.2 From Example 4.1, we are most concerned with our outlet flow rate q_4. The operator's control input is q_0. Even in the case of normal operation, the operator may need to make periodic adjustments to q_0 in order to obtain the target value of q_4, defined as $\hat{q}_4$. It is likely, then, that the operator has some threshold offset from $\hat{q}_4$, δ, that must be exceeded before the COSS notifies the operator. Ideally, the operator would be able to avoid ever initiating this notification by minimizing the distance between q_4 and $\hat{q}_4$. Our objective function is therefore:

$$\left|\hat{q}_4 - q_4\right| \tag{4.4}$$

For this problem our control variable, u, is bounded by operating constraints on q_0. This means the optimal control action delivered by this optimization problem will never be infinite. Our problem is then constrained by its physical configuration via the plant model and available control actions. If we add the additional safety constraint of keeping the outlet flow q_4 from exceeding a maximum value Q_4, we get the following optimization problem:

$$\begin{aligned} \min_{u \in U} \quad & \left|q_4 - q_4\right| \\ \text{s.t.} \quad & \hat{q}_4 < Q_4 \\ & \text{plant model} \\ & x \in X,\, u \in U \end{aligned} \tag{4.5}$$

where the optimal control value u at each timestep gives the operator a suggestion for their control input q_0. By including the entire plant model in our optimization problem, we are looking for the consequences of all possible faults rather than one specific fault such as fH_1. The calculated u may differ for a different objective, such as optimizing the offset from a target value of q_3 or h_2. The decision support tool designer may wish to allow the operator to choose on which goal to focus or may automate that choice behind the scenes. In any case, the thresholds that cannot be violated should be formulated as constraints. If we have continuous small deviations in faults, the optimization problem yields inputs more relevant to the actual plant status than if we only consider the fault-free plant model. Optimization problems such as the one above can be solved in real-time using algorithms such as the `fmincon` command in MATLAB.

The optimization problem in Example 4.2 is an optimal control problem specific to the bulk material handling facility but the same principles can be applied to any fault mitigation study. From an operations standpoint, certain faults and fault magnitudes may be acceptable. Compensating for them unnecessarily may be detrimental to plant operation. The approach in this section prioritizes a plant's defined performance goals without necessarily "fixing" the fault.

For those interested in optimal control problems that specifically neutralize the impact of faults, Jung et. al. propose a sensitivity dynamics approach in [53]. Sensitivity dynamics models are excellent tools for plants with well-characterized uncertainty and small numbers of equations but can quickly become prohibitively time-consuming to formulate for industrial-scale plants without experimental study. For the purposes of design-phase development, this chapter suggests the above approach as plant designers explore operational priorities and inform the specification of control strategies. It is likely that some faults inspire multiple competing objective functions and, for systems that require operator decision-making, design-phase experiments are an excellent opportunity to study how operators balance priorities in their control decisions. If the different options are formulated as above, the operator can take advantage of fault prognostics and mitigation tools to test their options rather than to guess at the outcome.

Chapter 5

System description

5.1 Description of the Mark 1 PB-FHR

This chapter focuses in on a specific advanced nuclear reactor design, the Mark 1 Pebble Bed Fluoride-salt-cooled High-temperature Reactor (Mk1). This reactor design has been used as a reference FHR design for research in the Thermal Hydraulics Laboratory in the University of California, Berkeley Nuclear Engineering Department since 2014 [78]. First, this chapter will introduce the Mk1 and describe its key unique features before describing its basic design, safety case, and control system functions. Then, this chapter will describe the experimental thermal hydraulics facility, the Compact Integral Effects Test (CIET), that researchers at Berkeley use to study the Mk1. Finally, this chapter will describe the Advanced Reactor Control and Operations facility (ARCO) connected to CIET and used to study operational strategies and plant monitoring systems for the Mk1.

The Thermal Hydraulics Laboratory at Berkeley is continuing the development of test programs for performing design and safety analysis of fluoride-salt-cooled high-temperature reactors (FHRs). Specifically, Berkeley researchers focus on the prototypical Mark 1 Pebble Bed FHR designed in 2014 [78] as an evolution of the 2008 Pebble Bed Advanced High Temperature Reactor design [111]. The Mk1 is a 236 megawatt thermal, 100 megawatt electric small modular nuclear reactor that uses pebble fuel, solid graphite moderator, and fluoride salt coolant. Compared to other FHRs, it uniquely features a power conversion system that drives a nuclear air-Brayton combined cycle (NACC) for base-load electricity generation [71]. The NACC can co-fire using natural gas or other combustible fluids to provide peaking power up to 240 megawatts electric. The Mk1 design aims to simplify nuclear power plants as compared to existing light water reactors but it also features unique new technologies that must be developed and demonstrated. A schematic of the Mk1 design and flow paths is shown in Figure 5.1.

Advanced reactor technologies The main technologies unique to FHRs are high-temperature coated-particle fuel and cooling by the fluoride-salt flibe ($^7Li_2BeF_4$). The Mk1 then further

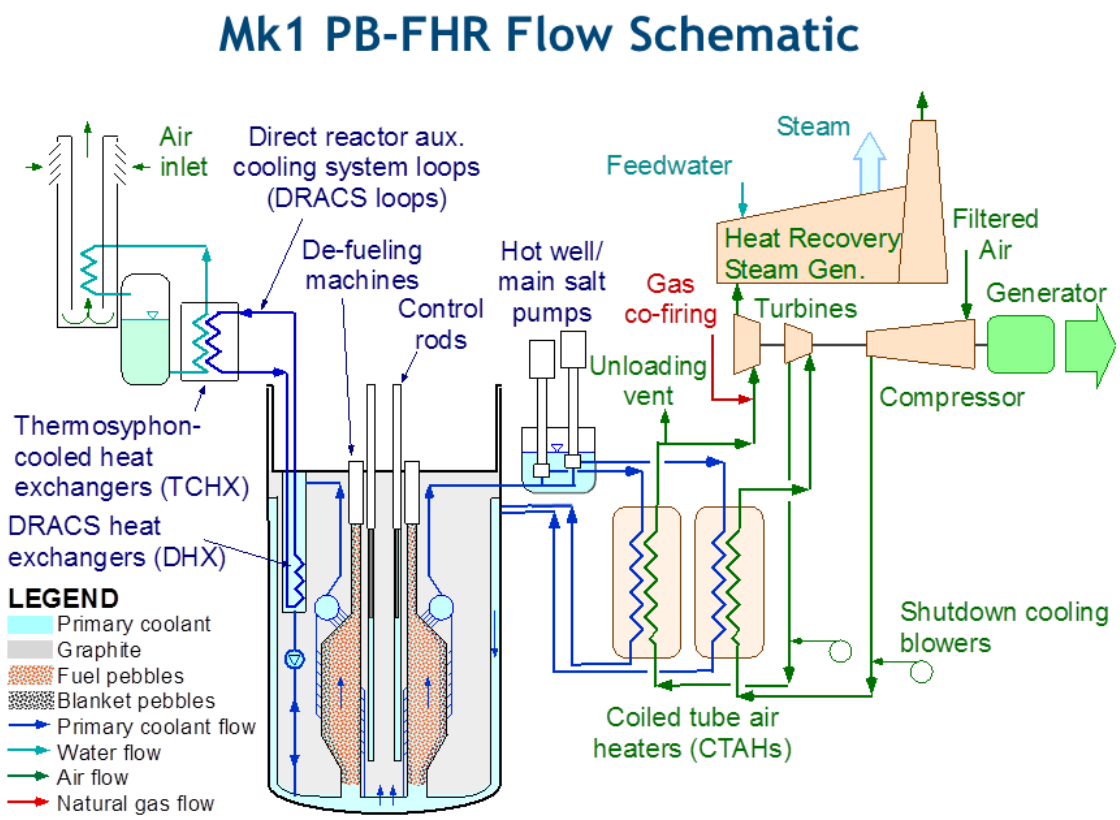

Figure 5.1: Mk1 flow schematic

implements the NACC cycle, modular construction, and no intermediate coolant loop between the primary and power conversion fluid.

The Mk1 fuel pebbles, pictured in Figure 5.2, contain coated uranium particles embedded in an annular layer with an outer high-density graphite coating and an inner low-density graphite core. Four of these fuel pebbles produce approximately enough electricity to last a year for an average U.S. household from 2011 [78].

Flibe is the fluoride salt employed by the Mk1 because it has the lowest possible parasitic neutron capture of all fluoride salts, enabling negative coolant void reactivity feedback. These features essentially mean that flibe's properties contribute to stable as-designed power output. Fluoride salts in general have a number of desirable characteristics including high volumetric heat capacity, low chemical reactivity with air and water, low volatility at high temperature, effective natural circulation heat transfer, and retention of most fission products.

The NACC allows the FHR to operate at different power outputs so that it can accom-

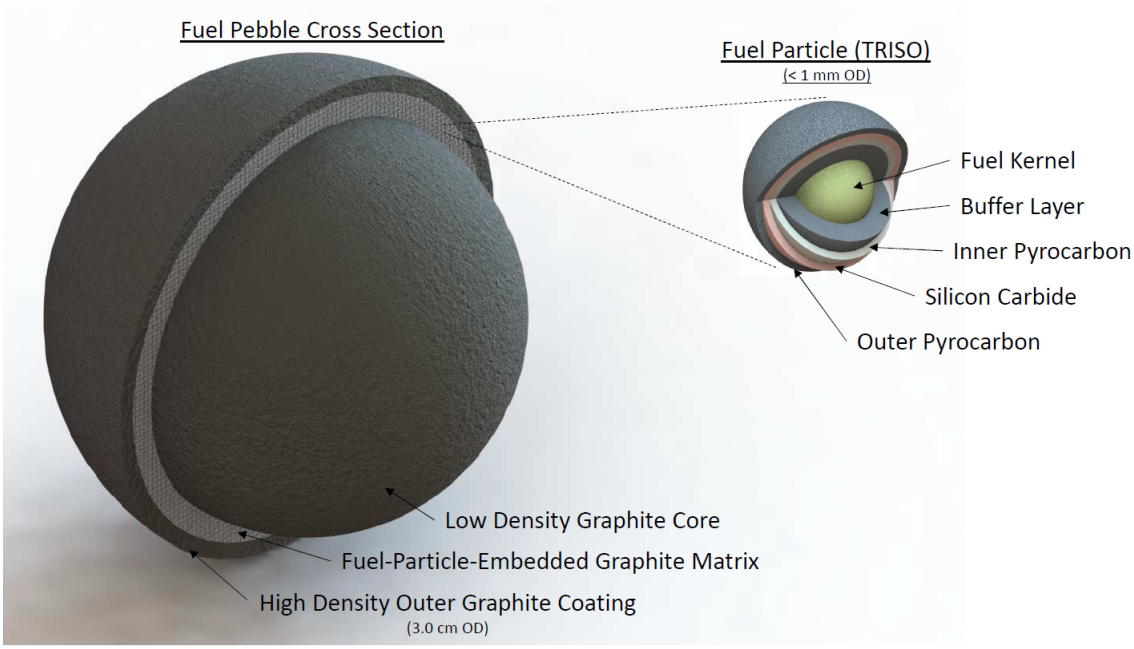

Figure 5.2: Mk1 fuel diagram

modate both baseload steady-state power generation and rapid power ramping. This is an important advantage of the Mk1 as compared to other nuclear power plants and other power plants in general: it produces carbon-free baseload energy and uses natural gas to ramp with higher efficiency than even natural gas plants themselves [78].

The Mk1 uses components that can be constructed from modular sections and transported by rail. The reference Mk1 configuration consists of 12 reactors and is designed for economies of scale and standardization so that the construction process is both repetitive and repeatable.

While these advanced reactor technologies contribute to the Mk1's value proposition as an electricity generating facility, the Mk1 also has a strong safety case. The Mk1 design incorporates a set of passive safety features and mechanisms that minimize conceivable safety issues over its operating lifetime.

Passive safety features The Mk1 has passive safety by design through its coolant, fuel, and materials selection. Intrinsic negative reactivity feedback in the reactor comes from negative fuel, moderator, and coolant temperature reactivity feedback. While the reactor operates at 600°-700°C, its coolant and fuel have significant thermal margins to damage. Flibe boils at 1430°C and the Mk1 coated particle fuel has a thermal limit of over 1600°C [112]. In fact, the most significant concern about coolant temperatures comes from its high freezing temperature of 459°C. Overcooling is therefore a potential issue that must be mitigated. The substantial thermal inertia of the Mk1, however, ensures that overcooling

phenomena evolve slowly. Flibe also protects the fuel pebbles from chemical attack by air.

The Mk1 also incorporates passive safety through structural, mechanical, and thermal-hydraulic systems. Buoyant control rods supply normal reactivity control but also insert passively into the core if the coolant temperature in the control rod channel exceeds their buoyant stability limit of 615°C. If electrical power is lost, magnetic latches for the control rods and shutdown blades disengage, causing the control elements to drop into the core and effectively shut down the reactor. Emergency heat removal from the core is completely passive using a check valve that allows primary loop natural circulation to transfer heat to the Direct Reactor Auxiliary Cooling System (DRACS) containing Thermosyphon-Cooled Heat Exchangers (TCHXs) if the primary pump stops and forced circulation is lost. The thermosyphons in the TCHX receive water through fail-open valves that can be used to regulate potential overcooling if the reactor is shut down for long periods of time. These emergency heat removal systems can also be supplemented with the power conversion system and normal shutdown cooling.

The primary water pools for the Mk1 have their own tank-within-tank secondary confinement. This configuration has its own leakage detection that can limit inventory loss without safety function compromise even in the presence of leaks. These pools supply water to the TCHXs and the reactor cavity liner cooling system. The Mk1 also has a "gas gap" system at each free surface and vessel penetration to make the transmission of excessive pressures to the reactor vessel and cavity/containment from tube or manifold ruptures in the primary heat exchanger physically impossible.

Electrical and I&C Systems The Mk1 maintains constant core inlet and outlet temperatures during normal operation and uses air bypass flow or turbine inlet temperature control for load following. The pump controls primary flow rate to maintain core temperature drop and the control rods control average core temperature. Additionally, the pebble handling system controls fuel loading and unloading to allow for rapid power reduction of up to 60% from full power.

Because the Mk1 coolant and fuel have such significant thermal margins to damage compared to normal operation, the design purpose for reactor trip functions are to limit acute and long-term thermal transients in the metallic primary loop structures. Important sensors for safety functions include power range neutron flux, primary coolant temperature, primary coolant level and inventory, and primary coolant flow rate.

The Mk1 design includes an emphasis on online monitoring and plant health optimization although the design for such a system has not yet been defined. The design report states that "effective component health and performance monitoring to permit maintenance prior to catastrophic degradation is...highly important to successful commercial deployment" [78]. Outside of the adoption of wireless instrumentation, there is no further specification for online monitoring and plant health optimization for the Mk1. Strategies presented in this dissertation could help to fill this gap.

5.2 The Compact Integral Effects Test

Integral effects test (IET) experiments can aid in the formulation and validation of theoretical models for a nuclear power plant design to support its safety case, operational considerations, and prototypical design choices. The Compact Integral Effects Test (CIET) was designed to support the verification and validation of thermal hydraulic system codes [113]. It has provided actual data as a scaled facility representing the Mk1 design for steady-state power operation, passive heat removal during shutdown [114], transient behavior, and even for the study of online inspection methods like frequency response testing [76, 115].

Description of the CIET Facility CIET consists of two coupled flow loops that replicate the integral thermal hydraulic response of FHRs using DRACS under forced and natural circulation at a scaled height and reduced flow area [113]. By using Dowtherm A heating oil as a simulant fluid for the prototypical FHR coolant, flibe ($^7Li_2BeF_4$), this scaling can simulate prototypical FHR performance at significantly reduced temperatures [116]. Figure 5.3 shows a 3-D model of CIET. CIET replicates the two major flow paths in a prototypical FHR: the natural circulation DRACS loop and the forced circulation primary loop. The primary loop heat structures are a vertical heated section, the shell side of a vertical single-pass straight shell-and-tube DRACS heat exchanger (DHX), and a variable speed fan-driven air-to-oil heat exchanger used to simulate the coiled-tube air heat exchanger (CTAH). The DRACS loop has the tube side of the DHX and a TCHX.

Mechanical Systems The structural materials in the primary loop of CIET include thin wall (Schedule 10) 304L stainless steel piping, as well as more weakly coupled thermal structures such as flanges and valves. The heater section provides power though copper electrodes that are connected to its outer tube from DC power supplies operating between 0 and 10 kW and controlled through a LabVIEW interface. All of the primary loop, excluding the CTAH, has 5-cm-thick fiberglass insulation to limit heat losses to ambient air. Researchers inspected the insulation for parasitic heat losses under steady-state operation using an infrared camera and added additional local insulation to reduce localized heat loss. Each loop accommodates volumetric expansion of the fluid using expansion tanks maintained at atmospheric pressure and installed at the uppermost elevation.

Control and Data Acquisition Control of heater power input is accomplished using a LabVIEW control system. The temperatures and mass flow rates in each loop are recorded with a National Instruments data acquisition (DAQ) system [113]. Pressure data throughout the loop can be directly measured with manometers and digital cameras, devices more difficult to implement at flibe operating temperatures. All data is displayed on interfaces in LabVIEW front panels. The experimenters also control CIET using the front panel via digital buttons and input fields. Here the experimenters have control over the heater, the pump, the CTAH fan, and the TCHX fan by specifying set points or frequencies. Both the

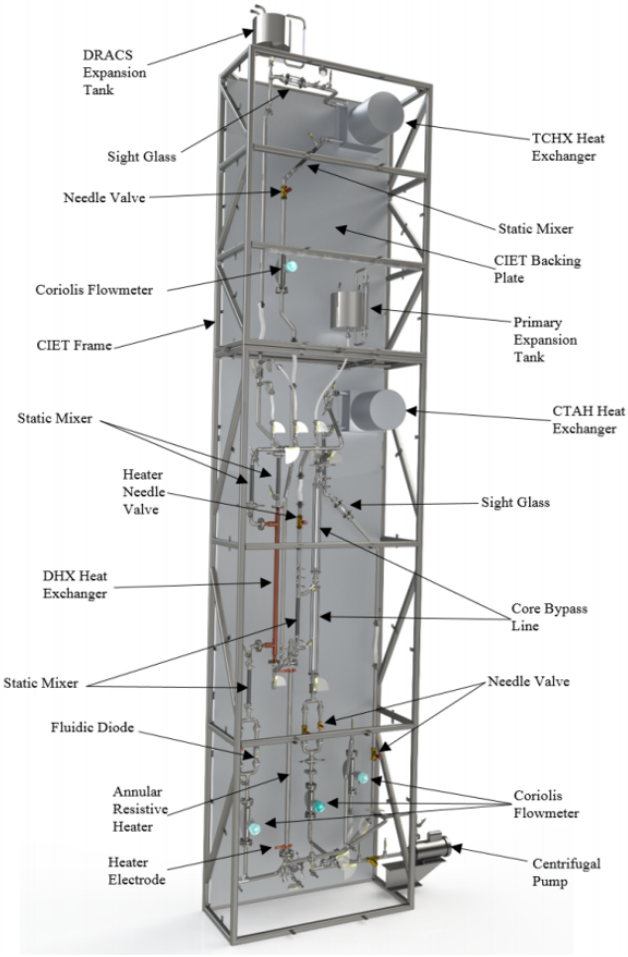

Figure 5.3: CIET SolidWorks model

TCHX and the CTAH are computer-controlled, variable-speed fan-cooled air-to-oil heat exchangers. TCHX and CTAH outlet temperatures may be controlled to desired values using PID controllers.

The heater control was designed to produce steady-state output signals with step changes from one steady-state power level to another. This control capability was expanded to include the ability to output sinusoidal signals with the operator controlling the offset, amplitude, and frequency of the sinusoid. The digital-to-analog conversion of the output signal from the control system to the analog power input signal to the system heater has shown to be fairly coarse, which further limits output signal frequencies. Therefore, researchers have also added the capability to switch the power supplies to direct analog control for frequency response studies.

Instrumentation Temperatures in CIET are measured with type-T inline thermocouples with 0.5-mm-diameter sheaths and ungrounded junctions in direct contact with the Dowtherm A coolant, providing very rapid thermal response. Their accuracy is $\pm 0.5°C$ in the $0 - 200°C$ range [113]. Thermocouples are located at the inlets and outlets of each heat structure. In order to ensure that the bulk (mixing cup) temperature can be determined, each measurement position has a thermocouple both at the center and near the wall. A thermowell in the loop contains a NIST-calibrated thermistor, which provides an independent measurement of temperature and which can be used to check thermocouple calibration in-situ by running with isothermal conditions. Coriolis flowmeters with accuracies of $\pm 2\%$ over the range of flow rates tested provide direct measurements of mass flow rates [113].

5.3 The Advanced Reactor Control and Operations facility

The Advanced Reactor Control and Operations (ARCO) facility is a digital control room testbed designed to support the development and application of new digital technologies for advanced nuclear power plants, especially as they pertain to the FHR. As shown in Figure 5.4, it consists of three workstations and two displays that support the functionality of a distributed control system and advanced nuclear plant control room. This section describes ARCO's concept of operations and operator roles in the advanced reactor control room. It then describes ARCO's design and the rationale for the selection of its components. Then it details its data communication using the networking protocol OPC UA before discussing experimental capabilities.

Concept of Operations When moving to a new reactor design philosophy, control room designers must consider the concept of operations, or the role of operators in the control room [117]. Existing regulations lay out strict requirements for control room staffing and responsibility [118] but improvements may exist outside of current regulatory constraints. Finding these improvements is an essential requirement to optimally allocate tasks best suited for computers and for people. ARCO provides just three roles for the control room: Supervisor, Reactor operator, and Balance of Plant (BoP) operator. The Supervisor sits at the Supervisor workstation shown in Figure 5.4 and monitors plant status including forthcoming fault detection and cybersecurity systems. The Supervisor's role is to guide operational actions and to coordinate off-normal condition identification, investigation, and mitigation. The actual control actions are the responsibility of the Reactor operator and BoP operator. Aside from their specialization with their respective systems, the Reactor and BoP operators work from the adjacent workstations shown in Figure 5.4.

One further consideration for a digital control room concept of operations is the communication policy – necessarily different from the verbal three-way communication and continual standing and movement in current analog control rooms [69]. To successfully address the

Figure 5.4: Labeled photo of the ARCO facility in its current configuration

need for a new communication system, ARCO must support situation awareness for each operator and also for the group of operators. This means not only that each operator understands information pertinent to their individual tasks, but also that they understand information pertinent to others' tasks and the plant situation overall. To this end, tools that foster clear communication and enable efficient information sharing between operators are essential. ARCO makes additional provisions for communication through its physical design.

Layout and technology selection Originally, a single utilitarian computer was used to control CIET for thermal-hydraulic experiments, changing with each new desired capability and designed more for obtaining the results needed immediately than for refining an intuitive and usable interface. The original workstation, now expanded and distributed across multiple workstations and displays, still maintains that legacy functionality in addition to new features. Now ARCO can further develop the details governing relationships between operator roles and system response.

One significant advantage of digital control rooms over analog ones is that designers have the chance to develop individual capabilities as software rather than as hardware. Software is much more flexible and amenable to change. This also means that digital control room hardware resembles hardware for any office space – computers and displays. The selection of components for ARCO prioritizes features that enable the deployment of these software tools and their use by operators.

The main parameters that support human-machine interface (HMI) goals are display resolution and size, processing power and memory, and input method support. ARCO's displays optimize legibility following discussions in [65]. Modern workstations with touch and pen input open the possibility of studying human-machine interface technologies that are impossible to employ in analog control rooms.

The Reactor and BoP operator actuate and manipulate the control system while the Supervisor uses the workstation to observe and share information with the rest of the control room. The Overview displays show coordinating information to facilitate control room communication [68]. They show the entire plant, consisting of both reactor and power conversion system, with the most pertinent indications prominently displayed. This ensures that, at a glance, operators can reinforce the context of their system compared with the plant as a whole. The Overview Displays may also host plant performance information and relevant summaries of online analytics.

The physical locations, orientations, and furniture heights of ARCO facilitate clear line-of-sight for each operator to the Overview Displays from the same angle at which they view their own workstations. The Supervisor can see both the Reactor and BoP operators' workstation displays and the Reactor and BoP operators can also see one another's workstation displays. Further enhancing physical awareness in the open lab space, a convex security mirror above the Overview Displays allows the Supervisor to see activity behind ARCO.

Networking To facilitate distributed control, ARCO uses the OPC UA networking protocol, the emerging standard for Industrial Internet of Things. OPC UA stands for "Open Platform Communications Unified Architecture" and is designed to connect databases, analytic tools, and more [119]. With respect to the Open Systems Interconnection model, OPC UA handles the application, presentation, and session layers so that it can work directly on top of wired or wireless TCP/IP communication [120]. Essentially, this means that OPC UA can easily connect devices without the need for additional configuration between the communication and user endpoints. Its server-client architecture is platform-independent so that desktop computers and proprietary industrial devices can be connected with minimal specialized setup. It supports a variety of data types with minimal need for pre- and post-processing between clients. OPC UA also offers fully-customizable security options even for individual data streams from one source. Finally, it is highly scalable and can handle far more data streams than ARCO could ever generate. However, proving OPC UA's utility with ARCO helps establish its utility for larger and more complex systems. ARCO features a distributed control client-server architecture in which servers handle most calculations and clients pri-

oritize display and interaction characteristics. The Supervisor workstation has substantial computational power and stores most plant data along with supporting high-fidelity calculations. The Reactor and BoP operator workstations act as clients and prioritize aesthetics and screen size. These capabilities closely match operator roles. As shown in Figure 5.5, the Supervisor workstation is the current main server for ARCO while clients for each of the two workstations and the Overview interface with the server, pushing and pulling data continuously. In future iterations, contingency servers on each workstation that duplicate capabilities of the Supervisor server and can be swapped in to maintain functionality in the face of hardware, software, or cybersecurity-based failures.

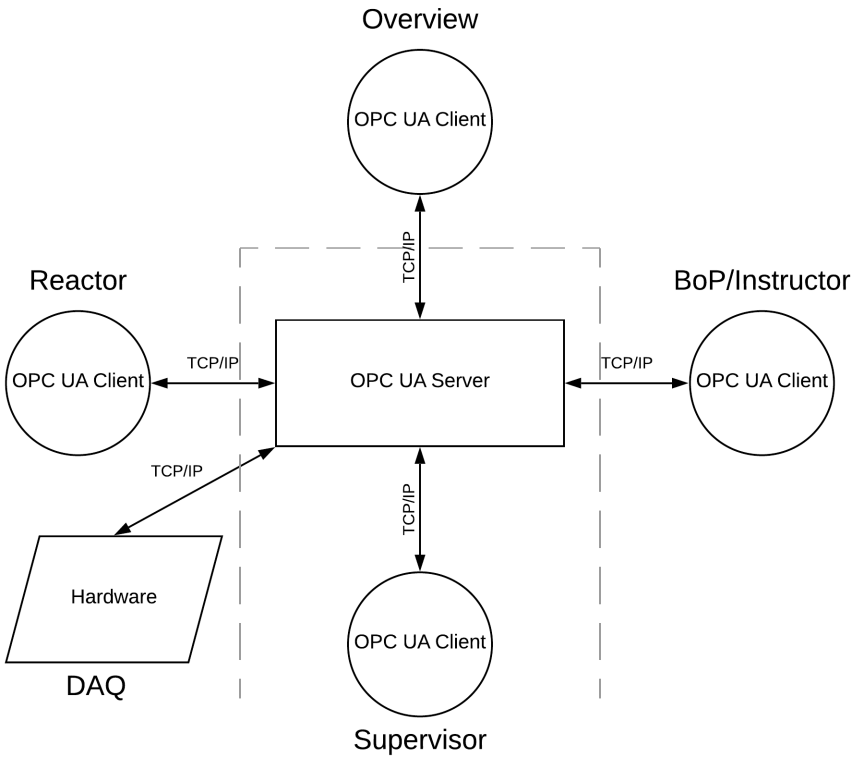

Figure 5.5: Client-server architecture using OPC UA in ARCO

ARCO-CIET Capabilities By controlling CIET from ARCO and simulating plant components that interface with the physical experiment, researchers can operate CIET and ARCO together as an advanced nuclear power plant. The CIET and ARCO facilities in combination form an advanced reactor design and operations test bed to open new topics of research to explore at university laboratories, including concept of operations, cybersecurity,

licensing, and much more. As researchers develop sophisticated models of core neutronic behavior, long-term materials degradation effects, and quantifiable distortion between scaled systems and prototypical ones, those models can be programmed into the control logic of ARCO. Once the operators see the controls of a prototypical system and obtain a prototypical response by actuating them, ARCO-CIET blurs the line between simulation and experiment. Of course, researchers must rigorously work to verify and validate any findings through code-to-code benchmarking and comparison with forthcoming experiments and prototypes. As of June 2019, ARCO interfaces with CIET only through the power removed in the primary heat exchanger by simulating conditions on the power conversion side appropriate to a given load. As the research program moves forward to study faults, transients, and unique occurrences associated with varying initiation events, additional connection points will reveal themselves. Until then, the following sections describe the initial set of scenarios developed using ARCO-CIET.

To fully realize ARCO's potential, researchers need to work diligently to create and improve upon the system. ARCO benefits from an iterative development process, in which it deploys individual systems not in fully polished forms but as proofs of concept. Lessons learned from each test then influence further tests. Of interest are not only plant systems, interfaces, or tools but also the method and experience of operation. Working in a university research facility, students are ARCO-CIET's primary operators and their experiences shape the evolving training process. A variety of different test types with prescribed formats facilitates conclusions, analysis, and comparison. Example test categories include new functionality evaluation, fault detection, cybersecurity, and plant process monitoring and optimization. For each of these categories, there are tests focused on deployment testing for specific tools such as maintenance early warning systems and tests focused on operations experience by monitoring operator use of ARCO.

Chapter 6

Operator support system implementation

This chapter describes design principles and guiding philosophies for Computerized Operator Support System (COSS) development applied to the human-machine interfaces (HMIs) in ARCO. The first section provides a discussion of digital control room technologies in the nuclear industry before focusing on background and fundamental concepts for COSSs along with motivation and opportunities for improvement on nuclear industry standard practice. Then it will describe the inherent connection between plant monitoring systems and COSSs. The second section describes the conceptual development of COSS features in ARCO. The third section details the current state of ARCO including its data signal architecture and HMI design process before concluding with plans for future work.

6.1 Control room background concepts

With new nuclear plant designs, the industry is transitioning to mostly- or fully-digital control rooms. Current nuclear plant control room HMIs are either primarily analog or a mix of both digital and analog where digital components mainly emulate analog appearance and functionality [65]. Change has lagged technology availability due to regulatory and licensing concerns as well as costs resulting from training needs and interruptions to operation [65]. Operators, therefore, perform most actions manually using prescribed logic trees in paper procedure manuals [66, 67, 121]. If system conditions differ from those described in manuals, operators must then go off-script and risk misdiagnosing plant state [66, 68, 121]. Analog systems often require precision or timeliness from operators, such as for grid synchronization [68], leading to periods of heightened risk or vulnerability to human error.

A well-designed control room supports optimized plant control. Digital systems afford a number of benefits as compared to analog systems for this purpose. Analog systems have hardwired control logic, often abstracted from the desired control objective, making them difficult to tune or optimize after installation. Operators may need to change multiple

setpoint controllers in order to achieve a single goal. With digital control, designers can employ sophisticated control and feedback relationships. Furthermore, they can iterate and update control logic without alterations to the physical control system.

Programmatic control routines mitigate human error resulting from operators' inaccurate plant mental models while simultaneously fostering simple and functionally efficient system understanding. Applying modern and efficient algorithms can minimize operating costs, increase the ease and reliability of operation, and decrease system uncertainty. In fact, the structure of existing plant procedures as logic trees makes the move toward control system automation very straightforward. As designers assign routine tasks to a reliable, autonomous system, human operators will be available to perform complex tasks involving critical thinking and decision-making.

Digital systems for data collection and visualization allow advanced nuclear plant control rooms to capitalize on modern technologies. Digital systems can organize, manipulate, and display plant information for operators in intuitive and efficient ways. They allow designers to decouple physical instrumentation and control location from the corresponding display or manipulation point. Designers can organize interfaces logically to support staff's mental models of the system and modify them as further efficiencies reveal themselves. By adopting this approach, designers liberate themselves from strict constraints so that they may draw from modern best practices in user-centered human-machine interface design.

One key area of improvement for digital versus analog displays is data visualization. By presenting operators with flexible data visualization tools that allow for customizable analysis in real-time, designers ensure a powerful level of human-machine understanding. Not only do digital systems support higher-fidelity visualization of the signals available to analog systems, but they also enable designers to give operators access to implied signals and analysis tools such as those provided by virtual sensors and statistical algorithms.

Finally, digital control rooms are well-suited to modern plants that must be flexible actors in electrical grids with high penetration of variable generators, heightened risk of severe weather events, and increased diversity of loads with increased infrastructure electrification. Digital control systems can implement algorithms and logic based on various data sources, including external data such as weather conditions and grid status. That means that plant owners can configure control systems to anticipate and respond optimally to fluctuating energy market conditions. Systems can also supplement the robustness of the plant to transient conditions through the possibility of modification and reassignment of control logic online without operational interruptions or alterations to the physical system. For example, contingency algorithms may activate automatically in the face of valve failure, rather than requiring human operators to explicitly change their control actions.

One of the chief concerns with the move towards digital for critical plant systems is cybersecurity. Digital systems carry with them the weight of persistent threats to use the digital world as a bridge to the physical one [122]. This dissertation asserts that digital control does not need to be avoided entirely but that cybersecurity must be considered in the design phase of nuclear plants. Important cybersecurity design strategies include network segregation, diverse and redundant instrumentation and control, and fault detection systems.

Further detail about the history and challenges associated with cybersecurity in digitalization can be found in [81]. The desire to address cybersecurity concerns arising from digitalization is a primary driver of a digital control room testbed like ARCO.

Computerized operator support systems Advanced instrumentation and control has the ability to introduce additional information streams as compared to existing nuclear plant control rooms: signals calculated from combinations of directly measured values, data presented in human-readable ways, metadata concerning data type and size, and more. This abundance of information, however, means that modern HMIs necessitate information prioritization if they are to avoid overwhelming human operators [123]. As defined by researchers at the Idaho National Laboratory (INL), a Computerized Operator Support System (COSS) is a collection of technologies that assists operators in monitoring overall plant performance and making timely informed decisions on appropriate control actions for projected plant conditions. COSSs may assist in monitoring plant states to detect off-normal conditions, diagnosing plant faults, predicting future plant states, recommending fault mitigation actions based on embedded expert knowledge, and supporting decision-making for selecting appropriate fault mitigation actions [123]. The researchers then give concrete examples of possible COSS features including digital alarm management systems, computer-based procedures, piping and instrumentation diagram system representations, and mitigation action recommender modules.

There are existing COSS-type systems that have been applied to a variety of human-controlled processes. These include [123]

- Traffic Collision Avoidance System (TCAS) to facilitate air traffic control via advisories and aircraft-to-aircraft communication
- Terrain Avoidance and Warning System (TAWS) to warn airplane pilots of proximity to terrain with the help of GPS
- NASA Mission Control Intelligent Flight Support System to assist goal-seeking by conducting what-if analysis and facilitating data visualization using expert information
- Chemical Volume and Control System COSS (CVCS COSS) to demonstrate principles of nuclear COSS applied to a digital HMI in a light water reactor simulator at the Human Systems Simulation Laboratory (HSSL)

There are many possible approaches to support human operators and facilitate human-machine collaboration but these examples each perform calculations and assist reasoning that would otherwise constitute a significant burden on operators' mental workload. Because this dissertation focuses on plant monitoring systems, this chapter focuses on the connection between COSSs and plant monitoring.

COSSs and plant monitoring According to INL researchers, the four categories of operator cognitive processes are [123]:

1. monitoring plant status and detecting plant upsets
2. situation assessment
3. response planning
4. response implementation.

From the tools and techniques described in Chapters 3 and 4, a plant monitoring system can assist with all four of these cognitive processes in order to reduce mental workload, support situation awareness, and facilitate decision-making for operators. Well-designed residual generators continuously monitor plant status, detect plant upsets, and facilitate state assessments through the characterization of both qualitative and quantitative aspects of faults. Operators can then incorporate this information into response planning by testing control actions and implementing mitigation routines as in Chapter 4. What is missing, however, is the method of interaction between the plant monitoring system and the operator. This is where the COSS comes into play. Without a notification system that communicates pertinent plant monitoring information to the operator, the sophisticated algorithms of previous chapters have little use. This chapter describes the approach to this problem, as implemented in ARCO, in the following sections.

6.2 COSS development in ARCO

ARCO affords the opportunity to explore design options for COSSs optimized for advanced nuclear power plants. The control rooms, concepts of operations, and technologies in advanced nuclear power plants are something of a blank slate. Furthermore, they will likely come to fruition in a different regulatory environment than that of nuclear power plants in current operation. ARCO can be used to prototype COSSs for the general set of advanced nuclear power plants. Its first reactor design application, however, is the FHR.

Researchers at INL have published a logical progression of research related to COSSs from both the theoretical and practical perspectives [15, 55, 123–125]. This dissertation leverages the experience and knowledge in their work as applied to light water reactors and seeks to further explore the concepts as applied to advanced nuclear plants. This section starts by introducing a conceptual prototype plant monitoring COSS demonstrated in a light water reactor turbine control system HMI. It then describes the design of a COSS for iterative development in ARCO.

Fault Understanding and Navigation Control Interface The Fault Understanding and Navigation Control Interface (FUNCI), pictured as an embedded component of the Turbine Control System Overview in Figure 6.1, is a proof-of-concept COSS. Licensed nuclear power plant operators went through a series of operating scenarios during a study in August 2017 [124] to become familiar with and offer feedback on the upcoming digital version of their plant's turbine control system (TCS). Some scenarios focused specifically on the addition of FUNCI and its utility to the operators for assessing plant condition and handling faults. This exploratory research sought to qualitatively assess whether FUNCI is helpful, whether its visual affordances are intuitive, and whether modifications might improve the design.

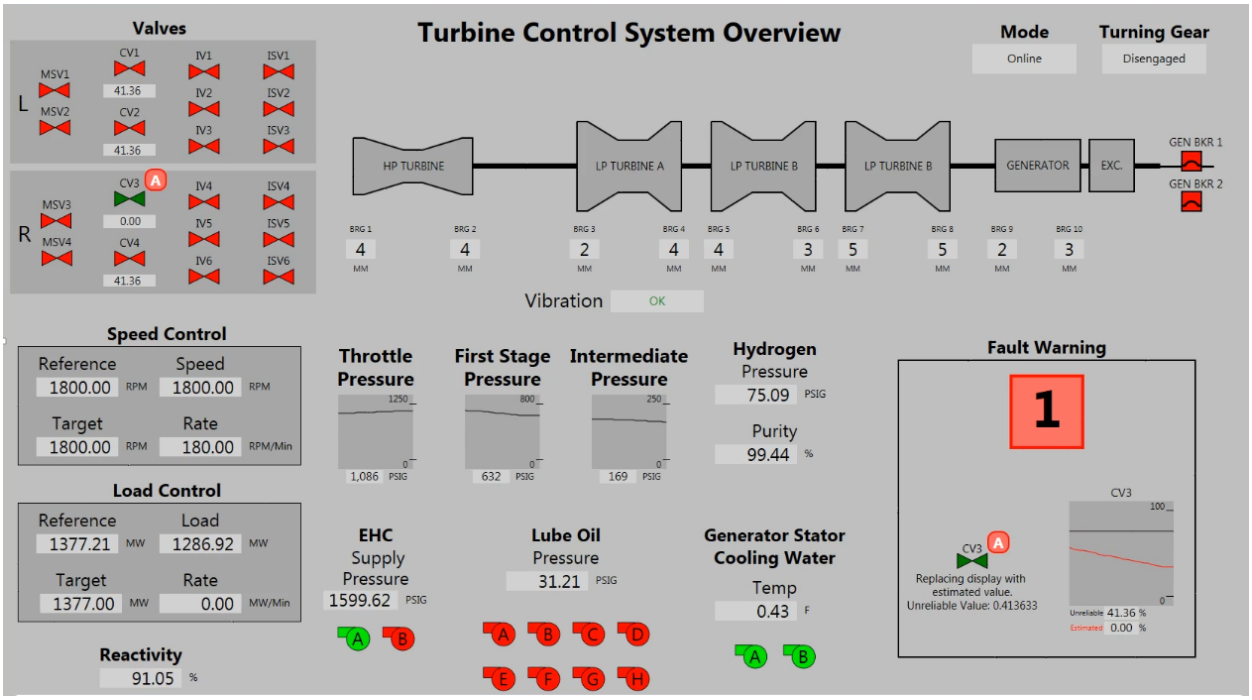

Figure 6.1: Digital Turbine Control System HMI, containing the FUNCI early COSS concept

FUNCI consists of two main sections: a dedicated HMI section (the "Fault Warning" box in the lower right corner of Figure 6.1) and an integrated capability within the context of the existing HMI (the red circle with the letter "A" on valve CV3 in the upper left corner of Figure 6.1). The main concept is that a physics-based plant model checks for consistency between indications and notifies the operator when consistency is not satisfied. The number of inconsistencies shows up in the notification box (the red square with the large number "1") to alert the operator. In order to clearly convey the issue, FUNCI flags the concerning indication both in the context of the HMI and also by replicating the indication inside the Fault Warning box. Then, to ensure trust and to support the operator's conceptual model of the plant and situational awareness, FUNCI explains the inconsistency by giving both the erroneous value and the expected value of the indication, both as instantaneous values

and also as a trend over time. In this iteration, FUNCI also automatically replaces the HMI indications after a few seconds with its calculated value so that the operator has realistic indications to work with.

To test FUNCI, the operators worked through four separate short scenarios using the TCS. The four scenarios were:

1. Turbine shaft vibration (spoof)
2. Power ramp rate surge
3. Control valve fault and spoof (FUNCI with text only)
4. Control valve fault and spoof (FUNCI with text and trend)

Scenario 1 represented a compromise of the HMI without a compromise of the physical plant. FUNCI showed the operators that the indication of bearing vibration was likely non-physical because adjacent bearings showed no signs of vibration. This confirmed suspicions the operators already had that the reading, not the system, was faulty.

Scenario 2 represented a plant trajectory likely to end in a turbine trip. In this case, FUNCI acted as an early warning system to ensure the operators could act with sufficient time to potentially avoid a trip. The operators were first alerted to the issue thanks to FUNCI. While they still decided to trip the turbine, they avoided reaching power conditions necessary for automatic systems to actuate and demonstrated the way COSSs can potentially reduce overall wear and thermal cycling on plant components.

Scenario 3 represented a compromise of the physical behavior of valve CV3 with a simultaneous spoof of its indication to mask the physical fault. The operators did not notice the fault without FUNCI and, in fact, used their analog readings to confirm that FUNCI was telling them the truth that a fault was present. It is worth noting that Scenario 3 had only a text-based explanation and that the operators did not know how FUNCI arrived at its conclusions.

Scenario 4 was the same as Scenario 3 except that FUNCI also provided a trend of the calculated and indicated valve positions' divergence to explain its conclusions. The operators here more readily trusted FUNCI and reported that they were beginning to gain familiarity with the COSS and also that the trend increased the information's trustworthiness.

Overall, the operators found a FUNCI-like COSS to be an asset in digital HMIs. They saw its simple visual implementation as intuitive and well-integrated into the existing interface. Most importantly, their feedback provided a useful set of principles upon which to improve FUNCI's design. Moving from light water reactors to advanced nuclear power plants, the FUNCI study greatly informed ARCO's COSS HMI.

Networked Operator Analytical Helper The strengths of FUNCI are its simple and intuitive visual design, its ability to reinforce the location and function of existing HMI elements, and the way it assists operators via early warnings and explanatory information. Operators also requested the following features and modifications:

- scrolling notifications with searchable log and timestamps
- efficient alarm organization and presentation
- audio integration as diverse indication of alarms and information
- alarm acknowledgement and highlighting
- alarm priority indication
- dedicated HMI space

These requests lead directly into ARCO's COSS prototype: the Networked Operator Analytical Helper (NOAH). The original wireframe for NOAH is pictured in Figure 6.2. Because NOAH is the focus of COSS development in ARCO, the wireframe concept has a significant amount of information packed into one HMI. The rest of this chapter describes NOAH one section at a time.

The **At-A-Glance Box** strives to improve upon the initial proof-of-concept in FUNCI's number box. It retains the large number so that operators can quickly glance over to see the number of issues. It also has a separate status light, the color of which can indicate the overall plant status. For NOAH, issues are categorized into warnings and problems. Warnings may require no action while problems specifically require operator intervention. To the left of the total number of issues, operators can find the breakdown by warnings, problems, and prompts. Prompts are notifications generated by NOAH that require the operator to respond. These prompts could simply be requests for acknowledgement or guides for fault-mitigating actions. Finally, a countdown timer sits at the bottom of the At-A-Glance Box. This timer indicates the overall time remaining before the plant trajectory enters into undesirable territory. This is likely a long-term capability for NOAH because it requires thresholds for undesirable plant health and plant trips to be well-defined. The timer will hopefully assist operators in understanding the severity and time-sensitivity of plant state so that they are able to cope in the face of multiple issues. Even if the notification number reads 20, the timer may say that the operators have hours to address plant issues and therefore allow them to proceed without undue stress.

The **Fault Box** has a very similar organization to FUNCI's split between messaging and explanatory trends but with more detail. The left side presents issue descriptions. Here in Figure 6.2 are a problem and a warning. Note that iconography reinforces NOAH's style methodology. The pump problem, assigned priority #1 with a "time to handle" and a posting time stamp, also includes an explanatory message that the pump flow rate seems to deviate from the indication. NOAH also provides the other indications with which it makes this determination. As in FUNCI, NOAH shows the relevant component icon with a corresponding colored circle over the component's top left section. The colored circle would also show up in the relevant HMI location. On top of the message, each entry in the issue description section of the Fault Box also has two buttons: the pin button and the link button. The pin button allows the user to keep the issue visible for tracking purposes. The link button

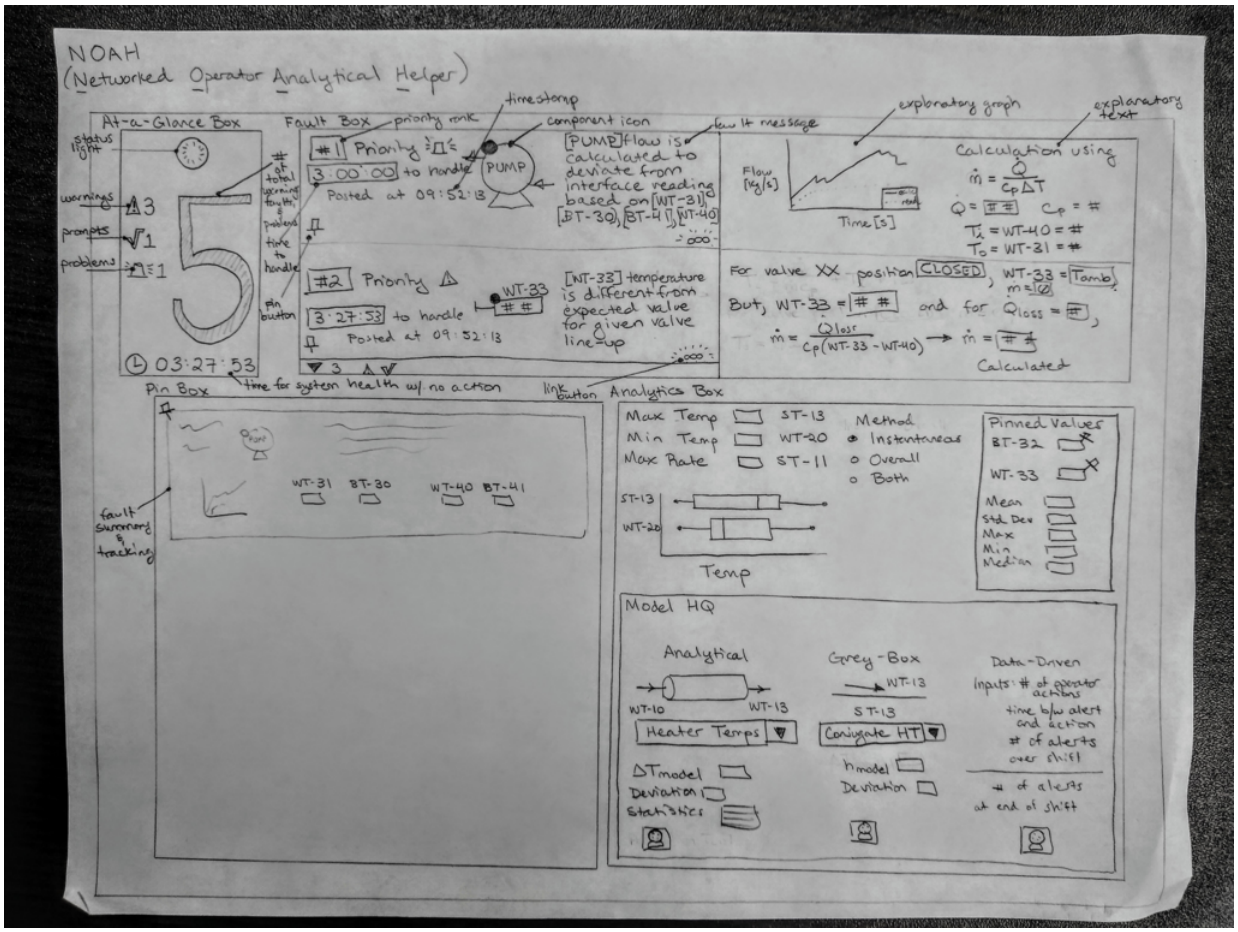

Figure 6.2: NOAH HMI wireframe

allows the user to connect issues that may be related to one another. Additionally, NOAH flashes the link button if it assesses that issues are indeed linked. These buttons offer some customization and management capabilities not present in FUNCI. The second issue shown in the wireframe is very similar to the first, but with a warning instead of a problem. The wireframe shows two displays issues with a downward arrow at the bottom of the issue description section indicating three more issues revealed by scrolling further down. Because these issues are not currently visible, the warning and prompt icons show the user that they are not currently missing a higher-priority problem.

The right side of the Fault Box is the issue explanation section. Here, NOAH provides relevant trends, as seen in FUNCI, and also displays the equations it uses for its issue assessment. In this way, NOAH not only facilitates user trust and situational awareness but also reinforces the user's conceptual model of plant behavior. The issue explanation section builds operator intuition throughout plant operation while guiding issue diagnosis and user decision-making.

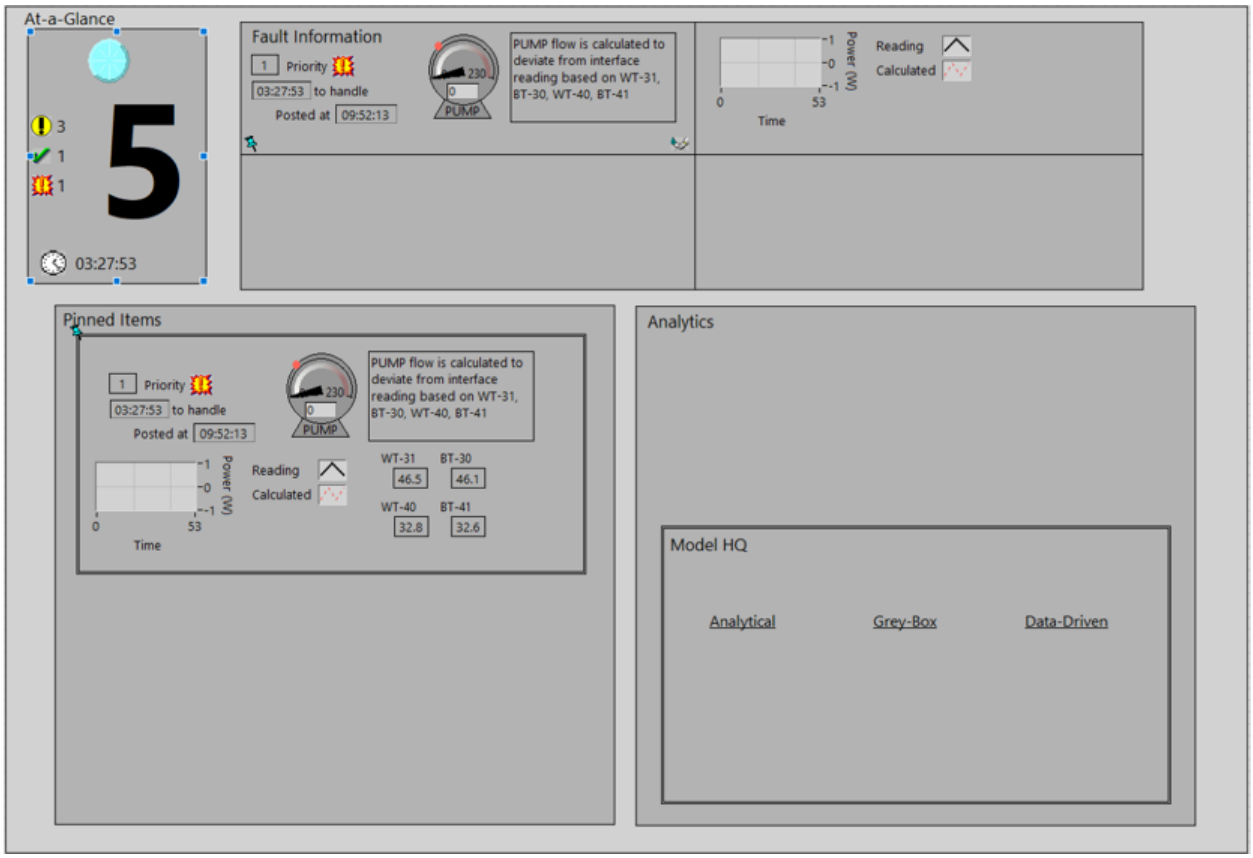

Figure 6.3: NOAH HMI mockup

At the lower left of NOAH is the **Pin Box** that contains "Pinned Items". Here, each of the issues that the user pins stays prominently displayed so that the user can track their progression. In a way, the Pin Box acts as a customizable to-do list. Each pinned item has a summarized view and can be highlighted quickly in the Fault Box if the user so chooses.

Finally, the **Analytics Box** shows detailed tools for the user to investigate and diagnose plant issues or normal operation. The Analytics Box will likely be the section of NOAH most prone to changes throughout the experimental evaluation and development process. For this iteration, the top section shows a variety of statistics along with pinned HMI values for the user to specifically track. The bottom, or the "Model HQ", reveals the plant monitoring system algorithms. Here, the user can choose between different plant models to conduct analyses while operating. The user can set custom notification thresholds for indications based on their analyses. The implementation shown in this wireframe gives the user significant customization options, providing a valuable platform on which COSS designers can test different tools.

Figure 6.3 shows a mockup of NOAH in LabVIEW. This mockup follows directly from the wireframe in Figure 6.2 and will likely change over time through iterative development.

For now, it provides guidance for developers to visualize the end goal of their algorithms.

Other COSS features in ARCO In addition to NOAH, ARCO also contains some other COSS features integrated into its HMIs. Specifically, undergraduate student researcher Sala Tiemann has developed algorithms to collect operator inputs and generate human readable reports of their time-stamped actions to broadcast to the control room and support coordination. The pseudocode for her algorithm is shown in Figure 6.4.

```
1 have old data
2 for ever
3     obtain new data
4     if new data != old data:
5         print ('Operator action taken')
6         old data = new data
7     end
8 end
```

Figure 6.4: Operator action recorder pseudocode, courtesy of Sala Tiemann

Undergraduate student researcher Ian Kolaja has developed a LabVIEW program that integrates into the Supervisor and Overview HMIs and guides plant personnel through the main procedure steps while tracking relevant data streams to automatically proceed to following steps. A screenshot from one of the early iterations of the task manager is shown in Figure 6.5.

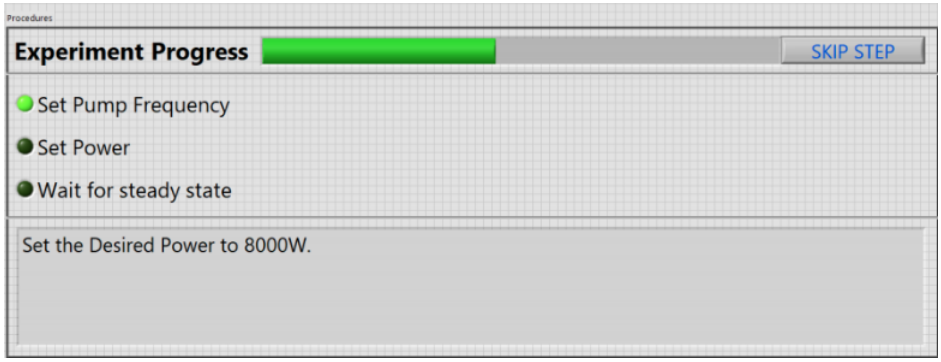

Figure 6.5: Task manager early iteration screenshot, courtesy of Ian Kolaja

These tools are invaluable during ARCO experiments to match operator actions with observations and guide HMI interaction. They will prove even more valuable in future studies focused on operator situational awareness and computer-based procedures development.

Current state The Supervisor workstation interface should intuitively present fully computerized procedures, integrated management and workflow tools for coordinating control

room activities, and integrated fault detection and cybersecurity. In earlier iterations of the design, these tools occupy reserved locations on the interface. In future work to define FHR operations, the main interface will consist of computerized procedures with fault detection, cybersecurity, and management tools as integrated features so that the Supervisor's activities are entirely context-based.

6.3 Data signals and design in ARCO

Chapter 5 described the roles and capabilities of ARCO's physical components. Here, this chapter presents the data streams and manipulations across its workstations. For the following descriptions, refer to Figure 6.6, a diagram building on the architecture depicted in Figure 5.5.

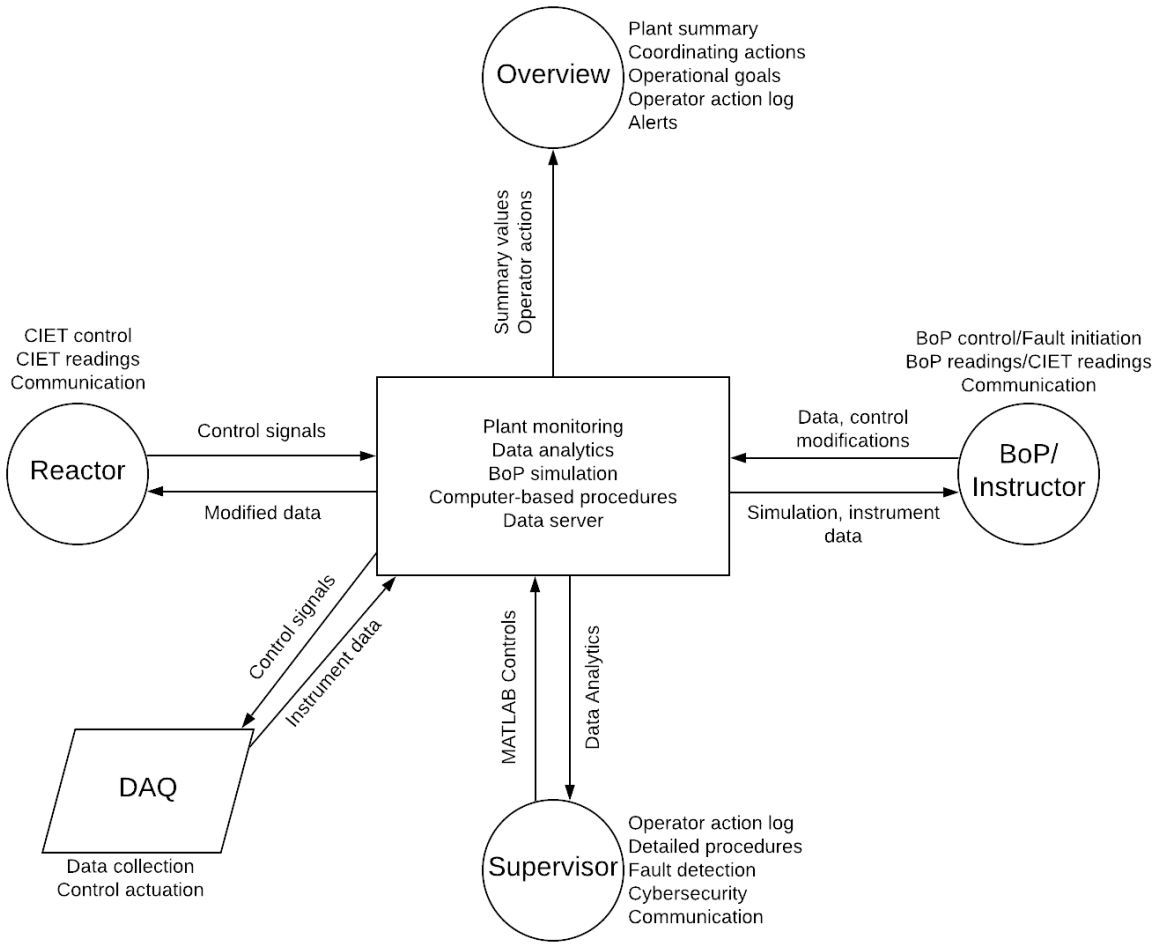

Figure 6.6: Data streams in ARCO

Figure 6.6 shows each OPC UA client and the central server with its corresponding functionality and data streams. The blocks of text close to each client circle describe the client's HMI functionalities. The labeled arrows represent data streams. Finally, the text in the center block details the functionality of the central server. This sections explains the figure, in detail, starting with the central server and then describing the clients from the Supervisor HMI and moving clockwise.

The **central OPC UA server** (located on the Mission Control workstation) supports the majority of computationally-intensive functionality in ARCO. It runs the necessary background LabVIEW software to host OPC UA data flows, handle communication between the DAQ and ARCO, log data, and track computer-based procedures. It also runs MATLAB routines that produce records of operator actions, data analytics, and corresponding plant monitoring information. Finally, the central server runs a dynamic simulation of the NACC using Simulink in lieu of a physical experiment. The server does not store data itself; each client automatically documents historic data in a redundant local database. It is also possible to run multiple copies of the same server to build in redundancy and isolate issues affecting one server uniquely.

The **Supervisor** HMI provides the necessary indications and controls to manage the entire control room and oversee operation. Specifically, the Supervisor HMI features a log of all actions taken by the operators, detailed computer-based procedures, information relevant to fault detection and cybersecurity, and text-based communication with other control room staff. The Supervisor client receives this information from the central server with data analytics (residual generators, statistics, etc.) being the primary data stream. The Supervisor client sends signals to the central server to activate and deactivate external MATLAB data analysis routines.

The Right Operator workstation can either run the **BoP** (Balance of Plant) client or the **Instructor** client. The BoP HMI features a piping and instrumentation diagram (P&ID) of a NACC power conversion system with the corresponding indications and controls along with text-based communication capability. Alternatively, the Instructor HMI features a P&ID of CIET with corresponding indications. In addition to the indications of plant states, the Instructor HMI includes an input field for each indication so that false, or "spoofed" values can be written. The Instructor can then choose to activate spoofing and cause these indications to be overwritten with the spoofed values at each of the other operator stations. To support both BoP and Instructor functionalities, the main data streams to the BoP/Instructor client are data from instrumentation, the BoP simulation, and the server spoof handler. The main data streams from the BoP/Instructor client are BoP HMI controls and modifications to indications and controls from the Instructor HMI.

The **Overview** HMIs present a simplified P&ID connecting both CIET and the BoP to reinforce the common goals of the entire control room. Using this P&ID, they also show relevant plant summary values calculated from available signals, coordinating actions and operational goals from computer-based procedures, and an operator action log. Supervisor-prompted alerts and information also show up on the Overview as related to plant performance, fault detection, and cybersecurity. The Overview clients do not send any information

to the central server, but instead pull their plant summary values, computer-based procedures, and operator actions from the main server.

The **Reactor** HMI features a P&ID of CIET that is nearly identical to that of the Instructor HMI. It also includes a few additional graphs to facilitate trend-watching. Most importantly, the Reactor HMI has the necessary controls for the Reactor Operator to run CIET. Finally, as with the other operator HMIs, the Reactor HMI has text-based communication tools. The Reactor client receives the modified (potentially spoofed or faulted) data from the central server and sends control signals.

The **DAQ** is the final member of the ARCO data ecosystem. It is a separate controller that handles data acquisition and control via instrumentation and CIET control hardware. It has no dedicated HMI in ARCO and runs primarily in the background unless troubleshooting becomes necessary. The DAQ sends instrument data to the central server and receives control signals from it. If hardware errors occur, the DAQ can be easily reset from the Mission Control workstation with full functionality restored.

With the interplay between the different HMIs, clients, and data streams in ARCO defined, the next focus is on the HMI development in ARCO. These HMIs turn ARCO's design into reality and provide the link between human operators and plant operation. This chapter will next describe ARCO's HMI design process.

From wireframing to prototyping As a standard design process, each ARCO HMI began as a wireframe sketch to mock up the spatial organization of information and list the desired features at each operator's workstation. Figure 6.7 and Figure 6.8 show the near-term and long-term concepts for ARCO interface development defined just after Berkeley researchers built the physical facility in the Nuclear Engineering Innovation Laboratory in Etcheverry Hall.

The near-term "now" concept from January 2018 shown in Figure 6.7 echoes much of the functionality described in Figure 6.6. Designers must create these staged development goals iteratively throughout the research process in order to guide their focus and ensure that each task, in context, supports overall efforts. While the OPC UA architecture has since evolved to centralize more data processing and the Reactor Operator HMI was never distinct from the CIET HMI, these wireframes proved extremely useful for early-stage specific HMI development and their influence is evident in the wireframes for each individual HMI concept.

The long-term "then" concept shown in Figure 6.8 introduces some advanced new functionalities such as interactive procedures and Supervisor management tools. While these capabilities are currently in an early stage, the "then" concept helped inform an approach to interface spatial allocation that reinforces the modularity and recognizability of different tools. For example, the operator HMIs mirror one another to simultaneously hint at similarity and contrast. No two displays feature the same size and shape boxes in the same locations so that control room staff have additional context for HMI elements outside of text alone.

After the "now" and "then" concepts helped cement the ARCO HMI roles, individual

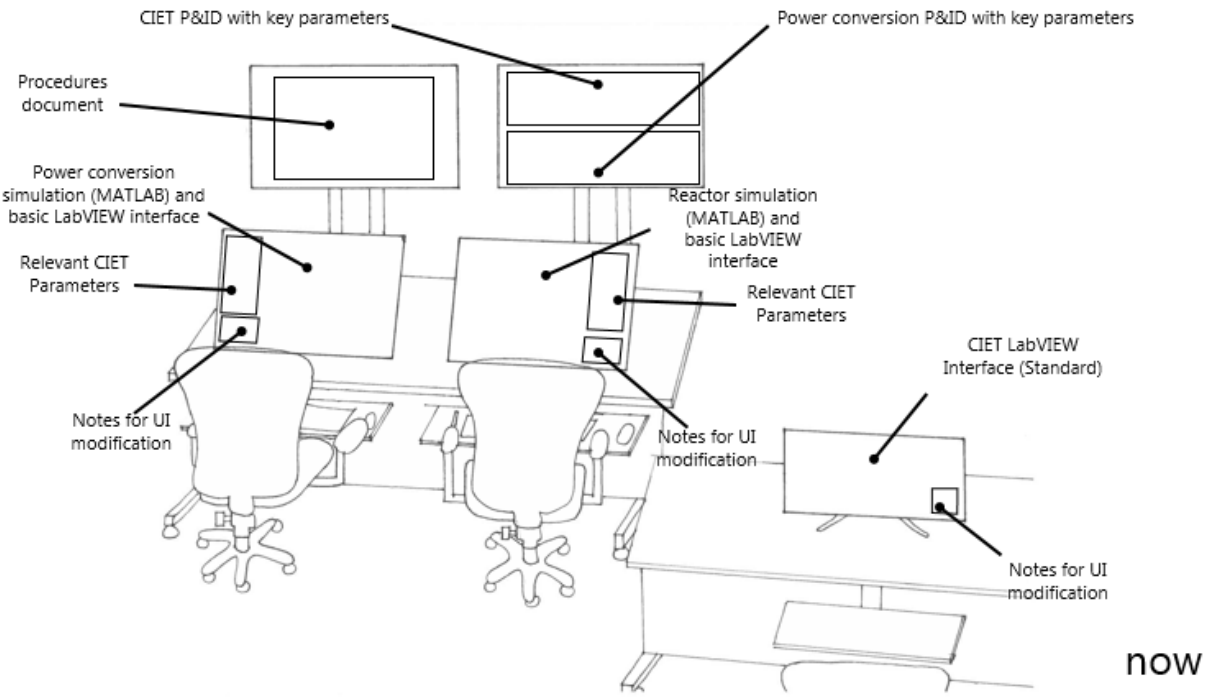

Figure 6.7: "now", or near-term, concept for ARCO in January 2018

wireframes further defined specific features. Because CIET used to have only one interface for experimental facility control, the Reactor HMI was the logical first task. Figure 6.9 shows the initial wireframe for the Reactor HMI.

The Reactor HMI design is simple: a basic P&ID representation of CIET with controls and indications located next to the components to which they are related. There is little additional information on the Reactor HMI outside of room for additional graphs or trendlines, possible additional controls, and an error readout. An additional feature originating in this wireframe is the use of circle pointers to indicate BT thermocouples (Bulk Temperature) inserted into the piping and flat line pointers to indicate WT thermocouples (Wall Temperature) closer to the pipe wall.

Figure 6.10 shows the Reactor HMI in its current form. It closely matches the wireframe in Figure 6.9 except that it has the additional control next to the CTAH (on the right side of the HMI) for changing the CTAH set-point type. Undergraduate researcher Jason Anderson implemented a controller for the CTAH that allows the Reactor Operator to control the CTAH automatically for outlet temperature. Other than that, the Reactor HMI clearly displays controls and indications to the Reactor Operator along with a communication box, indications of OPC UA server connection, and trends of Power Output, Core Temperatures, and CTAH Temperatures.

Looking next at Figure 6.11 for the BoP HMI wireframe reveals the same general simplified P&ID layout along with some expansion plans. The original vision for the ARCO BoP

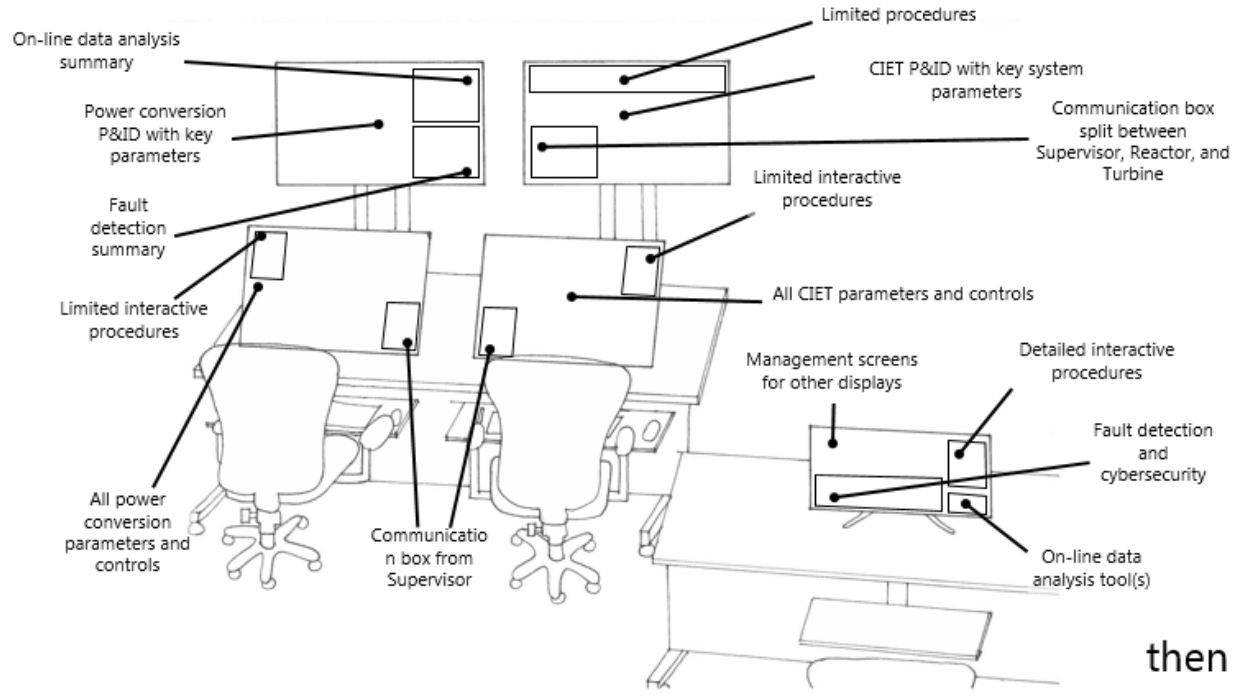

Figure 6.8: "then", or long-term, concept for ARCO in January 2018

included a steam-reheat cycle after the NACC low-pressure turbine outlet and the corresponding indications. The selection of controls and indications is a determination based on research needs and changes over the course of the BoP system design process. In addition to the trends and analytics section to match that of the Reactor HMI, the original design for the BoP HMI also included a load and demand section to plan for future research that could use ARCO to study load-following, plant performance goals, the integration of external drivers such as weather and grid dynamics, and more.

Because, in contrast to the Reactor HMI, the BoP HMI was a new interface for a new ARCO capability, BoP researchers gave direct input into the necessary HMI elements and capabilities. For the BoP and other HMIs, the design process began with a list of elements before spatially allocating them as shown in Figure 6.11. In general, ARCO HMIs follow a stepped approach with expected version iterations.

The BoP HMI, shown as currently implemented in Figure 6.12, has deviated a bit from the original wireframe shown in Figure 6.11. BoP researcher Shane Gallagher removed the reheat steam cycle from the BoP's first iteration, resulting in the very simple P&ID shown in Figure 6.12. There is also now a combustor in the bottom right for control of natural gas injection. Finally, the controls and indications are more well-defined and the trends are on the right side of the interface instead of along the bottom. The Load and Demand box is currently a placeholder but will feature additional indications, controls, and trends in the future.

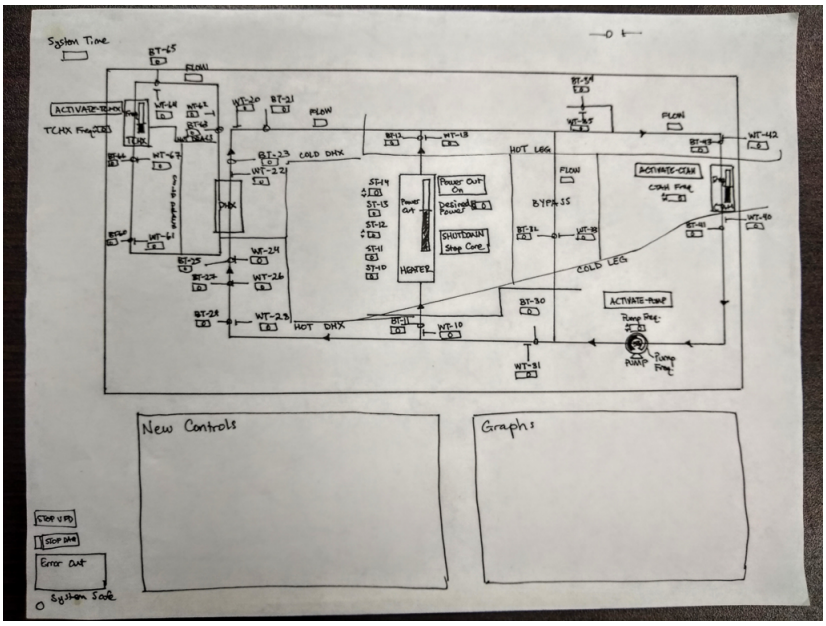

Figure 6.9: Reactor HMI wireframe

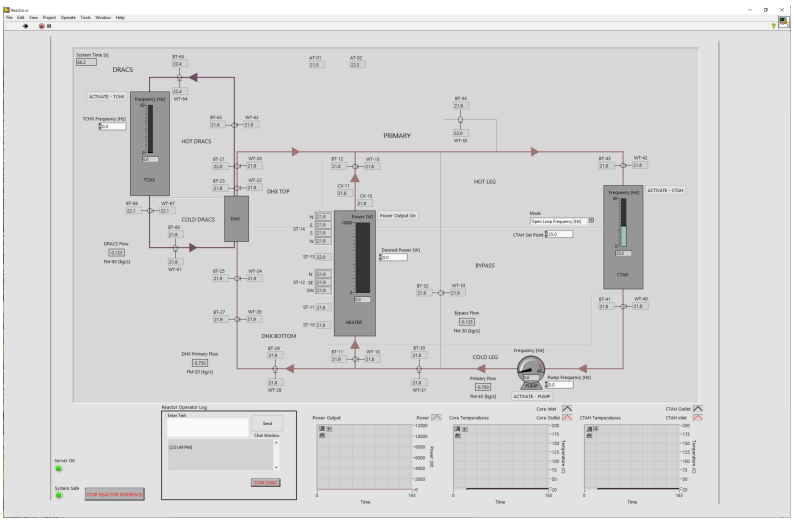

Figure 6.10: Reactor HMI

The Instructor wireframe shown in Figure 6.13 contains a simplified P&ID for CIET very similar to that of the Reactor HMI. The main differences are that it is smaller and should include some indication of whether or not values are being spoofed or manipulated. The wireframe also shows a System Analytics box with planned iterations including basic mathematical functions, graphs and data visualization, and plant prognostics models. The bottom right Action Log box similarly features three planned stages: first, a basic readout

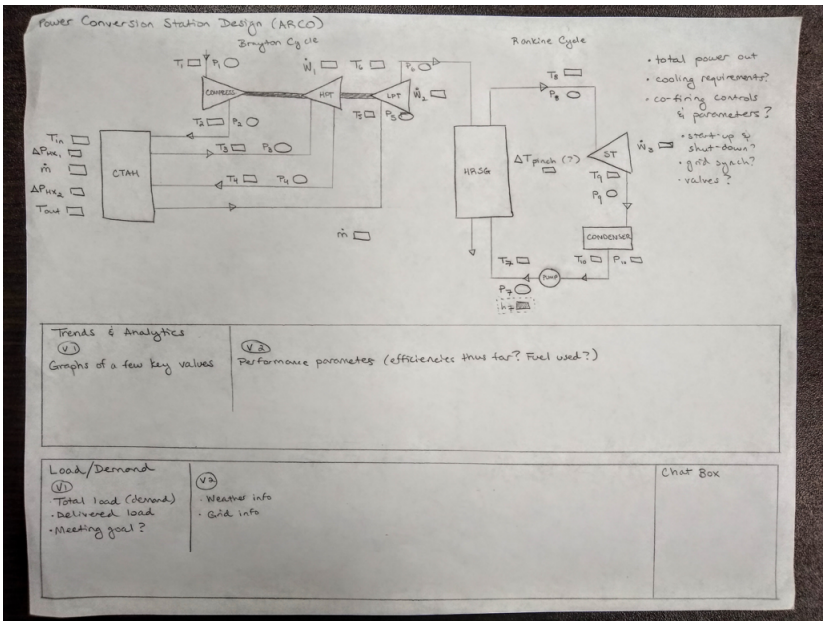

Figure 6.11: BoP HMI wireframe

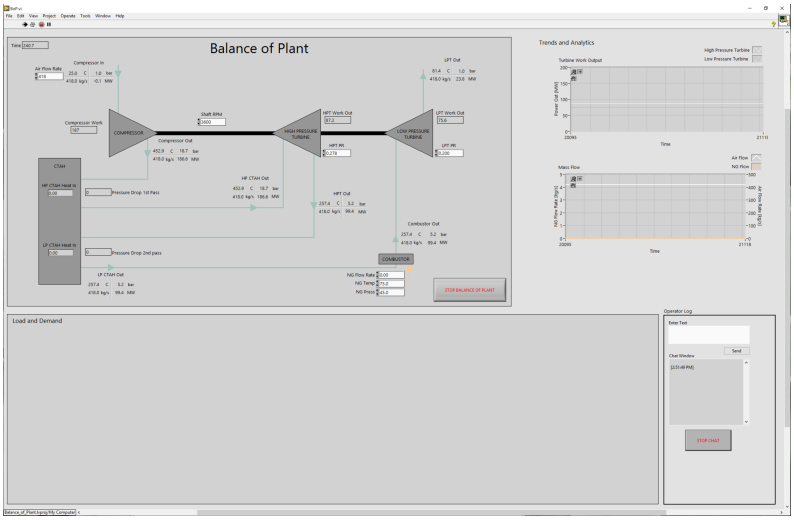

Figure 6.12: BoP HMI

of operator actions; second, action signals integrated into the P&ID; and third, an entire replica of the Reactor Operator (the word "Supervisor" is incorrect on this wireframe) HMI. The bottom left Build Attack box concept starts with a set of controls for building faults and cyber-attacks, then a Reactor Operator HMI-integrated set of data manipulation controls, and finally a text-based input for defining manipulations.

The Instructor HMI shown in Figure 6.14 took a slightly different approach than the

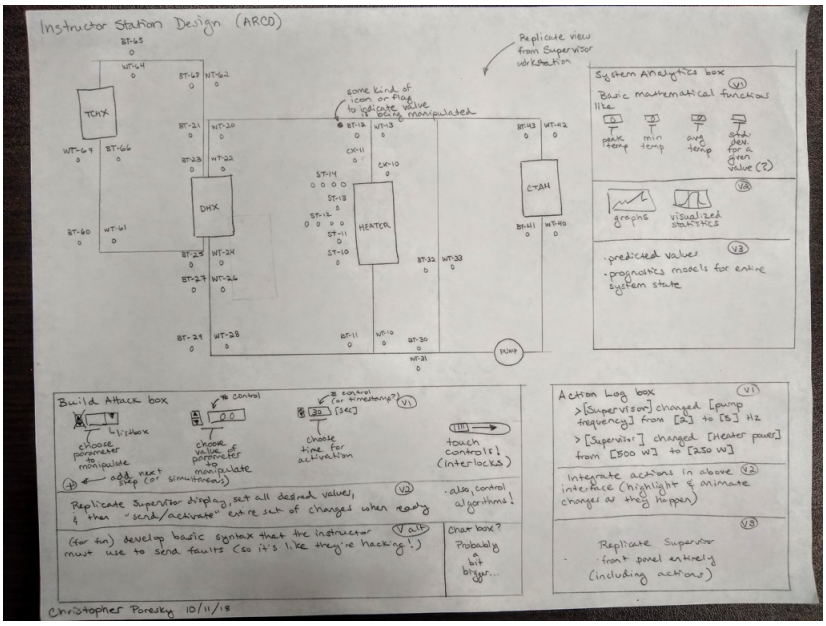

Figure 6.13: Instructor HMI wireframe

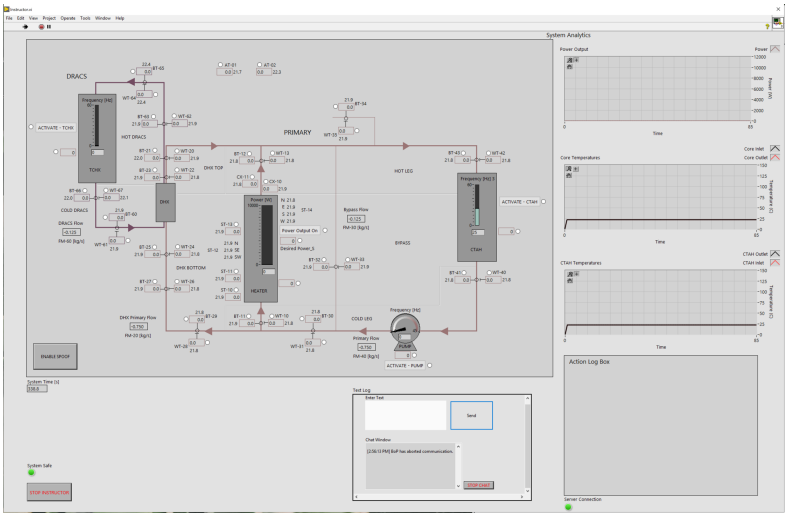

Figure 6.14: Instructor HMI

one conceptualized in Figure 6.13. It doesn't have any true "System Analytics" yet but instead has the same graphs as seen in the Reactor HMI. The Action Log box is functional and represents the first version shown in the wireframe. Finally, the spoof and fault control implementation is similar to that of the second version in the "Build Attack" box. Each indication on the P&ID has a corresponding input control where the Instructor can write their own value. Then, by clicking the radio button, the Instructor "activates" that particular

indication's spoof. Finally, once the Instructor has configured all desired indication and control manipulations, they can click the "ENABLE SPOOF" button in the bottom left to send all manipulations at once. The radio button and the "ENABLE SPOOF" button must be simultaneously active for a particular manipulation to be active. This acts as an interlock. Even during faulted or spoofed operation, the Instructor alone has access to raw data values and the true status of the plant. The Instructor leads and orchestrates fault detection and cybersecurity tests by manipulating ARCO (and even CIET) without the knowledge of the control room staff.

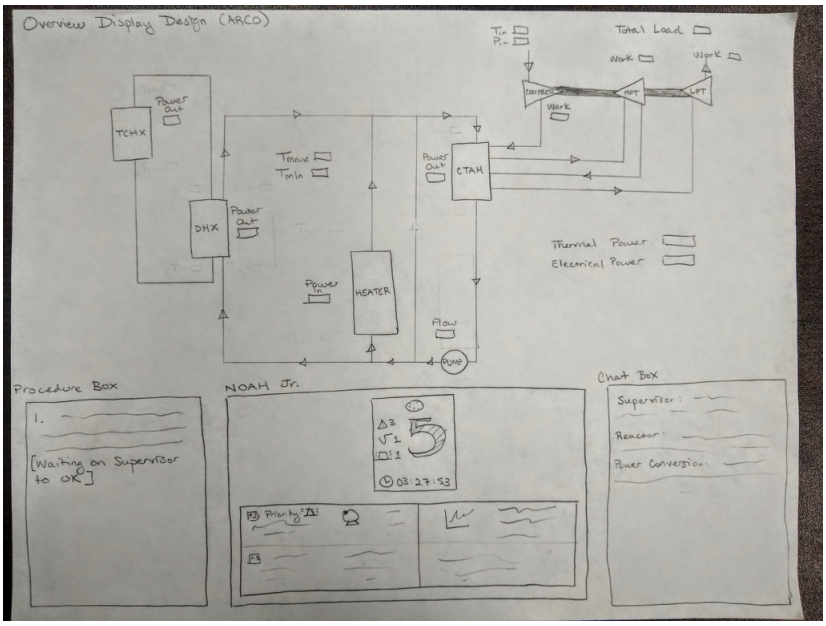

Figure 6.15: Overview HMI wireframe

Figure 6.15 shows the wireframe for the Overview HMI. Because digital HMIs fundamentally change the concept of operations in nuclear plant control rooms and operators can accomplish all tasks sitting at one workstation [126], Overview HMIs may assist in maintaining operator situational awareness by reinforcing the context with which operators' individual tasks relate to one another. By visually displaying the connection between the BoP and the Reactor on the Overview plant P&ID, operators can quickly glance up at the Overview to see summary values and how their actions affect the rest of the plant. In addition, the Overview should contain a summarized version of the computer-based procedures and communication tools known as "NOAH Jr."

The concept behind the Overview HMI(s) is that the control room staff will periodically look up at them to check on overall plant status and to ensure they properly understand the context of their individual tasks. The Overview has only indications and no controls present. Operators look to the Overview to understand what they should be doing, what others are doing, and whether the plant as a whole is operating properly.

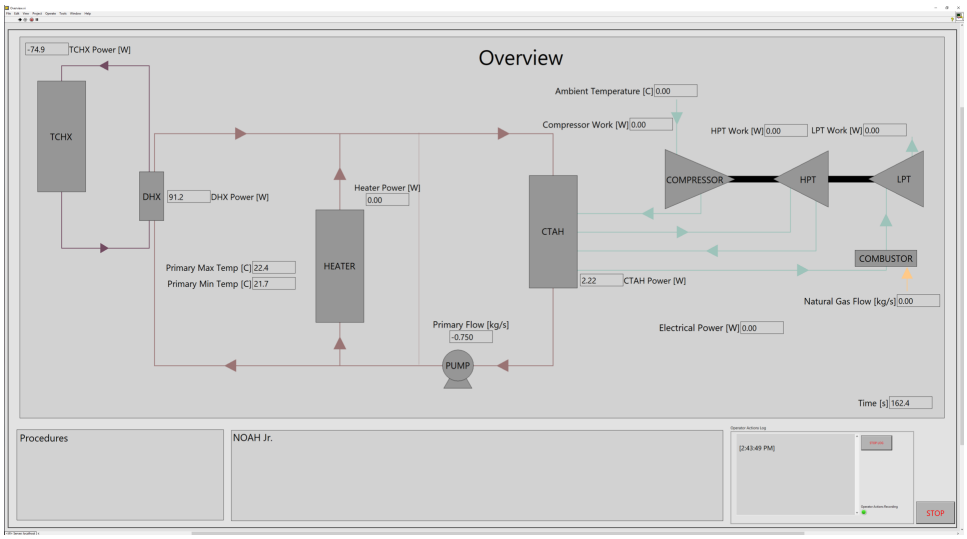

Figure 6.16: Overview HMI

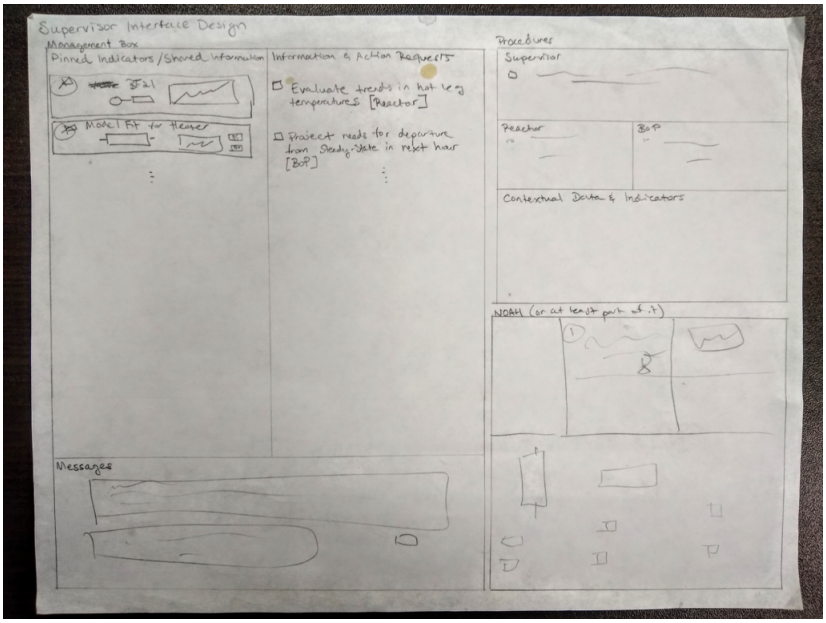

Figure 6.17: Supervisor HMI wireframe

The Supervisor HMI, with initial wireframe depicted in Figure 6.17, represents ARCO's most significant evolution from conventional nuclear plant control rooms. The Supervisor HMI will ideally develop over time to provide the Supervisor all necessary tools for managing the control room including the operators and the plant monitoring system. Because the Supervisor plays a role of managing plant operation and advanced features, the Supervisor

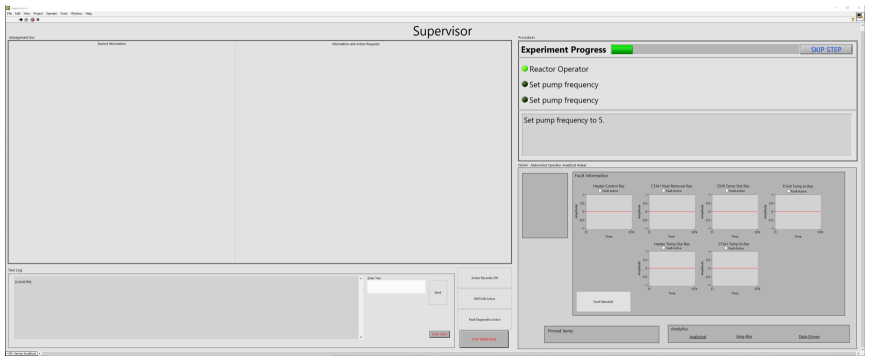

Figure 6.18: Supervisor HMI

HMI is essentially the headquarters of COSS capabilities in ARCO. The wireframe shows a variety of features for this purpose including text-based communication, detailed computer-based procedures for all control room staff, NOAH, and a management box allowing the Supervisor to assign tasks and highlight elements on the operator HMIs.

Some of the features depicted in the wireframe require more advanced development in the ARCO software and some of it can be easily implemented. An important aspect of HMI development, especially for the Supervisor and COSS capabilities, is to conduct iterative testing to experimentally determine the optimal organization of information and capabilities. Additional desirable features not shown in the wireframe include

- the ability for the Supervisor to flag or "comment" on procedure steps,
- contextual data indications at each procedure stage, and
- the ability to selectively share or send information to the operator or Overview HMIs.

Experimental development Before attempting to use ARCO for any plant monitoring experiments, the research team at Berkeley conducted some exploratory HMI evaluation trials to understand the user-friendliness of operation. These trials not only yielded insights for iterative HMI development but also for procedure definition, common personnel mistakes during operation, and general best practices for quality assurance. The tests, objectives, and takeaways were as follows:

The first three tests using ARCO focused on evaluating the Reactor HMI. CIET always had an HMI but this was the first iteration of the design planned in Figure 6.9. Over the course of these tests, researchers-as-operators gave feedback on the HMI elements including suggestions to:

- improve HMI control and indication terminology,
- standardize HMI control and indication styles,

- improve HMI control input feedback,
- make control locations more intuitive,
- clarify control operation ranges,
- divide P&ID into labeled sections,
- increase text and image size,
- remove or hide non-functional HMI elements,
- adjust graph scales and label with source data,
- add further labels and information to the HMI,
- expand tooltips and diverse means of indication, and
- adjust chat windows to auto-scroll.

They also requested additional capabilities such as the option to:

- adjust graphs while operating,
- capture HMI current state,
- set and customize thresholds for notifications on plant states,
- troubleshoot issues during operation by accessing HMI code,
- input control values with decimal precision, and
- access multiple pieces of software from one window.

As the researchers had the opportunity to train on the brand-new facility, they also recommended changes to experimental procedures and ARCO itself such as:

- manage facility wires,
- check access hazards,
- create training documents for operators to read before tests,
- increase the detail and clarity of procedures, and
- place knowledge in the environment (i.e. print directions for initial facility set-up and place them on the relevant components)

After the initial Reactor HMI proved useful, the next set of tests focused on the full ARCO control room including the Supervisor, Reactor, BoP, and Overview HMIs communicating over OPC UA with each other and the DAQ. Here, new steps for improvement included:

- adjust timing for data streams in OPC UA to ensure smooth data point updates,
- redefine data stream properties to ensure expected data communication behavior,
- allow the Instructor to spoof both indications and controls,
- integrate other researchers' work such as new control algorithms,
- define routines to introduce cyber and physical faults to ARCO,
- iterate set of indications and controls on new HMIs,
- integrate new COSS capabilities such as task management and operator action recording, and
- successfully integrate dynamic BoP physics-based model for real-time simulation during CIET experiments.

Each test revealed a rich set of new recommendations and steps for iteratively improving ARCO's HMIs. Even as the test plan progressed past HMI evaluation to plant monitoring studies, operators provided feedback that will ultimately be integrated into general guidelines for advanced reactor control room HMI design.

Future plans and next steps In the final realization of ARCO, the Reactor and BoP Operator workstations and the Supervisor workstation will be entirely task-based while the Overview Displays will be static docks for orienting information and coordination between control room staff. NOAH will realize its design capabilities but will likely also change conceptually with operating experience and revealed desirable functionality. The main overarching goals are to pursue:

- integrated HMIs with context-based available information,
- increased information and control automation to facilitate operator workflow,
- heightened plant monitoring capabilities to provide richer operator support,
- actuation methods leveraging modern technologies such as touchscreen, audio, and more.

Chapter 7

Case studies

This chapter provides a case study of the development and application of a plant monitoring system in the Advanced Reactor Control and Operations — Compact Integral Effects Test (ARCO-CIET) facility through experiments involving multiple physical and control system faults. The first section describes the plant models and phenomena of interest for the case study as well as their mathematical formulation and implementation into plant monitoring algorithms. The next section describes the experiment in theory and execution. Finally, the last section presents the experimental data and resulting conclusions used in the iterative plant monitoring system development process.

CIET and FHR operating phenomena Because there is no fully-specified design for a prototypical Fluoride salt-cooled High temperature Reactor (FHR), targeting specific faults for detection is an open-ended task. CIET's reference design is the Mk1 PB-FHR with 10 kW of electrical heating in CIET corresponding to 10% of full power in the Mk1 PB-FHR. In order to scale ARCO values up to show prototypical FHR values, further scaling work must first be completed. A structured Failure Methods and Effects Analysis (FMEA) can help produce candidate faults, as can experimental data and lessons from similar systems. As part of the brainstorming process, Table 7.1 presents potential faults and failure modes that were used for the development of the ARCO-CIET plant monitoring system. As indicated, some faults that can be experimentally studied in CIET have relevant and important counterparts in a prototypical FHR. On the other hand, some faults in CIET may be relevant to non-FHR systems and some FHR faults are difficult to simulate in CIET. The left side of the table lists CIET faults with FHR relevance and the right side lists faults that would require further experimental development to test.

The goal in choosing faults of interest for initial case studies using the fault network plant monitoring methodology is to select a small set of diverse faults that illustrate different initiation sources, effects, and relevant signals. For CIET, this chapter focuses on component models that isolate and describe a sub-section of the overall plant. Specifically, this chapter investigates the heated test section representing an FHR core, the primary heat exchanger, and the passive primary and DRACS loop piping.

CIET	FHR
Heater/core failure	Reactivity transients
Loss of primary heat sink (CTAH)	Heat exchanger tube rupture
Loss of secondary heat sink (TCHX)	Stuck check valve
Leaks and blocks	Frozen salt
Control system disconnection	Pebble handling malfunction
Cyber-attacks to HMIs	Electrical system malfunctions
Cyber-attacks to control system	Facility flooding or coolant collection
Pump dead head	Long-term structural deformation
Gas entrainment	Pump cavitation
Balance of Plant faults	Turbine trips
Instrumentation failures	Pebble dust deposits

Table 7.1: Selected CIET and FHR faults of interest.

- The **heater** represents an FHR core or, more generically, the heat input section of a plant or process. The operator typically controls some aspect of heat input to achieve desired plant state and deliver the output goal. It will be very important to detect and understand faults associated with the heater.
- The **primary heat exchanger** represents the FHR's Coiled Tube Air Heater (CTAH) or, more generically, the heat removal section of any power plant. The operator typically controls some aspect of heat removal by varying the oil cooler fan speed to remove the appropriate amount of heat gtom the power conversion fluid. Real-time detection of compromises in the as-designed heat exchange relationship enables the operator (or autonomous control routines) to adapt and ensure safe, reliable, economical operation even during plant upsets.
- The **loop piping** represents the majority of CIET and is of primary relevance to the FHR in which long-term structural piping degradation may be more affected by transients than core integrity. Furthermore, the generic problem of being able to trust instrumentation and maintain calibration is essential for inspection and maintenance planning. Monitoring CIET thermocouples for erroneous readings supports virtual sensor and on-line calibration research.

Model formulation

With no additional modeling, the physical CIET facility can already be described by its known temperature and flow measurements as well as its controllable inputs. A structural model with only these values would be just-determined — there is one equation to describe each known variable. This model would never, therefore, be able to detect a fault in any sensor or input without some additional information. As discussed in Chapter 3, additional

information might come from various sources such as further instrumentation, conceptual models of interdependent measurements (i.e. relationships between inputs or system states that lie in designer or operator intuition), or prescribed value ranges with high and low limits, among others. These approaches all have caveats: cost and physical constraints, lack of definition or physical meaning, and lack of context. Introducing models of the system that describe the physical processes in CIET, however, should provide supplemental understanding of the ways each instrument reading are related to one another. This section describes each model used for plant monitoring by first introducing physical considerations and then providing the corresponding mathematical formulations. Detail about the formats of equations implemented in the Fault Diagnostics Toolbox can be found in Appendix A and numerical data for model parameters with reference sources can be found in Appendix B.

Modeling the heater The CIET heater, shown schematically in Figure 7.1, is a cylindrical test section consisting of three main components: an outer shell (a), an inner tube (b), and a flow volume (c). During experiments, operators drive an electric resistance heating element to input power into the outer shell and heat the fluid through convective heat transfer. Fluid therefore enters from the cold leg of the primary loop and flows vertically through the test section as it rises in temperature via constant heat flux at the outer shell's surface. The inner tube is electrically isolated from the outer shell to avoid electrical shorts. It serves primarily as a static mixer to augment heat transfer in the test section at the expense of pressure drop. The inner tube augments heat transfer in two main ways: it has perforations that allow flow into the center of the test section to increase heater fluid volume and it uses an internal twisted tape to increase mixing and trip turbulent flow [127].

The first step in modeling is to define the phenomena, variables, performance outputs, and inputs of interest (note that these are currently CIET values and not FHR values, as shown in Appendix B):

- *Phenomena:* Power input to outer shell, convective heat transfer from outer shell to fluid, convective heat transfer from fluid to inner tube, convective heat transfer from outer shell to ambient air
- *Parameters:* Masses, specific heats, heat transfer areas, convection heat transfer coefficient, volumes, densities
- *Variables:* Temperatures, flow rate
- *Performance output:* Heater outlet temperature
- *Input:* Heater power

Researchers have experimentally measured convective heat transfer coefficients at different flow rates [127] but the challenge in characterizing conjugate heat transfer between the solid outer shell and the fluid is an interesting and important problem for anticipating system response in both steady-state and transient conditions. Furthermore, because CIET is a

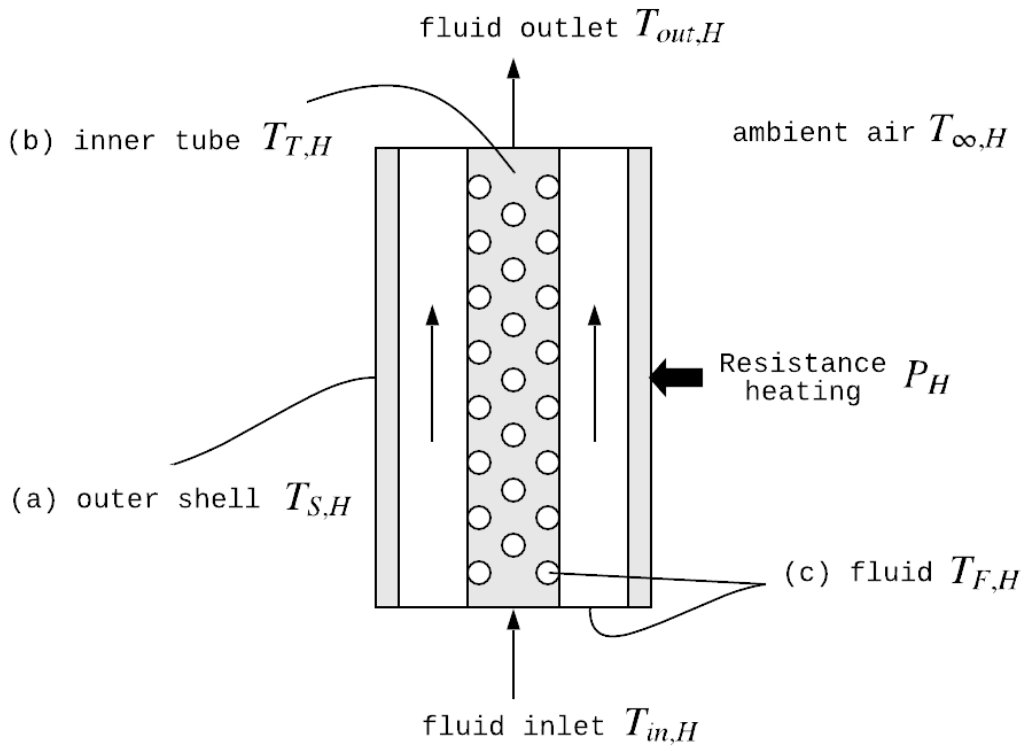

Figure 7.1: Schematic of the CIET heater showing the heat transfer components

scaled integral effects test using simulant fluids for the FHR, ensuring that distortions in the relative thermal inertias and heat capacities of the heater solid and fluid components are well understood is essential to supporting CIET's role as a predecessor to commercial prototype demonstration.

Berkeley researchers have conducted exploratory research into complementary interrogation methods for understanding conjugate heat transfer in single-phase systems with a focus on frequency response methods [74, 76, 115]. It is particularly important to cultivate a sound understanding of conjugate heat transfer in FHRs because, in contrast to light water reactors, primary system integrity concerns likely stem from thermal damage to reactor vessel metallic structural materials rather than thermal excursions in fuel elements [75]. This is a result of very high thermal margins to degradation and boiling in the fuel and coolant. Frequency response work in [76] produced models that examine the relationship between heater power input, convection heat transfer, and the resulting structure and fluid temperatures. These values are useful to relate to one another not only for the purpose of exploratory research, but also for fault detection and plant monitoring purposes. Specifically, the relationships between fluid and structural temperatures compared with human-machine interface (HMI) temperature readings reinforce confidence in measured values for system power. This chapter

presents models that build on these previous formulations.

The model contains equations describing the different heat transfer effects that result from the electrical power input in each component of the CIET heater, divided into inner tube, fluid, and outer shell. As power enters the outer shell via resistive heating, it

1. raises the average temperature of the shell,
2. raises the average temperature of the fluid,
3. raises the average temperature of the inner tube,
4. stimulates convection heat transfer between the shell and the fluid,
5. stimulates convection heat transfer between the fluid and the inner tube, and
6. stimulates convection heat transfer between the shell and ambient air.

This relationship, expressed mathematically, is:

$$P_H = \frac{dT_{S,H}}{dt}(Mc_p)_{S,H} + \frac{dT_{F,H}}{dt}(Mc_p)_{F,H} + \frac{dT_{T,H}}{dt}(Mc_p)_{T,H} + \dot{Q}_H + \dot{Q}_{T,H} + \dot{Q}_\infty \tag{7.1}$$

where the expressions for convection heat transfer to the fluid, inner tube, and ambient air are:

$$\dot{Q}_H = (hA)_{S,H}(T_{F,H} - T_{S,H}) \tag{7.2}$$

$$\dot{Q}_{T,H} = (hA)_{T,H}(T_{F,H} - T_{T,H}) \tag{7.3}$$

$$\dot{Q}_\infty = (hA)_{\infty,H}(T_\infty - T_{S,H}) \tag{7.4}$$

and the power balance in the heater fluid can also be described as the power needed to maintain its inlet and outlet temperature:

$$\dot{Q}_H - \dot{Q}_{T,H} = (\dot{m}c_p)_{Dow}(T_{out,H} - T_{in,H}) \tag{7.5}$$

where

- P_H = power input to heater outer shell $[W]$
- $T_{S,H}$ = mean outer shell temperature $[^\circ C]$
- $(Mc_p)_{S,H}$ = heat capacity of shell $[W \cdot sec/^\circ C]$
- $T_{F,H}$ = mean heater fluid temperature $[^\circ C]$

- $(Mc_p)_{F,H}$ = heat capacity of fluid $[W \cdot sec/^\circ C]$
- $T_{T,H}$ = mean inner tube temperature $[^\circ C]$
- $(Mc_p)_{T,H}$ = heat capacity of tube $[W \cdot sec/^\circ C]$
- $\dot{Q}_H$ = power input to fluid $[W]$
- $\dot{Q}_{T,H}$ = power input to inner tube $[W]$
- $\dot{Q}_\infty$ = power input to ambient air $[W]$
- t = time $[sec]$
- $(hA)_{S,H}$ = mean heat transfer coefficient times area for fluid-to-shell heat transfer $[W/^\circ C]$
- $(hA)_{T,H}$ = mean heat transfer coefficient times area for fluid-to-tube heat transfer $[W/^\circ C]$
- $(hA)_{\infty,H}$ = mean heat transfer coefficient times area for shell-to-ambient heat transfer $[W/^\circ C]$
- T_∞ = mean ambient air temperature $[^\circ C]$
- $(\dot{m}c_p)_{Dow}$ = mass flow rate times specific heat for Dowtherm A in heater $[W/^\circ C]$
- $T_{out,H}$ = heater outlet fluid temperature $[^\circ C]$
- $T_{in,H}$ = heater inlet fluid temperature $[^\circ C]$

This equation captures the heater's physics in both steady-state and transient power cases. At steady state, all of the power going into the outer shell will go to maintaining shell and fluid average temperatures while contributing to the $\dot{Q}$ terms and all $\frac{d}{dt} \approx 0$. During power transients, the power change will cause all $\frac{d}{dt} \neq 0$ for some time before arriving at steady state. Practically speaking, incorporating these dynamics into the model is important to ensuring the model can differentiate between conditions where power may be the same but power distribution may be different due to thermal inertia.

These equations are based on modeling the heater as a single control volume. While the heater shows significant axial variation in temperature, focusing on the overall power balance needed to maintain inlet and outlet temperatures may closely approximate net behavior with this simple formulation.

Because there is no direct measurement of the inner tube temperature and no available fluid-to-tube convection heat transfer coefficient measurement, the inner tube poses a modeling problem. To remedy this, a plausible simplifying assumption is that the fluid and inner tube are at the same temperature. This may be reasonable because researchers designed

the inner tube to induce mixing and bring flow into the center of the heater [127]. While discounting the separate temperature dynamics of the inner tube may lead to discrepancies, the associated error can be assessed via experimental investigation. One of the goals of this study is to investigate systems of low fidelity models to predict dynamic behavior efficiently and with acceptable accuracy to challenge the need for high-fidelity models.

Figure 7.2 shows a schematic of the simplified heater model with only the (a) outer shell and the (c) fluid. The simpler model removes two terms from the input power balance

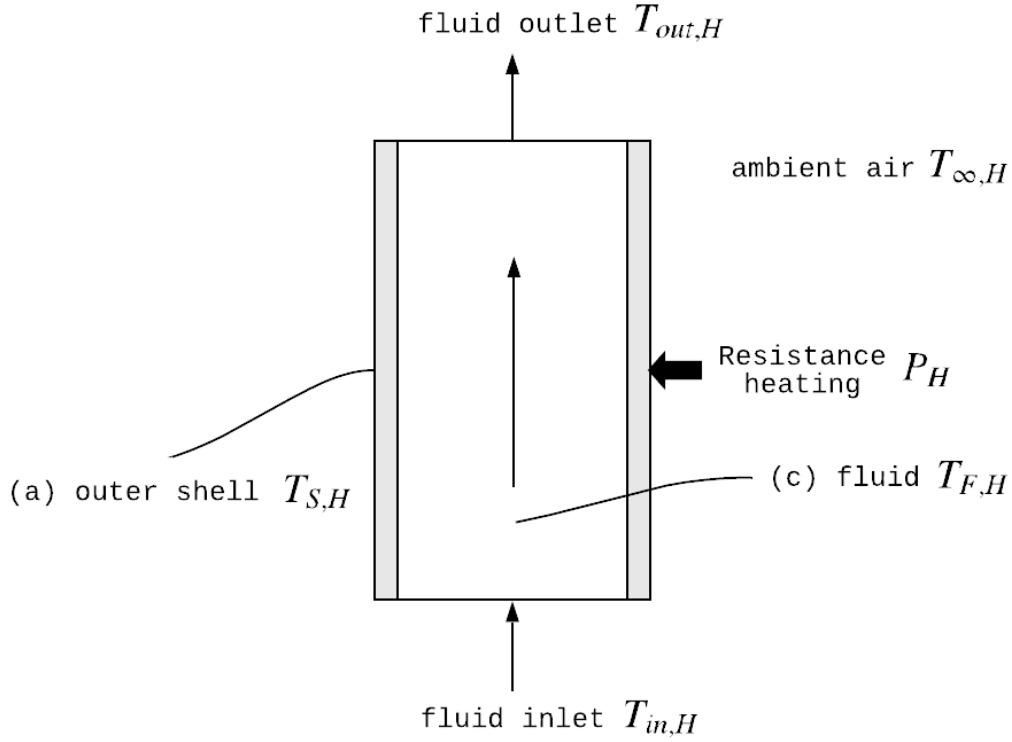

Figure 7.2: Simplified heater schematic, with no inner tube, used to formulate case study model

$$P_H = \frac{dT_{S,H}}{dt}(Mc_p)_{S,H} + \frac{dT_{F,H}}{dt}(Mc_p)_{F,H} + \dot{Q}_H + \dot{Q}_\infty \tag{7.6}$$

where the expressions for convection heat transfer to the fluid and ambient air are

$$\dot{Q}_H = (hA)_{S,H}(T_{F,H} - T_{S,H}) \tag{7.7}$$

$$\dot{Q}_\infty = (hA)_{\infty,H}(T_\infty - T_{S,H}) \tag{7.8}$$

and the power balance in the heater fluid is the same as the power needed to maintain its inlet and outlet temperature:

$$\dot{Q}_H = (\dot{m}c_p)_{F,H}(T_{out,H} - T_{in,H}) \tag{7.9}$$

where the variables are the same as above except that $(Mc_p)_{F,H}$ and $(\dot{m}c_p)_{F,H}$ refer to values that average the properties of the inner tube and heater fluid together. The mean fluid temperature comes from a simple average of inlet and outlet fluid temperatures. The mean shell temperature comes from averaging all surface temperatures.

Thermocouples in the heater measure fluid and shell temperatures. A mass flow meter measures mass flow rate. Power is both an input and a measurement. This is a full model of the heater that can, at each time step, predict the temperature evolution of the heater fluid outlet and outer shell inner surface at the next time step using already-available system measurements.

The Dulmage-Mendelsohn (DM) decomposition of this structural model in the Fault Diagnostics Toolbox is shown in Figure 7.3.

Appendix A contains the numbered equations as entered into the Fault Diagnostics Toolbox model. Appendix B contains parameter values. Figure 7.3 shows that the entire model is over-determined and can be broken up into five equivalence classes and two additional over-determined equations. This means that one fault affecting the equations inside each box and in the lower-right equations can be isolated at a time. In other words, this model is suitable for isolating seven distinct faults from one another but cannot guarantee isolability for multiple faults affecting equations in the same equivalence class. Specifically, because the model uses the average value of multiple thermocouples for each temperature variable, it cannot be used to isolate faults unique to specific thermocouples. The equivalence classes, starting from the top left, correspond to faults affecting

- dynamic power distribution related to operator input,
- outlet fluid temperature measurement,
- inlet fluid temperature measurement,
- shell temperature measurement,
- primary flow rate measurement,
- power into the fluid across the heater,
- and power due to convection heat transfer in the heater fluid.

If research focus falls on other types of heater faults, additional equations or relationships can change the DM decomposition to break up equivalence classes and capture other phenomena. As shown in Figure 7.3, the fault of interest for this case study affects the operator-controlled power input. This fault clearly activates the top-left equivalence class describing dynamic power distribution given power input.

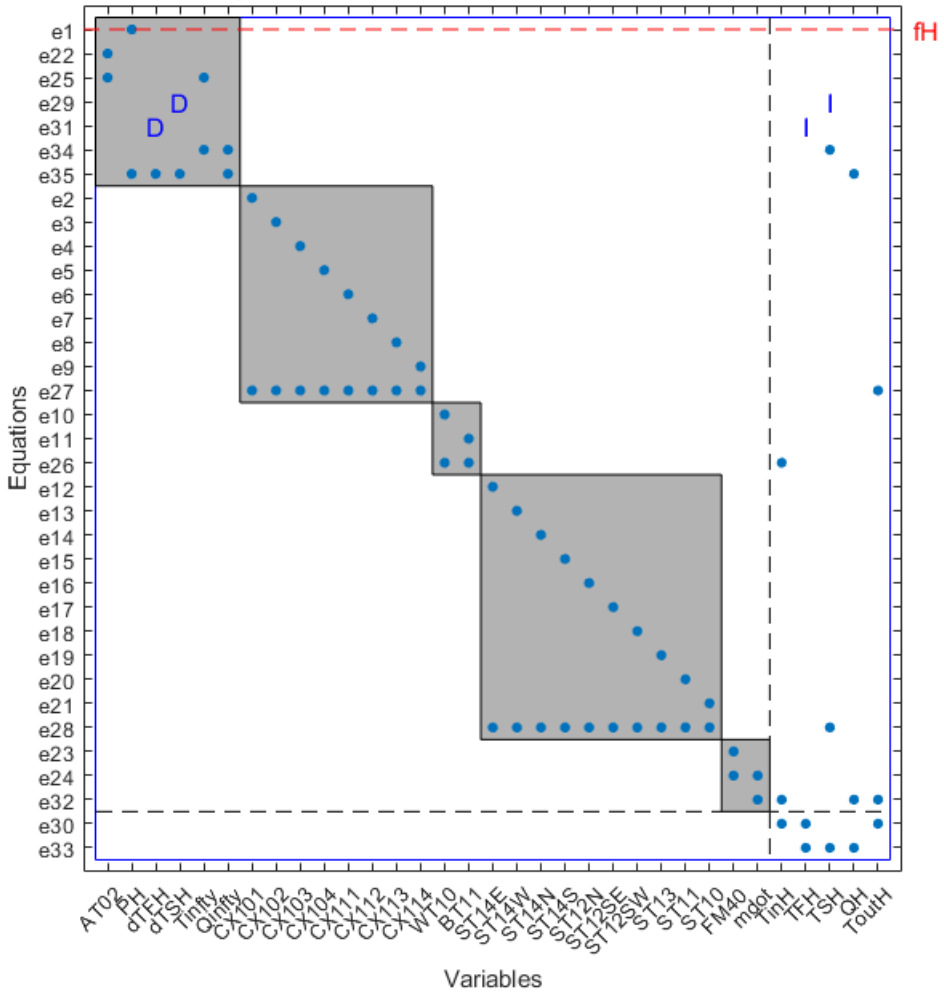

Figure 7.3: Dulmage-Mendelsohn decomposition of CIET heater structural model

Modeling the CTAH The CIET heat exchangers are very similar to the heater in that they feature convective heat transfer that can be described by the power into the working fluid needed to maintain a temperature difference. In fact, the only substantial difference in phenomena between the heat exchangers and the heater is the source of heating. While the heater has power input directly to the solid structure, the heat exchangers have heat transferred through stages of convection, driven primarily by temperature differences.

The primary loop of the Mk1 PB-FHR and of CIET each contain three heat exchangers: a primary heat exchanger (PHX) to facilitate heat transfer from the primary loop to the power conversion system, a direct reactor auxiliary cooling system (DRACS) heat exchanger (DHX) to facilitate heat transfer from the primary loop to a passive natural circulation loop, and a thermosyphon-cooled heat exchanger (TCHX) between the natural circulation loop and external air. The designs between the Mk1 and CIET differ somewhat but the simple

model below can easily adjust to fit either system or many others.

The PHX in the Mk1 FHR, a Coiled Tube Air Heater (CTAH) [78], is implemented in CIET as a fan-cooled heat exchanger with no actual power conversion system connection. Heat removal from the primary loop is therefore accomplished using a fan for which operators control signal frequency. Higher frequency fan operation then corresponds to a higher air mass flow rate and, therefore, greater convection heat transfer. The hot fluid flows out of the heater, through the hot leg piping, and down through the CTAH where it is cooled via convection with the outer piping. The user-controlled fan blows air over the piping. Figure 7.4 shows the CTAH and its heat transfer structures schematically.

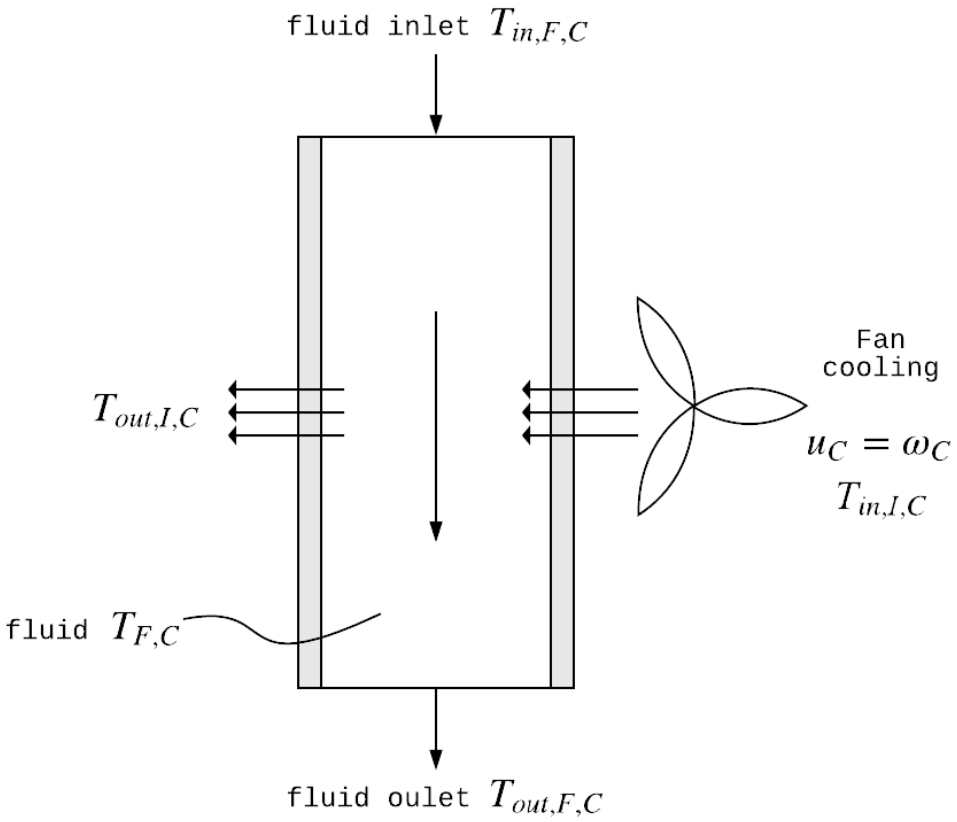

Figure 7.4: Diagram of the CTAH used to formulate case study model

The following CTAH model formulation begins by specifying the phenomena of interest, the parameters and unknown variables, the performance output of interest, and the inputs (note that these are currently CIET values and not FHR values, as shown in Appendix B):

- *Phenomena:* Power out of CTAH working fluid, power into ambient air blowing over CTAH piping, fan rotation driving air flow and convection heat transfer between CTAH working fluid and ambient air

- *Parameters:* Masses, specific heats, heat transfer areas, convection heat transfer coefficients, volumes, densities
- *Variables:* Temperatures, mass flow rates
- *Performance output:* CTAH outlet temperature
- *Input:* CTAH fan frequency

Our model then consists of two different expressions for the power across the CTAH:

$$P_C = \frac{dT_{F,C}}{dt}(Mc_p)_{F,C} + (\dot{m}c_p)_{F,C}(T_{In,F,C} - T_{Out,F,C}) \tag{7.10}$$

$$P_C = (\dot{m}c_p)_{I,C}(T_{In,I,C} - T_{Out,I,C}) \tag{7.11}$$

with air mass flow rate directly related to control input by

$$u_C = \omega_C \ , \ \dot{m}_{I,C} = f(\omega_C) \tag{7.12}$$

where

- P_C = power across the CTAH $[W]$
- $T_{F,C}$ = mean fluid temperature for CTAH $[^\circ C]$
- $(\dot{m}c_p)_{F,C}$ = mass flow rate times specific heat for Dowtherm A in CTAH $[W/^\circ C]$
- $T_{In,F,C}$ = inlet fluid temperature for CTAH $[^\circ C]$
- $T_{Out,F,C}$ = inlet fluid temperature for CTAH $[^\circ C]$
- $(\dot{m}c_p)_{I,C}$ = mass flow rate times specific heat for ambient air across CTAH $[W/^\circ C]$
- $T_{In,I,C}$ = inlet air temperature for CTAH fan $[^\circ C]$
- $T_{Out,I,C}$ = outlet air temperature for CTAH fan $[^\circ C]$
- u_C = control input to the CTAH
- ω_C = fan signal frequency $[Hz]$
- $f(\omega_C)$ = function between fan signal frequency and air mass flow rate $[kg/sHz]$

Like the heater, the power into the CTAH can be described by this model both in steady state and in transient power conditions. The model drops the term describing average temperature dynamics and thermal inertia of the ambient air due to its relative insignificance. Unlike the heater, the CTAH has no structural temperature measurements. There are rough empirical correlations for heat transfer coefficients but they are expected to vary in error at different operating conditions. For this reason, the first CTAH model implementation neglects to describe the convection heat transfer directly to avoid significant sources of uncertainty and error. Thermocouples measure the fluid temperature into and out of the CTAH as well as the CTAH fan inlet and outlet air temperatures. The primary loop flow meter measures mass flow rate. Figure 7.5 shows the corresponding DM decomposition of the CTAH structural model.

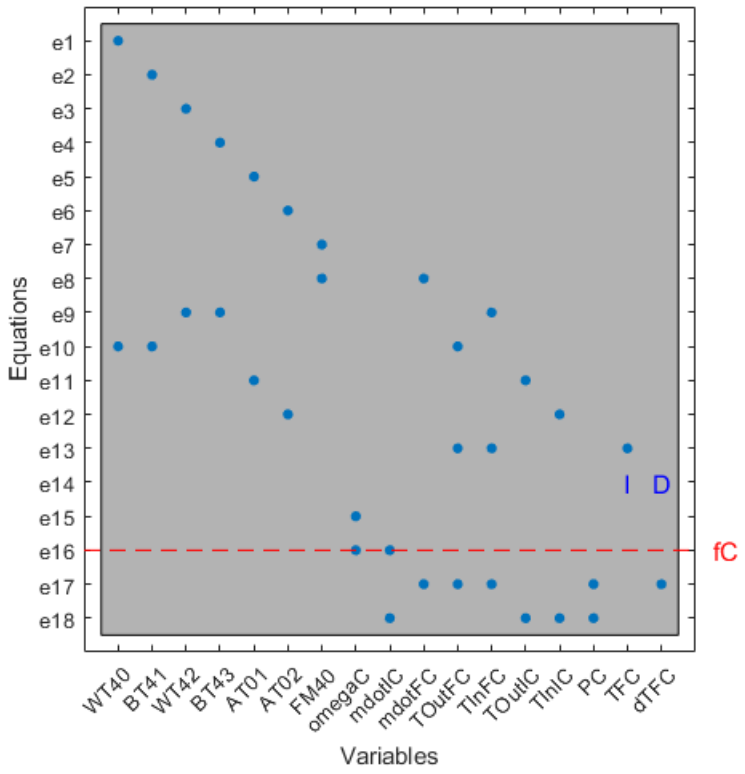

Figure 7.5: Dulmage-Mendelsohn decomposition of CIET CTAH structural model

Like the heater model, the CTAH model is entirely over-determined. As shown in Figure 7.5, however, it contains only one equivalence class. The CTAH model in its current form is primarily suitable for detecting one fault at a time. Faults in relevant temperature measurements, for example, are not structurally isolable from faults in fan operation using this model. The fault shown, however, is a fault that relates fan signal frequency to air mass flow rate. This fault is the focus of the case study due to the importance for operators to understand their control over CIET's primary heat exchanger. This model should provide

a signal for faults compromising the relationship between operator control and CTAH heat removal.

Modeling the thermocouple network CIET is instrumented with Type-T thermocouples [79] at key points to gain a thorough understanding of the working fluid's temperature profile through the primary loop and in the DRACS loop. There are two classifications for the thermocouples in CIET: WT or wall thermocouples and BT or bulk thermocouples, both inserted at the same axial location. Both WT and BT are inserted into the fluid but the WT thermocouples have smaller insertion depths and the BT thermocouples have larger insertion depths for the purpose of capturing radial temperature profile effects.

Because the FHR and CIET feature flow mixers after heating and cooling sections along the primary and DRACS loops, the following formulation assumes small variation in the radial temperature profile. Therefore, the model focuses on understanding loop temperatures from the axial direction only (along the flow path), assuming that averaging the WT and BT measurements adequately represents the bulk temperature. Furthermore, the model assumes that flow after mixers and bends becomes fully developed quickly, supporting a uniform treatment of different axial points along the flow path, distinguished only by the net heat transfer into the system between points. Each set of two thermocouple points can then be described as a "T_1" and a "T_2". Figure 7.6 shows the schematic for formulating a description of the relationship between two thermocouples.

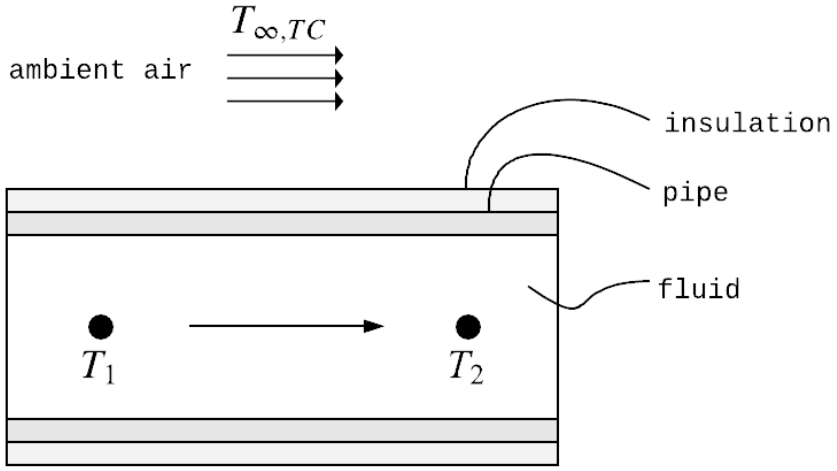

Figure 7.6: Diagram of two generalized thermocouples used to formulate case study model

The primary form of heat transfer along the loop piping and outside of the heat exchangers and heater is heat loss to ambient air outside of the pipe. It is important to note that this model neglects the effects of conduction along the pipe — a possible source of distortion during significant thermal transients but a minor effect at steady-state. There

is therefore a net heat loss in the fluid as it flows and exchanges heat via convection with the relatively cool solid piping material. The piping surface, in turn, exchanges heat with the fluid via convection and with its outer surface via conduction. CIET's piping is also covered in insulation which adds a second conduction layer. Finally, the outer surface of the pipe exchanges heat with ambient air via convection. There are no surface temperature measurements outside of the heater so it is difficult to know the pipe wall temperatures. It is unnecessary to describe the intermediate temperatures at the inner and outer pipe wall because an equivalent cylindrical thermal resistance network can be used to formulate a description of the relationship between fluid temperature and ambient temperature directly. Figure 7.7 shows this representation.

In the resistance network analogy, heat transfer is like current and temperature drop is like voltage drop. The overall equation for thermal power dissipated across the circuit in Figure 7.7 is

$$\dot{Q} = \frac{\Delta T}{R} \tag{7.13}$$

where R is the effective thermal resistance between two points and ΔT the temperature difference between those points. The resistances to heat transfer are simply

$$R = \frac{\Delta T}{\dot{Q}} \tag{7.14}$$

so that, in a cylindrical system,

$$R_{conv} = \frac{1}{2\pi r l h} \tag{7.15}$$

$$R_{cond} = \frac{ln(r_o/r_i)}{2\pi k l} \tag{7.16}$$

where h is the convection heat transfer coefficient, k the conduction heat transfer coefficient, r the radius of a convection layer, r_o the outer radius and r_i the inner radius of a conduction layer, and l the heat transfer surface length. Just like for a set of resistors in series, the total resistance between T_F and T_∞ can be described by

$$R = R_F + R_S + R_I + R_\infty = \frac{1}{2\pi r_i h_F l} + \frac{ln(r_o/r_i)}{2\pi k_S l} + \frac{ln(r_I/r_o)}{2\pi k_I l} + \frac{1}{2\pi r_I h_\infty l} \tag{7.17}$$

where the subscripts correspond to the labels on Figure 7.7 and the relationship between the two temperature measurements can be modeled. The focus of modeling is on the following phenomena, parameters, variables, performance output, and input:

- *Phenomena:* Convection heat transfer from fluid to pipe wall, conduction heat transfer from pipe inner wall to outer wall, conduction heat transfer from pipe outer wall to insulation surface, convection heat transfer from insulation surface to ambient air, fluid flow from T_1 to T_2

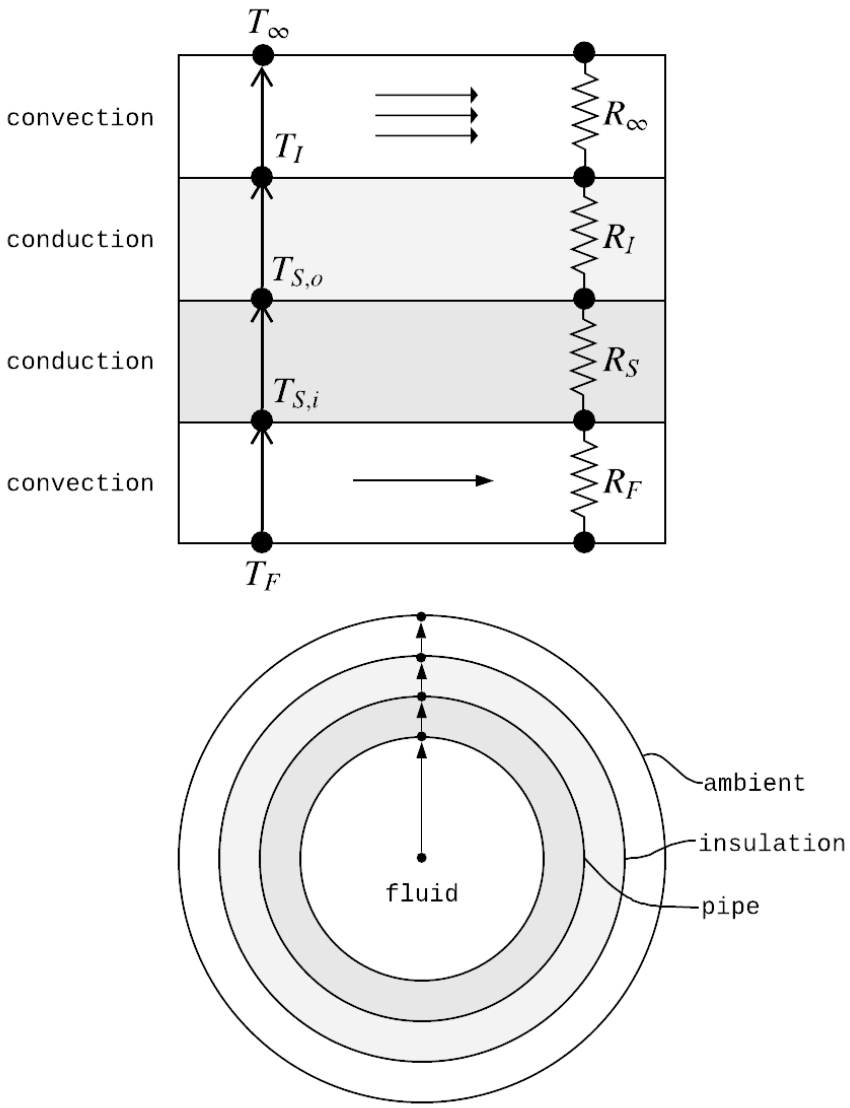

Figure 7.7: Thermocouple parasitic heat loss equivalent resistance network diagram

- *Parameters:* Masses, specific heats, heat transfer areas, convection heat transfer coefficients, conduction heat transfer coefficients, mass flow rate, pipe wall thickness, insulation wall thickness
- *Variables:* Fluid temperatures, pipe wall temperatures, ambient temperature
- *Performance output:* Fluid temperatures
- *Input:* None

The model can then be used to describe the relationship between T_1 and T_2 in terms of each other and of their loss to ambient air:

$$\dot{Q}_{TC} = (\dot{m}c_p)_{TC}(T_2 - T_1) \tag{7.18}$$

$$\dot{Q}_{TC} = \frac{T_\infty - T_{av}}{R} \tag{7.19}$$

$$T_{av} = \frac{T_1 + T_2}{2} \tag{7.20}$$

$$\frac{dT_1}{dt} = \frac{dT_2}{dt} \tag{7.21}$$

where

- $\dot{Q}_{TC}$ = heat loss to ambient between two thermocouple points $[W]$
- T_1 = upstream thermocouple location BT and WT average reading $[^\circ C]$
- T_2 = downstream thermocouple location BT and WT average reading $[^\circ C]$
- $(\dot{m}c_p)_{TC}$ = fluid mass flow rate times specific heat capacity between two thermocouple points $[W/^\circ C]$
- T_∞ = ambient air temperature outside pipe between two thermocouple points $^\circ C]$
- T_{av} = mean fluid temperature between two thermocouple points $^\circ C]$

T_1 and T_2 correspond to thermocouple measurements at any two points in CIET with no heat source or sink other than losses to ambient air. This model can therefore be applied at various sections of CIET and can even be applied to other plants as long as the user chooses parameters accordingly. Equation 7.21 is particularly important here because it establishes an expected relationship between the *dynamics* of each thermocouple's reading. Not only should their readings be related to one another, but they should exhibit similar dynamics.

There are a couple caveats to this model. First of all, depending on the rate of convection in the fluid, there may be a significant lag between T_2 and T_1 during heating and cooling transients. Second of all, this model does not allow the plant monitoring system to easily differentiate between faults affecting T_1 and faults affecting T_2 because it only describes relative behavior between them. These issues may be addressed with the introduction of additional rules (i.e. operating knowledge or expected dynamics based on plant status) but this chapter presents the above model for simplicity and generality. With this formulation, Figure 7.8 shows the DM decomposition of the general thermocouple network structural model.

The thermocouple network structural model consists of four equivalence classes corresponding to the key relationships described by the model. Starting from the top left, the equivalence classes relate to:

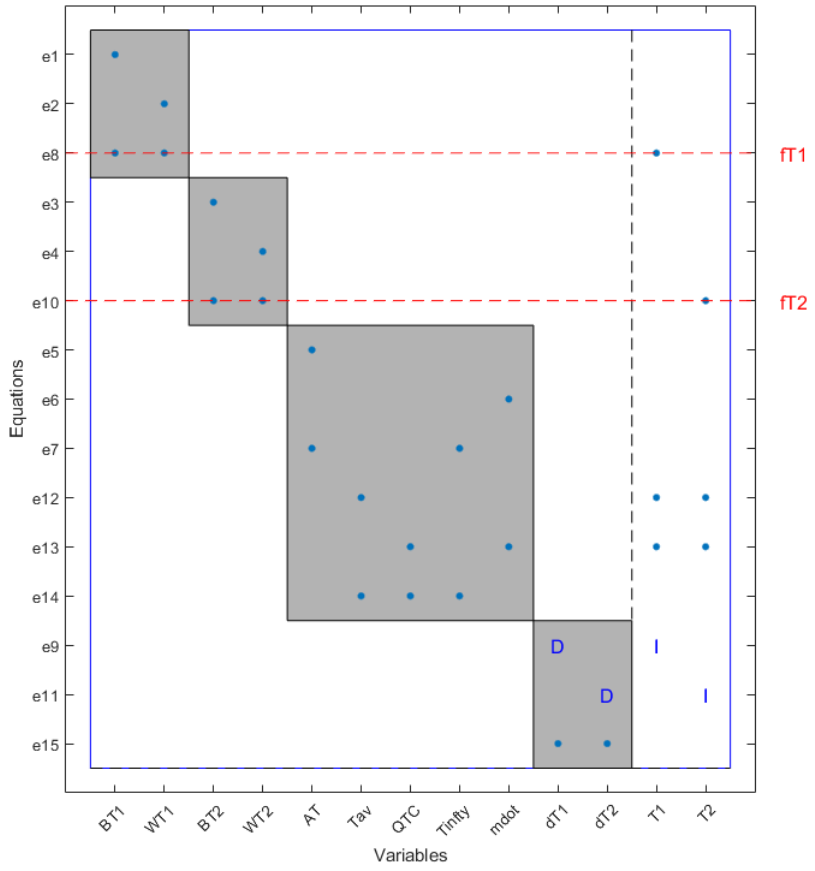

Figure 7.8: Dulmage-Mendelsohn decomposition of thermocouple network structural model

- T_1 measurements,
- T_2 measurements,
- heat losses to ambient air through the effective thermal resistance network,
- and thermocouple dynamics.

Noting that this model will likely suffer in detecting these faults during thermal transients, this simple formulation may prove interesting for assessing thermocouple calibration in general systems. One feature of the thermocouple model, as distinct from the heater and CTAH models, is that its measurements are not defined by specific thermocouples or flow meters. This chapter will show that the same model can be used to generate residuals for different faults as long as the unique parameters and inputs are well-defined. In this way, if a plant has many similar systems throughout, the plant designer can then tackle many similar faults with the same carefully chosen generic models.

Plant monitoring system implementation

In order to test and demonstrate the fault network methodology for industrial monitoring system development, this chapter presents the following faults of interest:

1. a fault in operator control of the heater causing a discrepancy between operator input power and actual power that may be the result of a control system malfunction or a cyber-attack,

2. a fault in CTAH fan operation resulting in reduced heat transfer and compromised operator control of primary loop heat removal that may be the result of a mechanical failure,

3. and a fault in temperature readings on the operators' HMI as the result of a cyber-attack, making it difficult for the operator to know which readings to trust. This chapter will present faults affecting both the primary loop hot leg temperature readings and also the DRACS loop temperature readings.

Fault 1. Heater Power Control Fault As shown in Figure 7.3 and Appendix A, the heater fault, f_H, is included in the input equation

$$u_H = P_H + f_H \tag{7.22}$$

to demonstrate that the fault affects heater power control specifically. If the fault affected the as-described heater physics, for example, it would be better placed in a different equation.

The heater power control fault is structurally detectable in the heater model as shown in Figure 7.3. The key to detecting this fault is, using the model and available measurements, to estimate the actual power and compare the estimated value to the power value input by the operator. Using the Fault Diagnostics Toolbox to generate a residual generator, Figure 7.9 shows a simplified diagram of the heater control fault signal generation algorithm.

It is important to note that, for selecting a residual generator with the ability to describe the heater dynamics and not only its steady-state operation, the only options with the given model are high-index problems. This means that the model, as formulated, would pose difficulties for quickly designing an observer-based residual generator. In the future, to capture dynamics while ensuring the residual signal generator options are low-index, alternative model types would be useful. For example, a table of values for different power trajectories versus temperature rates of change could be generated from experimental data to remove the need for actual integration and differentiation. Alternatively, case logic involving descriptions of empirical thermal time-dependent behavior given certain conditions could be implemented for additional detail. There is no problem, however, with using a sequential residual generator for this case study.

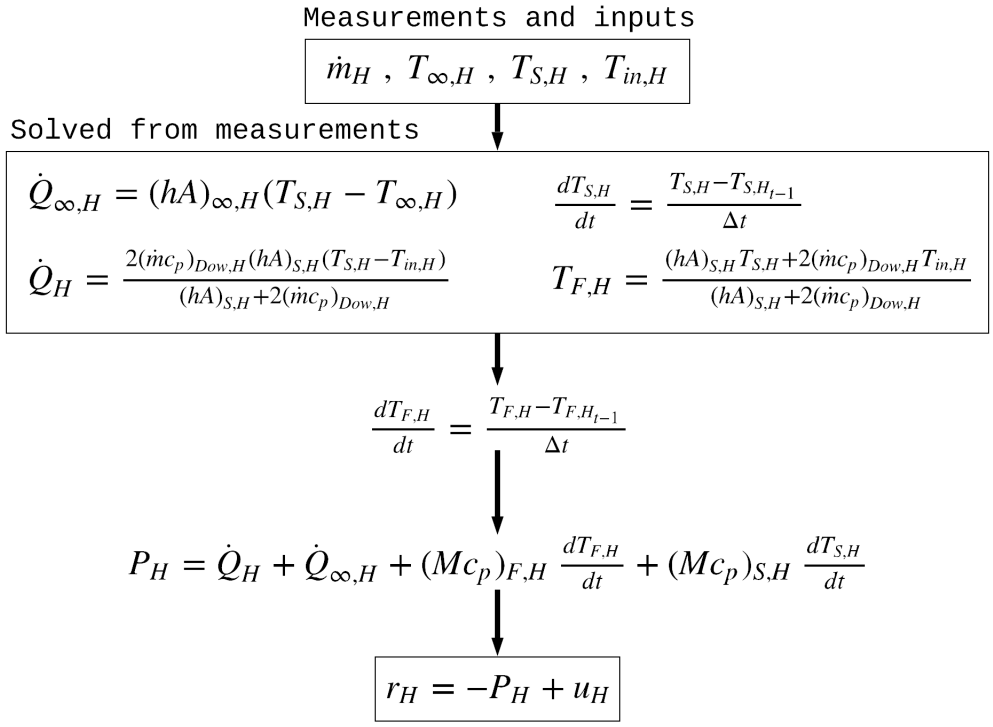

Figure 7.9: Simplified diagram of the heater fault residual generator

Fault 2. CTAH Heat Removal Fault As shown in Figure 7.5 and Appendix A, the CTAH fault, f_C, is included in the equation describing the relationship between CTAH fan signal frequency and air mass flow rate

$$\dot{m}_{I,C} = f(\omega_C) + f_C \tag{7.23}$$

to demonstrate that the fault affects the physical relationship between fan signal frequency and air mass flow rate as opposed to the control signal itself. If the fault were a cyber-attack overriding CTAH fan control, for example, it would be better placed in an equation like that of the heater fault.

The CTAH heat removal control fault is structurally detectable in the CTAH model as shown in Figure 7.5. For this fault, the main solution path is to calculate the power removed from the fluid and compare that to the required air mass flow rate and, consequently, operator input needed to achieve that air mass flow rate. If the values disagree, there is likely a fault affecting the fan's ability to remove heat as designed. Figure 7.10 shows a simplified diagram of the CTAH control fault signal generation algorithm.

The CTAH model is relatively simple compared to the heater model and therefore produces low-index residual signal generators. For that reason, the CTAH model is amenable to observer-based residual generator schemes.

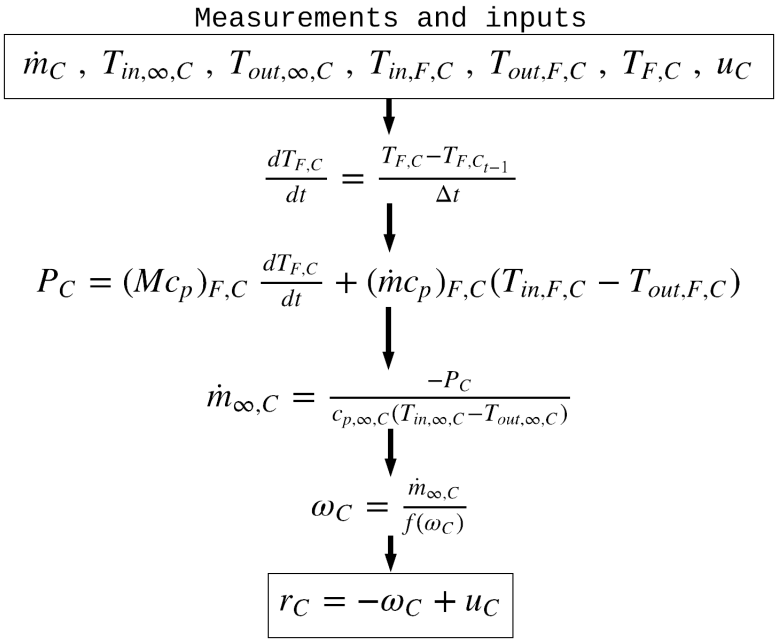

Figure 7.10: Simplified diagram of the CTAH fault residual generator

Fault 3. Temperature Measurement Faults As shown in Figure 7.8 and Appendix A, the thermocouple faults, f_{T_1} and f_{T_2}, are included in the respective equations defining T_1 and T_2

$$T_1 = \frac{BT_1 + WT_1}{2} + f_{T_1} \tag{7.24}$$

$$T_2 = \frac{BT_2 + WT_2}{2} + f_{T_2} \tag{7.25}$$

to demonstrate that the fault affects the measurements of T_1 and T_2 directly as opposed to any physical phenomenon that influences their reading. If the faults affected the rate of heat transfer to ambient air, for example, they would be better placed in equations like those describing $\dot{Q}_{TC}$.

The temperature measurement faults are structurally detectable in the thermocouple network model as shown in Figure 7.8. Even though the faults are structurally isolable from one another, the solution paths that enable isolability neglect the temperature measurements themselves, making the model very unstable in the face of transient conditions. For these faults, complementary solution paths are likely to yield the best results to differentiate and characterize their occurrence.

The first solution path, shown in Figure 7.11, uses only the dynamics of the temperature measurements to detect faults. Factoring in the dynamics requires not only calculation of

rates of change at each time step but also forecasting the progression of the temperature at each time step and checking it against the next measurement. This residual signal generator applies to T_1 because T_1 is the upstream thermocouple location and will "see" any dynamics driven by incoming flow before T_2 does. It will still generate fault signals for f_{T_2}, however, because it relies on measurements of T_1.

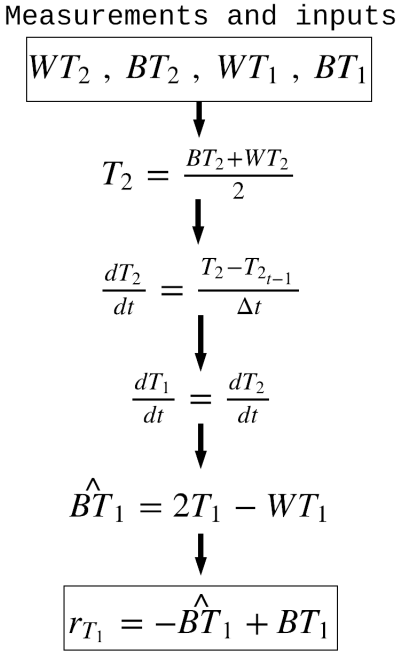

Figure 7.11: Simplified diagram of the thermocouple 1 fault residual generator

The second solution path, shown in Figure 7.12, uses the definition of the equivalent thermal resistance network and the power between the thermocouples to check for consistency between T_1 and T_2. Unlike the first solution path shown in Figure 7.11, the second path does not use feedback or dynamics and checks only the values at each time step against each other. The path shown in Figure 7.12 applies to f_{T_2} but, as for the first solution path, will also generate fault signals for f_{T_1} because it relies on measurements of T_1.

While neither of the above two residual signal generators reinforce structural isolability for each fault, they may still provide unique signals for different faults in practice.

Decision Support Trial The CTAH fault is a good candidate for the decision support concepts introduced by Chapter 4 because it represents a mechanical fault in which a control relationship *deteriorates* but is not completely compromised. The as-designed physical relationship changes and it is difficult for the operator to continue controlling the plant with confidence without significant trial and error. Because, in CIET, the role of the CTAH is to use fan speed control to maintain a constant outlet temperature (and therefore a constant

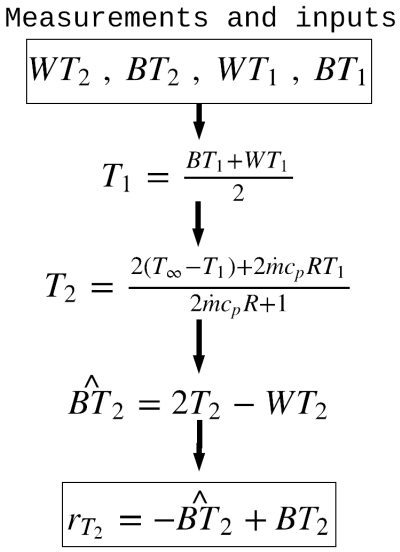

Figure 7.12: Simplified diagram of the thermocouple 2 fault residual generator

heater inlet temperature), the ability for the operator to determine if they can still control the plant accordingly is imperative. The same algorithm that generates the fault signal for the CTAH fault can also provide predictions of CTAH outlet temperatures for given operator actions. Reordering the same equations from Figure 7.10 yields an algorithm that takes the current plant state and hypothetical operator input frequency and uses the newly-identified relationship between signal frequency and air mass flow rate $\dot{m}_{\infty,C} = f(\omega_C) + f_C$ to calculate the expected corresponding $T_{out,F,C}$. Figure 7.13 shows the algorithm that enables the operator to test-drive controls even in situations with altered plant configuration.

One important note about this predictive algorithm is that it can be used in two different ways. The first way is for the operator to predict the immediate *dynamic* plant response to hypothetical control inputs. In other words, $\frac{d}{dt} \neq 0$ and the term influences the output over an operator-specified forecast time Δt. Because the predictive algorithm is not over-determined, further definition of the dynamic CTAH term $\frac{dT_{F,C}}{dt}$ would ensure much greater confidence in dynamic predictions. As shown in Figure 7.10, the value of $\frac{dT_{F,C}}{dt}$ comes from the current time step and therefore influences the calculated output over the entire chosen Δt. Since the CTAH typically operates at steady-state and $\frac{dT_{F,C}}{dt} = 0$ outside of temporary excursions, larger Δt likely results in larger prediction uncertainty and error.

For this reason, without explicit models of the CTAH fluid thermal dynamics, the algorithm is better-suited for predictions of new steady-state outputs. This causes $\frac{dT_{F,C}}{dt} = 0$ and

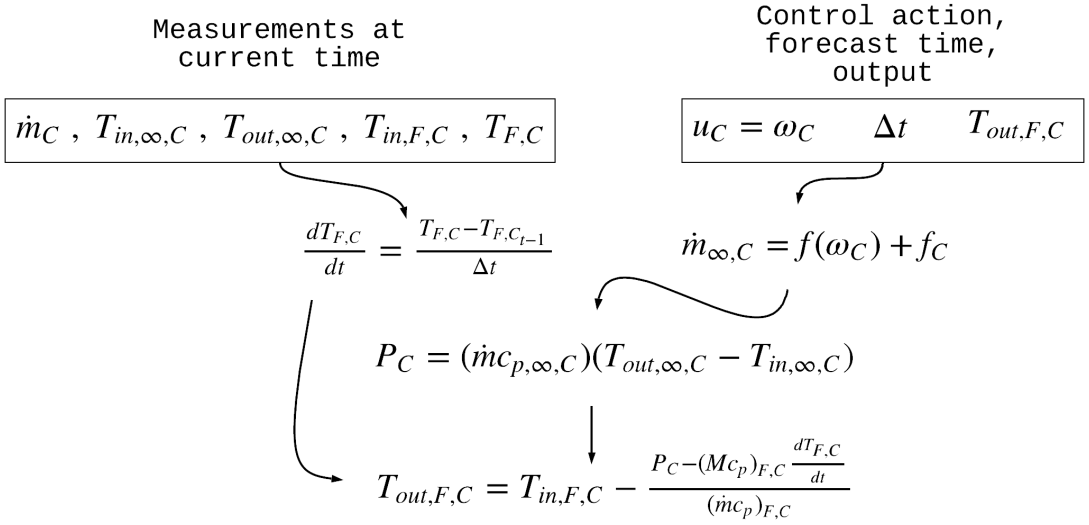

Figure 7.13: Simplified diagram of the CTAH fault residual generator

$$T_{out,F,C} = T_{in,F,C} - \frac{P_C - \frac{dT_{F,C}}{dt}(Mc)_{p_F,C}}{(\dot{m}c_p)_{F,C}} \rightarrow T_{out,F,C}\left(\frac{dT_{F,C}}{dt} = 0\right) = T_{in,F,C} - \frac{P_C}{(\dot{m}c_p)_{F,C}} \quad (7.26)$$

so that the solution does not rely on modeled transient behavior. The operator might be interested in alternative input-output relationships such as the temperature drop across the CTAH $\left|T_{in,F,C} - T_{out,F,C}\right|$ in the case of changing inlet conditions or the change in power across the CTAH for a different primary loop mass flow rate. This same model allows the operator to test control actuations using the same basic principles.

After the operator has been able to improve their understanding of faulted plant state by testing different control actuations or hypothetical changes in conditions, they may seek to steer the plant toward some desired goal. Continuing to focus on maintaining a CTAH outlet temperature of $T_{out,F,C}$, the operator wants to minimize the discrepancy between the actual value $\hat{T}_{out,F,C}$ and that target value. Following the discussion from Chapter 4, this can be formulated as the following optimization problem:

$$\begin{aligned} \min_{u \in U} \quad & \left|\hat{T}_{out,F,C} - T_{out,F,C}\right| \\ \text{s.t.} \quad & \dot{m}_{\infty,C} = f(\omega_C) + f_C \\ & \text{CTAH model} \\ & x \in X,\, u \in U \end{aligned} \quad (7.27)$$

where the set of possible control actions U is

$$u_C = \omega_C \ , 0 \leq \omega_C \leq 60 \ [Hz] \tag{7.28}$$

and all other values internal to the optimization problem are defined by the plant model described in this chapter and in Appendix A.

This optimization problem takes the output of the residual generator algorithm in Figure 7.10 and calculates the optimal control value u_C^* that minimizes $|\hat{T}_{out,F,C} - T_{out,F,C}|$. Due to the constraint posed by the set of possible control actions U, it is possible that there exist conditions and values of f_C for which no value of u_C^* causes $|\hat{T}_{out,F,C} - T_{out,F,C}| \approx 0$. In this case, the operator can readily decide whether the plant must be shut down or whether there are other control candidates, such as primary loop mass flow rate, that might be brought into the optimization. It may also be the case that the plant state is dynamic and the optimal value works at first but then under- or over-shoots the target value of $T_{out,F,C}$. It is likely that the operator will wish to perform the optimization multiple times to ensure desired plant performance. Notably, this methodology also provides the necessary algorithm to implement continuous online fault-resilient optimal control.

Case study description

The case study ARCO-CIET experiment to demonstrate this dissertation's proposed plant monitoring system methodology has the following steps (with all values in terms of actual CIET setpoints rather than scaled FHR values):

1. Operators bring CIET up to 8000 W of heater power and primary loop flow rate of 0.18 kg/s
2. Fault 1.1: heater power override to 1000 W, ARCO HMI power indicator spoof to stay at 8000 W
3. The Supervisor monitors fault signal generators in NOAH and makes them visible on the Left Overview display for the other operators by flagging them as active if they appear active
4. The control room staff discusses Fault 1.1 before the heater power control and indication return to their fault-free states
5. Fault 1.2: heater power override to 5000 W, ARCO HMI spoof to stay at 8000 W
6. As before, the Supervisor monitors NOAH and shares the fault signal generator graphs when appropriate
7. The control room staff discusses Fault 1.2 and the heater power control and indication return to their fault-free states

8. The Reactor operator now controls CTAH to achieve an outlet fluid temperature of 80 $°C$

9. Fault 2.1: physical obstruction of CTAH fan air inlet, no changes to the control system or HMIs

10. The Supervisor monitors and shares information as appropriate

11. The control room staff discusses Fault 2.1 and the physical obstruction is removed from the CTAH

12. The same sequence is repeated for Fault 2.2 and Fault 2.3

13. With CIET back to fault-free operation, the operators control CIET to approximate steady-state at 8000 W heater power, 0.18 kg/s primary loop mass flow rate, and 80 $°C$ CTAH outlet fluid temperature

14. Fault 3.1: WT indicator at the DHX outlet spoof to 80 $°C$ with no physical or control change to CIET. Importantly, the DRACS loop is valved off for this experiment and rests close to ambient temperature conditions.

15. The control room staff handles the fault as they did the others and fault-free operation is restored

16. Faults 3.2-3.4 occur, corresponding respectively to the BT indicator at the DHX outlet, the WT indicator at the TCHX inlet, and the BT indicator at the TCHX inlet

17. Finally, Faults 4.1-4.4 are the same as Faults 3.1-3.4 except that they affect the heater outlet and CTAH inlet thermocouple measurements with spoof values of 120 $°C$.

The purpose of this experimental design is to demonstrate a variety of fault types and effects while showcasing the applicability of the above-described plant monitoring tools to real-time on-line fault detection and identification.

Results and Discussion

This section will first present the response of all residual signals over the course of the test to demonstrate fault detectability and isolability before presenting in detail the response of each signal to its specific faults. All residual signal generators run online during the test and calculate residual values every 1.5 seconds. This timestep ensures that residual generation does not attempt to interrogate the plant state more often than data and control signals update. The heater power only updates every second.

Figure 7.14 shows each residual signal over the course of the test (start-up and shutdown activities occur before and the after the displayed time window) in separate subplots with

each fault labeled according to the numbering in the previous section. Faults 1.1-1.2 are the heater faults, Faults 2.1-2.3 are the CTAH faults, Faults 3.1-3.4 are the DRACS temperature measurement faults, and Faults 4.1-4.4 are the hot leg temperature measurement faults. The values of the residual signals are normalized through dividing their residual quantities by the expected quantities they estimate. Ideally, each signal will detect the fault it was designed to detect with a signal magnitude distinct from its non-detection value. Figure 7.14 therefore shows the response of each residual signal to not only the faults they were designed to detect but also to the faults outside of their design focus.

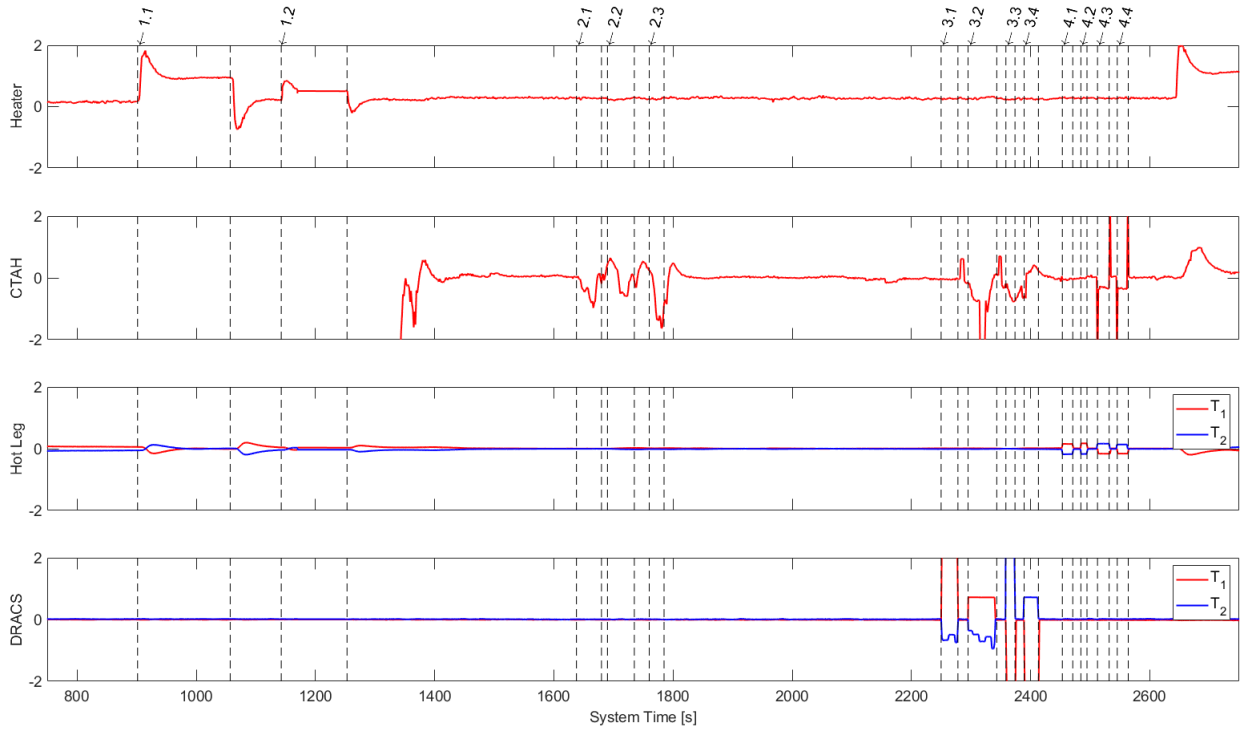

Figure 7.14: Fault diagnostic data analysis from 2019-05-15 Fault Detection III test

The heater residual provides clear detection of the two heater faults. Its value is relatively consistent and does not appear to be sensitive to any other faults, supporting good isolability of power input faults as distinct from the others tested. The jump in the residual signal at the end of the interval is likely due to shutdown activities rather than a fault.

The CTAH residual only becomes relevant partway through the test when the operator actually activates the CTAH. It is clearly sensitive to the three CTAH faults (with some delay) but is also sensitive to other faults in the test. The fluctuations during faults 3.1-3.4 are actually due to fluctuations in the CTAH frequency rather than the faults. This data provides evidence that the CTAH residual is very sensitive to the CTAH frequency and therefore may be difficult to use during frequency transients. It then seems quite sensitive to the hot leg temperature measurement faults. This is an intuitive result because those

Residual	$\mathbf{f_H}$	$\mathbf{f_C}$	$\mathbf{f_{T_{1,DRACS}}}$	$\mathbf{f_{T_{2,DRACS}}}$	$\mathbf{f_{T_{1,HotLeg}}}$	$\mathbf{f_{T_{2,HotLeg}}}$
Heater	X					
CTAH		X			X	X
$T_{1,DRACS}$			X	X		
$T_{2,DRACS}$			X	X		
$T_{1,HotLeg}$	X				X	X
$T_{2,HotLeg}$	X				X	X

Table 7.2: Residual signal fault detectability and isolability summary table

measurements feed into the CTAH model, which likely would require adjustment to isolate CTAH heat removal degradation faults from temperature spoofs. It is important to note that none of the other fault signals are sensitive to the CTAH fault, meaning that it still proves invaluable for the specific fault it was designed to detect.

The hot leg temperature measurement residual signals have very low magnitude throughout the experiment but still show discernible response during two sets of faults: the heater faults and the hot leg temperature measurement faults. Similarly to the isolability conflict in the CTAH, the hot leg temperature measurement residual relies on some of the same variables affected by the heater faults. The jumps in the hot leg temperature measurement fault signal seem to correspond to the heater residual's overshoot before settling to non-detect levels once again. This means that the hot leg temperature measurement residual probably fails to capture the short-term dynamics of the hot leg temperatures during power transients. In contrast, the signal jumps immediately during the hot leg faults and stays constant while the faults are active. It is therefore useful for detecting and isolating hot leg faults.

The DRACS temperature measurement residual signals also have very low magnitude throughout most of the test but exhibit strong responses to the DRACS temperature measurement faults. This is likely due to a combination of factors: the DRACS loop is valved off during the experiment and therefore does not have competing effects outside of these faults, the temperature measurement residual generator does not capture external forces which is an excellent approximation for the DRACS loop in these conditions, and the magnitude of the DRACS temperature spoofs is four times that of the actual temperatures, giving an extreme case to test the fault signal generator. Nevertheless, the DRACS loop temperature measurement residual signal performs excellently.

Table 7.2 summarizes the detectability and isolability results for each fault, marking an "X" for each fault to which the residual is sensitive. Note that, for this table, detectability of multiple faults by one residual signal does not mean that the detection signals for those faults are not unique and distinguishable from each other. Furthermore, combinations of residual signals may be used to fully establish confidence in the identity of a single fault.

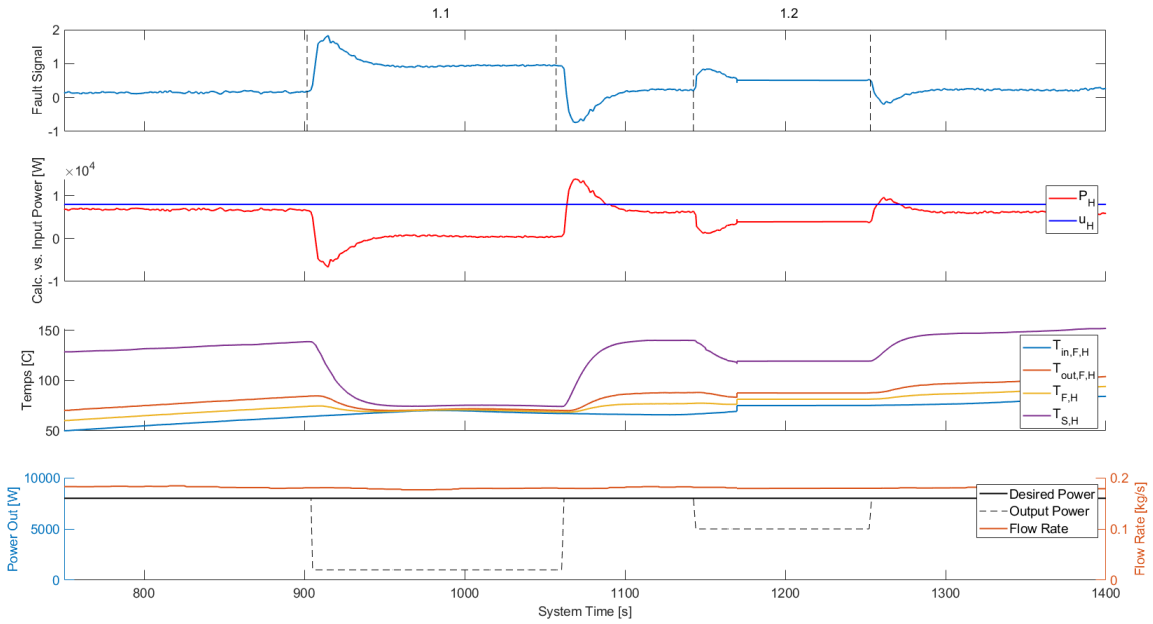

Figure 7.15: Heater fault diagnostic data analysis from 2019-05-15 Fault Detection III test

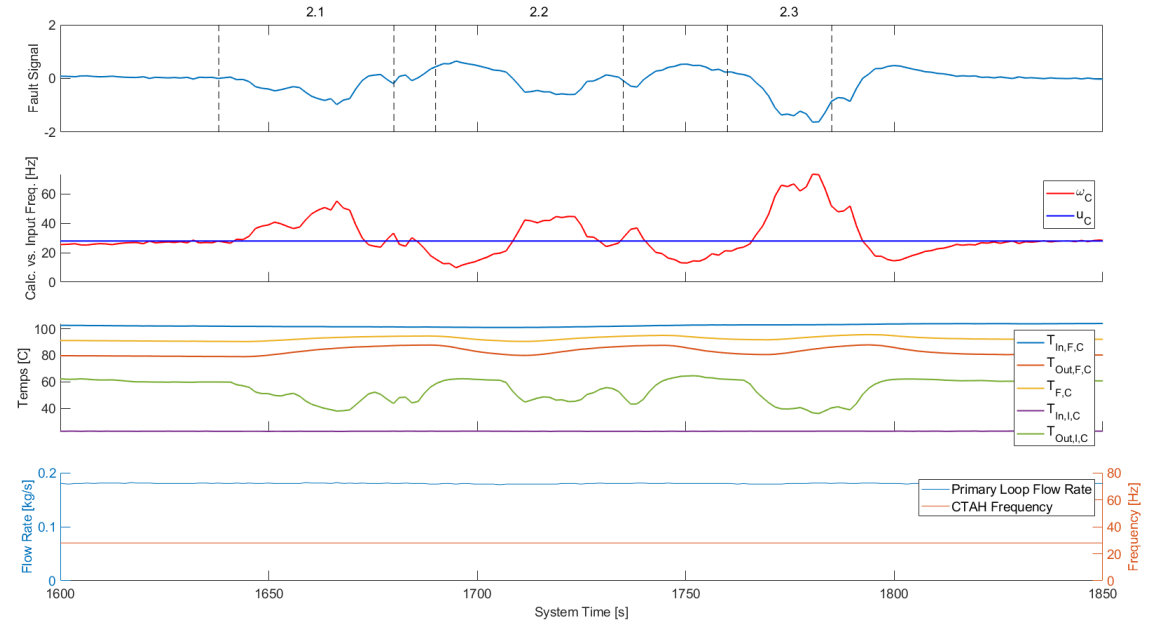

Figure 7.16: CTAH fault diagnostic data analysis from 2019-05-15 Fault Detection III test

Figure 7.15 shows the response of the heater residual generator to heater faults 2.1 and 2.2. The top plot shows the residual and fault start and stop times. The second plot shows

the model-calculated P_H based on operating conditions and the input u_C for comparison. The third plot shows the relevant heater temperatures used in the model and the fourth plot shows the relevant control variables: input heater power, actual output heater power, and primary loop mass flow rate.

The fault signal provides very quick detectability for the two faults with magnitude corresponding qualitatively to the higher and lower magnitude power discrepancies and proves quite stable during fault-free operation. The residual has a significant overshoot effect at the onset and end of each fault before settling at a constant value. This is likely due to the difficulty in characterizing power transients without an explicit formulation of the heater solid and fluid thermal time response. The model also seems to persistently under-predict heater power. As discussed earlier, the thermophysical properties of Dowtherm A vary strongly with temperature but the model uses average values. This residual generator is an excellent tool for detecting faults in heater control but may need additional modeling work to be used for decision support applications.

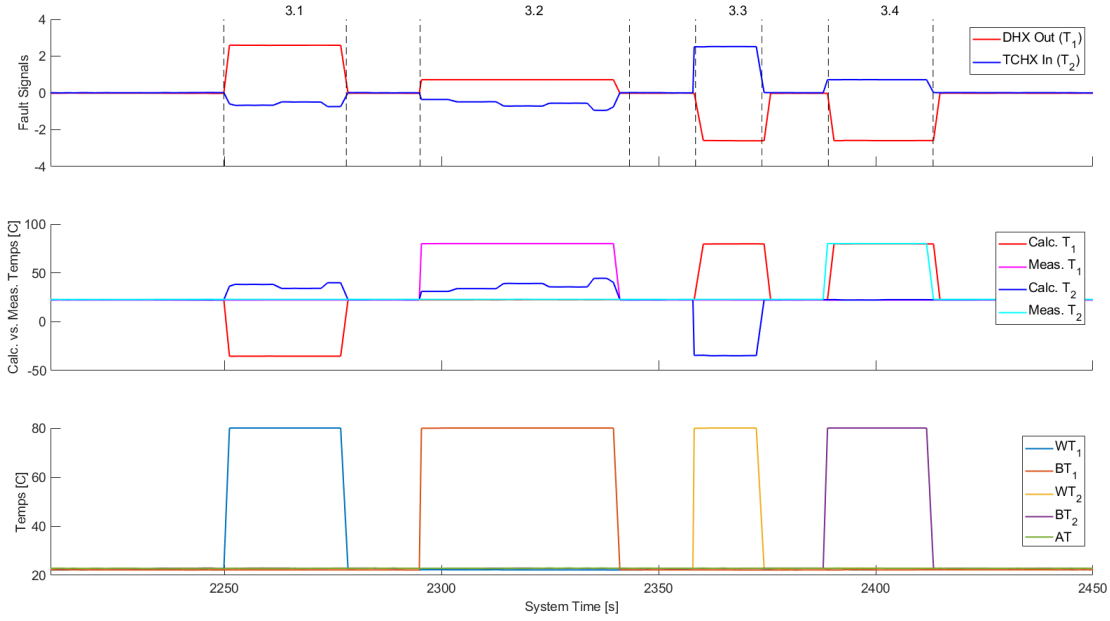

Figure 7.17: DRACS temperature measurement fault diagnostic data analysis from 2019-05-15 Fault Detection III test

Figure 7.16 shows the response of the CTAH residual generator to CTAH faults 2.1-2.3. As in Figure 7.15, the top plot shows the residual, the second plot shows the calculated ω_C compared to the input u_C, the third plot shows the model-relevant CTAH temperatures and the fourth plot shows the CTAH-relevant control signals. The CTAH residual hovers right around zero during fault-free operation and deviates noticeably during faults. Its response lags fault initiation times a bit but the CTAH faults are physically initiated by placing an object in front of the CTAH fan air intake rather than digitally initiated via a step function.

The CTAH model predicts ω_C almost perfectly during fault-free operation which means that it may be the ideal candidate to demonstrate decision support capabilities.

Figure 7.17 shows the response of the DRACS temperature measurement residual generator during faults 3.1-3.4. The top plot shows the DHX Out and TCHX In residual signal generators, the second plot shows model-calculated T_1 and T_2 along with the measured values, and the third plot shows the relevant individual thermocouple data. Both residual signal generators are sensitive to all four faults but exhibit different responses, meaning that T_1 and T_2 faults may still be isolable from one another. The T_1 residual generator gives a positive value for T_1 faults and a negative value for T_2 faults. It estimates the value of the faults quite well (keeping in mind that the faults only occur in a BT or WT thermocouple at once and the model averages the two quantities) and maintains a constant value due to its ability to capture dynamics. The T_2 residual generator likewise goes negative during T_1 faults and positive during T_2 faults. It exhibits less stable behavior. This is likely due to the very low temperature difference between different points in the DRACS loop during the test. The residual generator proves useful for detecting thermocouple measurement faults and even provides a criterion for differentiating between faults in T_1 and T_2.

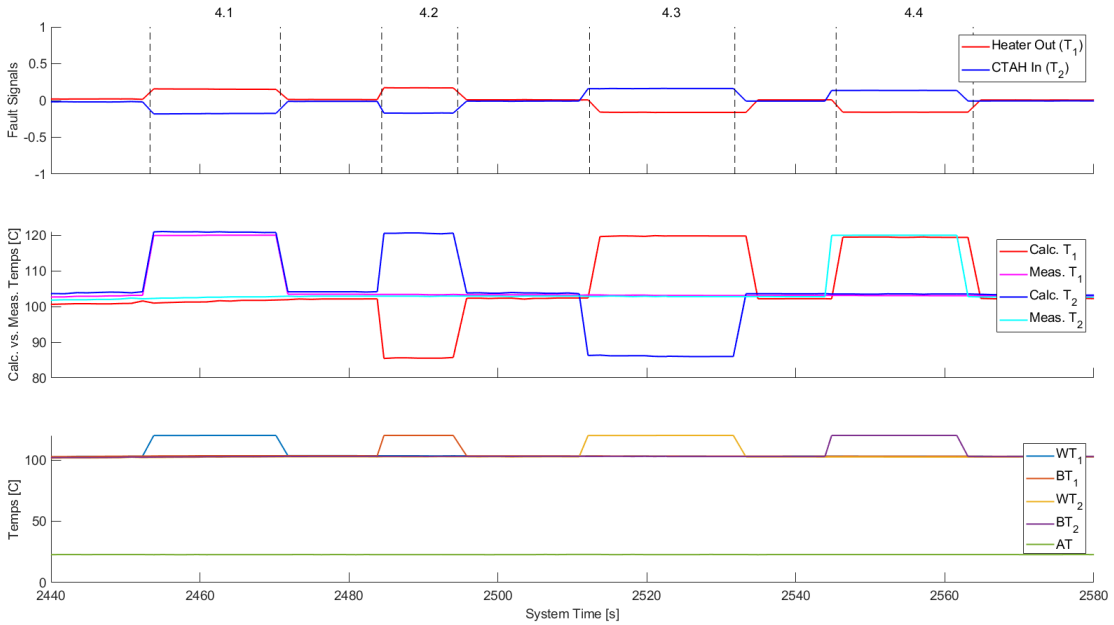

Figure 7.18: Hot leg temperature measurement fault diagnostic data analysis from 2019-05-15 Fault Detection III test

Figure 7.18 shows the response of the hot leg temperature measurement residual generator during faults 4.1-4.4. The top plot shows the Heater Out (T_1) and CTAH In (T_2) residual generators, the second plot shows the model-calculated T_1 and T_2 values along with the corresponding measurements, and the third plot shows the relevant thermocouple data. The hot leg results are very similar to those of the DRACS loop with the main difference

being the relatively small magnitude of the hot leg temperature spoofs (about 20 $°C$) vs. the DRACS temperature spoofs (about 60 $°C$). Like the DRACS loop fault signals, the T_1 signal is positive for T_1 faults and negative for T_2 faults and the T_2 signal exhibits the opposite behavior. The hot leg fault results show that the temperature measurement residual generator may be limited to relatively significant temperature spoofs before it becomes important to better incorporate outside dynamics (i.e. heater power heating the primary loop fluid).

Altogether, each residual generator is able to detect the faults for which it was designed and some even closely capture the quantitative fault value. Through an iterative design process, these models can likely be adapted to facilitate fault-resilient operation in industrial facilities.

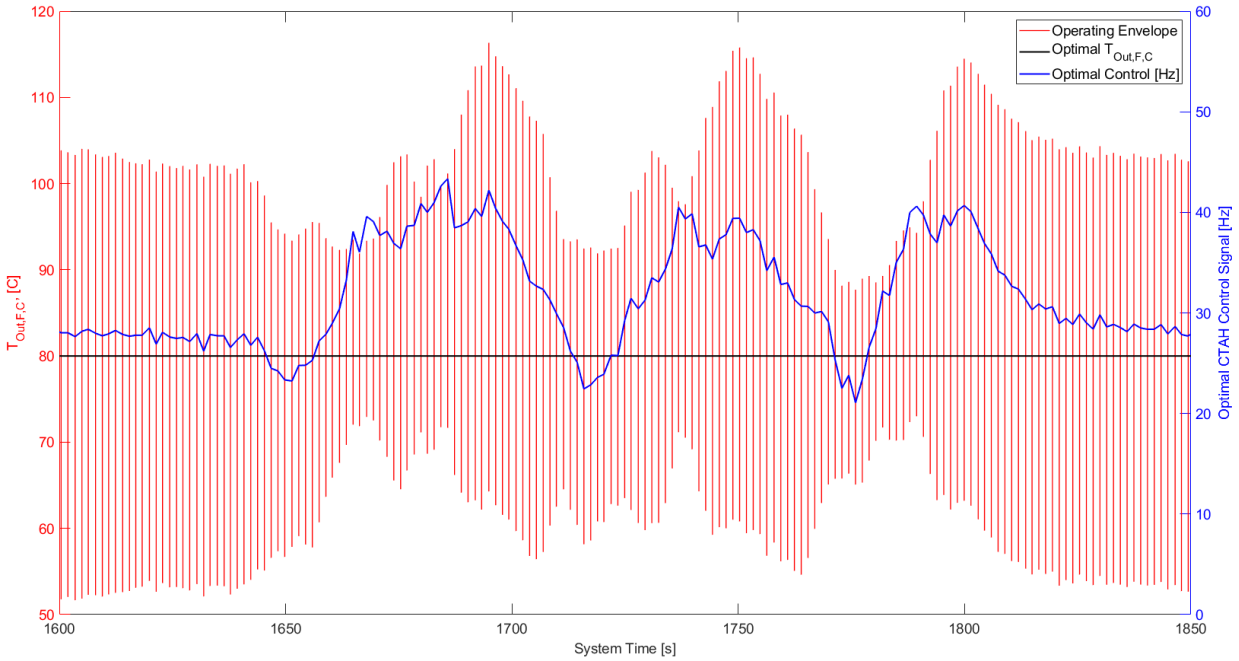

Figure 7.19: Decision support data showing possible control outcomes and optimal control routine in 2019-05-15 Fault Detection III test

Figure 7.19 demonstrates the CTAH residual generator reformulated to allow operators to test control outcomes, to run on-line optimal control algorithms, and to obtain optimal control inputs. The red vertical lines (corresponding to the left y-axis) show, at each point in time during the CTAH fault detection portion of the experiment, the reachable set of possible $T_{out,F,C}$ using the controllable CTAH fan. The highest-temperature values correspond to input frequencies of 0 Hz and the lowest-temperature values correspond to input frequencies of 60 Hz. The model calculated these values using a steady-state formulation so it does not account for the settling time for the plant before reaching these temperatures.

The blue line gives the optimal control action that the operator would use in looking to maintain 80 $°C$ CTAH outlet temperatures. This optimization uses the MATLAB `fmincon`

function in the same format as Equation 7.27. The optimal control value stays, throughout the entire CTAH fault portion of the experiment, greater than 0 Hz and less than 60 Hz. Vitally, the optimal value that ARCO recommends to the operator incorporates the diagnosed fault information to yield safe performance and maintain short-term ideal operation. This means that, in contrast to conventional disturbance rejection methods [128], the control system can assist the operator in steering plant operation even during faults without masking the faults in the process. The black line at $T_{out,F,C} = 80°C$ shows that, for the entire CTAH fault portion of the experiment, the operator can acquire an optimal input value to deliver the ideal operational goal. If the optimization yielded maximum or minimum CTAH values or informed the operator that the plant could not reach the setpoint outlet temperature, the operator might need to make a determination to shut down the plant.

The results of this case study are very promising in demonstrating the applicability of the fault network methodology to the design of industrial plant monitoring systems. Furthermore, this chapter presents models that are relatively simple and easily adaptable to similar plants through the substitution of relevant geometry and parameter information. The above results required some iterative development over the course of multiple tests but each test provided valuable insight into the fundamental physics of the plant.

Chapter 8

Conclusions

This chapter first reiterates the main takeaways from the preceding dissertation before discussing gaps and future work. The chapter then presents potential applications for the reader interested in adapting and building on this work.

Main takeaways This dissertation presents a methodology for developing a network of diverse plant models that builds context between various physical phenomena to enable a consistent physical description of the as-designed plant. It then describes how plant monitoring system designers can leverage the models to provide formulaic fault diagnostic algorithms suitable for online, real-time computation. Next, the dissertation demonstrates how the same algorithms can support plant operators' decision making by allowing them to "test drive" control actuations and determine optimal control inputs needed to steer the plant as they desire. The second half of the dissertation focuses in on the Fluoride salt-cooled High temperature Reactor (FHR) to demonstrate the methodology and its implementation in the Advanced Reactor Control and Operations (ARCO) facility. Chapter 7 describes multiple simple models suitable plant monitoring system design and shows the result of using them for online fault diagnostics and operator support.

The case study results demonstrate strong promise for simple, physics-based models to support operators' ability to detect and identify plant faults. In some cases, the operators may even be able to quantify the faults' effects and use them to plan and optimize control routines during continuous operation. Performing iterative experimentation and development for the models used in plant monitoring systems will be invaluable to establish confidence and understand the effects of uncertainty, signal noise, and model error. In many cases, the process will lead to a much richer understanding of the key phenomena and variables in plant processes.

Gaps and future work There are a few key ways to carry this research forward. Some promising areas include:

- Each of the individual component-level models can be compiled into a full-plant model that enables plant monitoring system designers to design for structural detectability, isolability, and computational efficiency using the context of the entire plant's available information. For example, models of relationships between thermocouples can be added to components with well-characterized heat transfer mechanisms, such as in the Compact Integral Effects Test (CIET) heater, to better differentiate between faults affecting different physical phenomena.

- To more accurately capture thermophysical properties, models of thermophysical property temperature dependence can be added to reduce uncertainty and error.

- Additional models describing the transient response of thermal structures will enable residuals to more quickly and accurately capture sudden fault initiation.

- The model network should be supplemented with additional, diverse models such as those requiring external software that can be used to handle sophisticated input-output relationships and data-based models that approximate relationships with physics that are difficult or impossible to model analytically.

- Systematic studies of residual sensitivity to different faults, with quantitative comparison between different residual generators using the same models, will enable the plant monitoring designer to optimize their signal set to provide the best signal differentiation for each individual fault.

- Residuals should be tested for multiple fault detection to characterize their response during plant operation events with competing effects.

- Fault prognostics models will support operators in projecting both the short- and long-term evolution of plant state after fault initiation. Furthermore, fault prognostics models will assist plant owners with condition-based maintenance planning.

- Testing plant monitoring technologies using experimental facilities and human operators will best approximate real-life situations and allow plant monitoring system designers to evaluate and iteratively improve both the algorithmic and human-machine interface implementation of their systems.

Applications This dissertation seeks to provide the reader with a detailed walkthrough of plant monitoring system design that can be readily adapted to a variety of industrial plants. Many processes would benefit from increased understanding of their physical phenomena and many owners and operators would benefit from being able to predict, mitigate, and prevent faulted operation. Furthermore, this methodology can be applied at different phases in the development process.

In the theoretical development phase, the model network methodology guides personnel in organizing and compiling various forms of plant modeling information. They also will

crystallize their goals and priorities in a systematic fashion to guide experimental design and iterative progress. In some cases, difficulties in fully characterizing possible faults may lead to plant design change recommendations or facilitate the formulation of models with multiple uses.

In the prototyping phase, the model network methodology enables specification of the capabilities and deficiencies of a physical system related to fault resiliency and controllability. The control system designers can also develop the optimal balance between human control and automaton by testing the plant monitoring system human machine interface. With a sophisticated plant monitoring system, the operators may be able to take on more sophisticated tasks and computational data tracking and logging may becomes much more efficient. Designers can also test the resiliency of plant operation during hypothetical cyber-attacks or digital control system failures.

In the operational phase, the model network methodology facilitates control system upgrades and maintenance planning. There may be significant potential in existing industrial facilities to implement simple algorithms and support operators in their existing supervisory tasks. Facility owners may also be able to amend maintenance policies, assess plant state, and interrogate instrumentation performance without physical modification or invasive inspection of the plant. This is likely both the most straightforward and most promising area of application for the work presented by this dissertation.

Bibliography

[1] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & information systems engineering*, vol. 6, no. 4, pp. 239–242, 2014.

[2] V. L. Winter, R. S. Berg, and J. T. Ringland, "Bay area rapid transit district advance automated train control system case study description," in *High integrity software*, pp. 115–135, Springer, 2001.

[3] N. Orenstein, "'troubleshooting on the fly': Riding in the cab with a bart operator," Mar 2019.

[4] I. Roumeliotis, N. Aretakis, and A. Alexiou, "Industrial gas turbine health and performance assessment with field data," *Journal of Engineering for Gas Turbines and Power*, vol. 139, no. 5, p. 051202, 2017.

[5] A. Hajat, C. Hsia, and M. S. O'Neill, "Socioeconomic disparities and air pollution exposure: a global review," *Current environmental health reports*, vol. 2, no. 4, pp. 440–450, 2015.

[6] C. E. E. Hess and W. C. Ribeiro, "Energy and environmental justice: Closing the gap," *Environmental Justice*, vol. 9, no. 5, pp. 153–158, 2016.

[7] P. M. Mannucci, S. Harari, I. Martinelli, and M. Franchini, "Effects on health of air pollution: a narrative review," *Internal and emergency medicine*, vol. 10, no. 6, pp. 657–662, 2015.

[8] B. C. O'Neill, E. Kriegler, K. L. Ebi, E. Kemp-Benedict, K. Riahi, D. S. Rothman, B. J. van Ruijven, D. P. van Vuuren, J. Birkmann, K. Kok, *et al.*, "The roads ahead: Narratives for shared socioeconomic pathways describing world futures in the 21st century," *Global Environmental Change*, vol. 42, pp. 169–180, 2017.

[9] P. A. Kharecha and J. E. Hansen, "Prevented mortality and greenhouse gas emissions from historical and projected nuclear power," *Environmental science & technology*, vol. 47, no. 9, pp. 4889–4895, 2013.

[10] M. Lehtveer and F. Hedenus, "Nuclear power as a climate mitigation strategy–technology and proliferation risk," *Journal of Risk Research*, vol. 18, no. 3, pp. 273–290, 2015.

[11] M. B. Roth and P. Jaramillo, "Going nuclear for climate mitigation: An analysis of the cost effectiveness of preserving existing us nuclear power plants as a carbon avoidance strategy," *Energy*, vol. 131, pp. 67–77, 2017.

[12] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring," *Mechanical Systems and Signal Processing*, vol. 115, pp. 213–237, 2019.

[13] E. Frisk, M. Krysander, and D. Jung, "A toolbox for analysis and design of model based diagnosis systems for large scale models," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3287–3293, 2017.

[14] M. Schluse, M. Priggemeyer, L. Atorf, and J. Rossmann, "Experimentable digital twins—streamlining simulation-based systems engineering for industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1722–1731, 2018.

[15] T. Ulrich, S. Werner, R. Lew, and R. Boring, "Cossplay: validating a computerized operator support system using a microworld simulator," in *International Conference on Human-Computer Interaction*, pp. 161–166, Springer, 2016.

[16] A. Ayodeji, Y.-k. Liu, and H. Xia, "Knowledge base operator support system for nuclear power plant fault diagnosis," *Progress in Nuclear Energy*, vol. 105, pp. 42–50, 2018.

[17] Z. Liu and H. He, "Sensor fault detection and isolation for a lithium-ion battery pack in electric vehicles using adaptive extended kalman filter," *Applied Energy*, vol. 185, pp. 2033–2044, 2017.

[18] W. Turner, A. Staino, and B. Basu, "Residential hvac fault detection using a system identification approach," *Energy and Buildings*, vol. 151, pp. 1–17, 2017.

[19] P. A. Delgado-Arredondo, D. Morinigo-Sotelo, R. A. Osornio-Rios, J. G. Avina-Cervantes, H. Rostro-Gonzalez, and R. de Jesus Romero-Troncoso, "Methodology for fault detection in induction motors via sound and vibration signals," *Mechanical Systems and Signal Processing*, vol. 83, pp. 568–589, 2017.

[20] K. M. Groth and E. S. Hecht, "Hyram: A methodology and toolkit for quantitative risk assessment of hydrogen systems," *International Journal of Hydrogen Energy*, vol. 42, no. 11, pp. 7485–7493, 2017.

[21] J. Zhu, Z. Ge, and Z. Song, "Distributed parallel pca for modeling and monitoring of large-scale plant-wide processes with big data," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 4, pp. 1877–1885, 2017.

[22] A. C. Cilliers, "Correlating hardware fault detection information from distributed control systems to isolate and diagnose a fault in pressurised water reactors," *Annals of Nuclear Energy*, vol. 54, pp. 91–103, 2013.

[23] A. K. Jardine, D. Lin, and D. Banjevic, "A review on machinery diagnostics and prognostics implementing condition-based maintenance," *Mechanical systems and signal processing*, vol. 20, no. 7, pp. 1483–1510, 2006.

[24] R. Ayo-Imoru and A. Cilliers, "A survey of the state of condition-based maintenance (cbm) in the nuclear power industry," *Annals of Nuclear Energy*, vol. 112, pp. 177–188, 2018.

[25] J. B. Coble, P. Ramuhalli, L. J. Bond, W. Hines, and B. Upadhyaya, "Prognostics and health management in nuclear power plants: a review of technologies and applications," tech. rep., Pacific Northwest National Lab.(PNNL), Richland, WA (United States), 2012.

[26] J. Coble, P. Ramuhalli, L. J. Bond, J. Hines, and B. Ipadhyaya, "A review of prognostics and health management applications in nuclear power plants," *International Journal of prognostics and health management*, vol. 6, p. 016, 2015.

[27] J. Ma and J. Jiang, "Applications of fault detection and diagnosis methods in nuclear power plants: A review," *Progress in nuclear energy*, vol. 53, no. 3, pp. 255–266, 2011.

[28] S. Yin, S. X. Ding, X. Xie, and H. Luo, "A review on basic data-driven approaches for industrial process monitoring," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 11, pp. 6418–6428, 2014.

[29] M. G. Fernandez, A. Tokuhiro, K. Welter, and Q. Wu, "Nuclear energy system's behavior and decision making using machine learning," *Nuclear Engineering and Design*, vol. 324, pp. 27–34, 2017.

[30] R. Ayo-Imoru and A. Cilliers, "Continuous machine learning for abnormality identification to aid condition-based maintenance in nuclear power plant," *Annals of Nuclear Energy*, vol. 118, pp. 61–70, 2018.

[31] M.-j. Peng, H. Wang, S.-s. Chen, G.-l. Xia, Y.-k. Liu, X. Yang, and A. Ayodeji, "An intelligent hybrid methodology of on-line system-level fault diagnosis for nuclear power plant," *Nuclear Engineering and Technology*, vol. 50, no. 3, pp. 396–410, 2018.

[32] A. C. Cilliers, *A deterministic approach for establishing a narrow band dynamic operating envelope to detect and locate hardware deterioration in nuclear power plants*. PhD thesis, North-West University, 2013.

[33] T. H.-J. Uhlemann, C. Lehmann, and R. Steinhilper, "The digital twin: Realizing the cyber-physical production system for industry 4.0," *Procedia Cirp*, vol. 61, pp. 335–340, 2017.

[34] Z. Ge, Z. Song, S. X. Ding, and B. Huang, "Data mining and analytics in the process industry: The role of machine learning," *IEEE Access*, vol. 5, pp. 20590–20616, 2017.

[35] "Computer codes," Aug 2018.

[36] R. Vilim, Y. Park, A. Heifetz, W. Pu, S. Passerini, and A. Grelle, "Monitoring and diagnosis of equipment faults," *Nucl. Eng. Int*, vol. 58, p. 24, 2013.

[37] D. Wang, K.-L. Tsui, and Q. Miao, "Prognostics and health management: A review of vibration based bearing and gear health indicators," *IEEE Access*, vol. 6, pp. 665–676, 2018.

[38] W. Kim and S. Katipamula, "A review of fault detection and diagnostics methods for building systems," *Science and Technology for the Built Environment*, vol. 24, no. 1, pp. 3–21, 2018.

[39] G.-Y. Lee, M. Kim, Y.-J. Quan, M.-S. Kim, T. J. Y. Kim, H.-S. Yoon, S. Min, D.-H. Kim, J.-W. Mun, J. W. Oh, *et al.*, "Machine health management in smart factory: A review," *Journal of Mechanical Science and Technology*, vol. 32, no. 3, pp. 987–1009, 2018.

[40] S. Yazdekhasti, K. R. Piratla, S. Atamturktur, and A. Khan, "Experimental evaluation of a vibration-based leak detection technique for water pipelines," *Structure and Infrastructure Engineering*, vol. 14, no. 1, pp. 46–55, 2018.

[41] J.-x. Cai, X. Zhou, Z.-l. Pan, P.-g. Gao, Y.-x. Luo, and Z.-x. Lin, "Study on the design and control of pipeline leak detection robot fish," *Cybernetics and Information Technologies*, vol. 18, no. 3, pp. 120–131, 2018.

[42] S. W. Glass, L. S. Fifield, N. Bowler, A. Sriraman, and W. C. Palmer, "Interdigital capacitance local non-destructive examination of nuclear power plant cable for aging management programs," 2018.

[43] D. Jung, H. Khorasgani, E. Frisk, M. Krysander, and G. Biswas, "Analysis of fault isolation assumptions when comparing model-based design approaches of diagnosis systems," *IFAC-PapersOnLine*, vol. 48, no. 21, pp. 1289–1296, 2015.

[44] L. J. Kangas, F. L. Greitzer, and O. Illi Jr, "Tedann: turbine engine diagnostic artificial neural network," tech. rep., Pacific Northwest Lab., Richland, WA (United States), 1994.

[45] X. Wu, X. Hu, S. Moura, X. Yin, and V. Pickert, "Stochastic control of smart home energy management with plug-in electric vehicle battery energy storage and photovoltaic array," *Journal of Power Sources*, vol. 333, pp. 203–212, 2016.

[46] X. Hu, S. J. Moura, N. Murgovski, B. Egardt, and D. Cao, "Integrated optimization of battery sizing, charging, and power management in plug-in hybrid electric vehicles," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 1036–1043, 2016.

[47] J. Zhang and J. Lee, "A review on prognostics and health monitoring of li-ion battery," *Journal of Power Sources*, vol. 196, no. 15, pp. 6007–6014, 2011.

[48] A. Cordoba-Arenas, S. Onori, and G. Rizzoni, "A control-oriented lithium-ion battery pack model for plug-in hybrid electric vehicle cycle-life studies and system design with consideration of health management," *Journal of Power Sources*, vol. 279, pp. 791–808, 2015.

[49] S. Yin, H. Luo, and S. X. Ding, "Real-time implementation of fault-tolerant control systems with performance optimization," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 5, pp. 2402–2411, 2014.

[50] Y. Han, J. D. Biggs, and N. Cui, "Adaptive fault-tolerant control of spacecraft attitude dynamics with actuator failures," *Journal of Guidance, Control, and Dynamics*, vol. 38, no. 10, pp. 2033–2042, 2015.

[51] S. K. Kommuri, M. Defoort, H. R. Karimi, and K. C. Veluvolu, "A robust observer-based sensor fault-tolerant control for pmsm in electric vehicles," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 12, pp. 7671–7681, 2016.

[52] L. Li, H. Luo, S. X. Ding, Y. Yang, and K. Peng, "Performance-based fault detection and fault-tolerant control for automatic control systems," *Automatica*, vol. 99, pp. 308–316, 2019.

[53] D. Jung and Q. Ahmed, "Active fault management in autonomous systems using sensitivity analysis," *IFAC-PapersOnLine*, vol. 51, no. 24, pp. 1099–1104, 2018.

[54] C. Zhang, P. Tang, N. Cooke, V. Buchanan, A. Yilmaz, S. W. S. Germain, R. L. Boring, S. Akca-Hobbins, and A. Gupta, "Human-centered automation for resilient nuclear power plant outage control," *Automation in Construction*, vol. 82, pp. 179–192, 2017.

[55] R. Vilim, A. Grelle, R. Lew, T. Ulrich, R. Boring, and K. Thomas, "Computerized operator support system and human performance in the control room," in *Proceedings of the 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2017)*, pp. 1195–1204, 2017.

[56] R. Westrum, "Automation, information and consciousness in air traffic control," in *Automation and systems issues in air traffic control*, pp. 367–380, Springer, 1991.

[57] G. I. Rochlin, "Safe operation as a social construct," *Ergonomics*, vol. 42, no. 11, pp. 1549–1560, 1999.

[58] J. Nelles, S. Kuz, A. Mertens, and C. M. Schlick, "Human-centered design of assistance systems for production planning and control: The role of the human in industry 4.0," in *2016 IEEE International Conference on Industrial Technology (ICIT)*, pp. 2099–2104, IEEE, 2016.

[59] F. Longo, L. Nicoletti, and A. Padovano, "Smart operators in industry 4.0: A human-centered approach to enhance operators' capabilities and competencies within the new smart factory context," *Computers & industrial engineering*, vol. 113, pp. 144–159, 2017.

[60] A. Moniz and B.-J. Krings, "Robots working with humans or humans working with robots? searching for social dimensions in new human-robot interaction in industry," *Societies*, vol. 6, no. 3, p. 23, 2016.

[61] J. Nicas and J. Caswell, "Boeing's 737 max: 1960s design, 1990s computing power and paper manuals," *The New York Times*, p. A1, Apr 2019.

[62] A. Anokhin, A. Ivkin, and S. Dorokhovich, "Application of ecological interface design in nuclear power plant (npp) operator support system," *Nuclear Engineering and Technology*, vol. 50, no. 4, pp. 619–626, 2018.

[63] M. Kim, Y. Kim, H. Kim, W. Piao, and C. Kim, "Operator decision support system for integrated wastewater management including wastewater treatment plants and receiving water bodies," *Environmental Science and Pollution Research*, vol. 23, no. 11, pp. 10785–10798, 2016.

[64] S. Makris, P. Karagiannis, S. Koukas, and A.-S. Matthaiakis, "Augmented reality system for operator support in human–robot collaborative assembly," *CIRP Annals*, vol. 65, no. 1, pp. 61–64, 2016.

[65] R. L. Boring, V. Agarwal, J. C. Joe, and J. J. Persensky, "Digital full-scope mockup of a conventional nuclear power plant control room, phase 1: installation of a utility simulator at the idaho national laboratory," *INL/EXT-12-26367*, 2012.

[66] R. Boring, T. Ulrich, R. Lew, C. Kovesdi, B. Rice, C. Poresky, Z. Spielman, and K. Savchenko, "Analog, digital, or enhanced human-system interfaces? results of an operator-in-the-loop study on main control room modernization for a nuclear power plant," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2017.

[67] B. P. Hallbert and T. Kenneth, "Advanced instrumentation, information, and control systems technologies research in support of light water reactors," 2014.

[68] A. Al Rashdan, R. Lew, L. Hanes, C. Kovesdi, R. Boring, B. Rice, and T. Ulrich, "Control room modernization early design study for the palo verde nuclear generating station," *INL/LTD*, vol. 16, p. 39901, 2016.

[69] K. Le Blanc, Z. Spielman, and R. Hill, "A human automation interaction concept for a small modular reactor control room," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2017.

[70] "Advanced small modular reactors (smrs)."

[71] C. Andreades, *Nuclear Air-Brayton Combined Cycle Power Conversion Design, Physical Performance Estimation and Economic Assessment*. PhD thesis, UC Berkeley, 2015.

[72] R. Wood, "Advanced reactor licensing: Experience with digital i and c technology in evolutionary plants," tech. rep., ORNL (US). Funding organisation: US Department of Energy (United States), 2004.

[73] C. Forsberg, "Future innovations for fluoride-salt-cooled high-temperature reactors (fhrs)," in *Proc. of ANS Winter Meeting 2017*, pp. 1097–1100, 2017.

[74] L. R. Huddar, *Heat Transfer in Pebble-Bed Nuclear Reactor Cores Cooled by Fluoride Salts*. PhD thesis, UC Berkeley, 2016.

[75] L. Huddar, J. C. Kendrick, C. Poresky, X. Wang, and P. F. Peterson, "Application of frequency response methods in separate and integral effects tests for molten salt cooled and fueled reactors," *Nuclear Engineering and Design*, vol. 329, pp. 3–11, 2018.

[76] C. Poresky, "Frequency response testing in the ciet facility," Master's thesis, University of California, Berkeley, Berkeley, CA, May 2017.

[77] G. Buster, R. Sawadichai, M. Laufer, and P. Peterson, *Control Blade Insertion Dynamics in Pebble-Bed Fluoride-Salt-Cooled High-Temperature Reactors*. Department of Nuclear Engineering, University of California, Berkeley, 2015.

[78] C. Andreades, A. T. Cisneros, J. K. Choi, A. Chong, M. Fratoni, S. Hong, L. R. Huddar, K. D. Huff, D. Krumwiede, M. R. Laufer, *et al.*, "Technical description of the 'mark 1'pebble-bed fluoride-salt-cooled high-temperature reactor (pb-fhr) power

plant," *Department of Nuclear Engineering, UC Berkeley, Report UCBTH-14-002*, 2014.

[79] B. R. Upadhyaya, M. R. Lish, J. W. Hines, and R. A. Tarver, "Instrumentation and control strategies for an integral pressurized water reactor," *Nuclear Engineering and Technology*, vol. 47, no. 2, pp. 148–156, 2015.

[80] L. Chi and B. Zhang, "Managing i&c obsolescence for nuclear power plant life extension," in *Proc. of 2nd International Symposium on Nuclear Power Plant Life Management*, pp. 160–162, 2007.

[81] C. Poresky, C. Andreades, J. Kendrick, and P. Peterson, "Cyber security in nuclear power plants: Insights for advanced nuclear technologies," *Department of Nuclear Engineering, University of California, Berkeley, Publication UCBTH-17-004*, 2017.

[82] D. Rotondo, F. Nejjari, and V. Puig, "A virtual actuator and sensor approach for fault tolerant control of lpv systems," *Journal of Process Control*, vol. 24, no. 3, pp. 203–222, 2014.

[83] D. G. Eisenhut, "Inadequate core cooling instrumentation system (generic letter no. 82-28)," Dec 1982.

[84] J. P. Cassar and M. Staroswiecki, "A structural approach for the design of failure detection and identification systems.," *IFAC Proceedings Volumes*, vol. 30, no. 6, pp. 841–846, 1997.

[85] M. Krysander and M. Nyberg, "Structural analysis utilizing mss sets with application to a paper plant," tech. rep., LINKOEPING UNIV (SWEDEN), 2002.

[86] S. Ploix, M. Désinde, and S. Touaf, "Automatic design of detection tests in complex dynamic systems," *IFAC Proceedings Volumes*, vol. 38, no. 1, pp. 478–483, 2005.

[87] B. Pulido and C. A. González, "Possible conflicts: a compilation technique for consistency-based diagnosis," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 34, no. 5, pp. 2192–2206, 2004.

[88] E. Frisk, M. Krysander, and J. Åslund, "Sensor placement for fault isolation in linear differential-algebraic systems," *Automatica*, vol. 45, no. 2, pp. 364–371, 2009.

[89] A. Rosich, E. Frisk, J. Aslund, R. Sarrate, and F. Nejjari, "Fault diagnosis based on causal computations," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 42, no. 2, pp. 371–381, 2012.

[90] E. Frisk, A. Bregon, J. Aslund, M. Krysander, B. Pulido, and G. Biswas, "Diagnosability analysis considering causal interpretations for differential constraints," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 42, no. 5, pp. 1216–1229, 2012.

[91] M. Krysander, J. Åslund, and M. Nyberg, "An efficient algorithm for finding minimal overconstrained subsystems for model-based diagnosis," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 1, pp. 197–206, 2008.

[92] M. Krysander and E. Frisk, "Sensor placement for fault diagnosis," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 38, no. 6, pp. 1398–1410, 2008.

[93] H. Khorasgani, D. E. Jung, G. Biswas, E. Frisk, and M. Krysander, "Robust residual selection for fault detection," in *53rd IEEE Conference on Decision and Control*, pp. 5764–5769, IEEE, 2014.

[94] A. L. Dulmage and N. S. Mendelsohn, "Coverings of bipartite graphs," *Canadian Journal of Mathematics*, vol. 10, pp. 517–534, 1958.

[95] M. Krysander, J. Åslund, and E. Frisk, "A structural algorithm for finding testable sub-models and multiple fault isolability analysis," in *21st International Workshop on Principles of Diagnosis (DX-10), Portland, Oregon, USA*, pp. 17–18, 2010.

[96] E. Frisk, M. Krysander, and J. Åslund, "Analysis and design of diagnosis systems based on the structural differential index," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 12236–12242, 2017.

[97] N. Li, Y. Lei, T. Yan, N. Li, and T. Han, "A wiener-process-model-based method for remaining useful life prediction considering unit-to-unit variability," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 3, pp. 2092–2101, 2019.

[98] E. Zio, "Reliability engineering: Old problems and new challenges," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 125–141, 2009.

[99] N. Li, N. Gebraeel, Y. Lei, L. Bian, and X. Si, "Remaining useful life prediction of machinery under time-varying operating conditions based on a two-factor state-space model," *Reliability Engineering & System Safety*, vol. 186, pp. 88–100, 2019.

[100] N. Li, Y. Lei, J. Lin, and S. X. Ding, "An improved exponential model for predicting remaining useful life of rolling element bearings," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7762–7773, 2015.

[101] L. Liao and F. Köttig, "A hybrid framework combining data-driven and model-based methods for system remaining useful life prediction," *Applied Soft Computing*, vol. 44, pp. 191–199, 2016.

[102] D. Zhang, S. Dey, H. E. Perez, and S. J. Moura, "Remaining useful life estimation of lithium-ion batteries based on thermal dynamics," in *2017 American Control Conference (ACC)*, pp. 4042–4047, IEEE, 2017.

[103] H.-C. Liu, L. Liu, and N. Liu, "Risk evaluation approaches in failure mode and effects analysis: A literature review," *Expert systems with applications*, vol. 40, no. 2, pp. 828–838, 2013.

[104] V. Boyko, N. Rudnichenko, S. Kramskoy, Y. Hrechukha, and N. Shibaeva, "Concept implementation of decision support software for the risk management of complex technical system," in *Advances in Intelligent Systems and Computing*, pp. 255–269, Springer, 2017.

[105] J. Rodrigues, L. Perera, and C. Guedes Soares, "Decision support system for the safe operation of fishing vessels in waves," in *Maritime Engineering and Technology*, pp. 153–161, Taylor & Francis Group, 2012.

[106] A. Arnaiz, S. Ferreiro, and M. Buderath, "New decision support system based on operational risk assessment to improve aircraft operability," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 224, no. 3, pp. 137–147, 2010.

[107] A. Alfonsi, C. Rabiti, D. Mandelli, J. Cogliati, R. Kinoshita, and A. Naviglio, "Dynamic event tree analysis through raven," tech. rep., Idaho National Laboratory (INL), 2013.

[108] A. Hakobyan, T. Aldemir, R. Denning, S. Dunagan, D. Kunsman, B. Rutt, and U. Catalyurek, "Dynamic generation of accident progression event trees," *Nuclear Engineering and Design*, vol. 238, no. 12, pp. 3457–3467, 2008.

[109] D. Mandelli, C. Smith, C. Rabiti, A. Alfonsi, R. Youngblood, V. Pascucci, B. Wang, D. Maljovec, P. Bremer, T. Aldemir, *et al.*, "Dynamic pra: an overview of new algorithms to generate, analyze and visualize data," *Proceeding of American Nuclear Society*, 2013.

[110] R. Gauntt, D. Kalinich, J. Cardoni, J. Phillips, A. Goldmann, S. Pickering, M. Francis, K. Robb, L. Ott, D. Wang, *et al.*, "Fukushima daiichi accident study (status as of april 2012)," *Sandia Report Sand*, vol. 6173, 2012.

[111] T. Fei, D. Ogata, K. Pham, M. Solom, C. Zhao, C. Xu, A. Cheng, C. Eastridge, M. Foxe, B. Reinhart, *et al.*, "A modular pebble-bed advanced high temperature reactor," *NE-170 Senior Design Project, Report UCBTH-08-001, Instructors: PETERSON, PF, STOJADINOVIC, B., UC Berkeley (May, 2008)*, 2008.

[112] T. Allen, S. Ball, E. Blandford, T. Downar, G. Flanagan, C. Forsberg, E. Greenspan, D. Holcomb, L.-W. Hu, R. Matzie, *et al.*, *Fluoride-Salt-Cooled, High-Temperature Reactor (FHR) Subsystems Definition, Functional Requirement Definition, and Licensing Basis Event (LBE) Identification White Paper*. Nuclear Energy University Programs, US Department of Energy, 2013.

[113] N. Zweibaum, J. Bickel, Z. Guo, J. Kendrick, and P. Peterson, "Design, fabrication and startup testing in the compact integral effects test facility in support of fluoride-salt-cooled, high-temperature reactor technology," in *International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-16), Chicago, IL, August 30-September 4 (2015)*, 2015.

[114] N. Zweibaum, *Experimental Validation of Passive Safety System Models: Application to Design and Optimization of Fluoride-Salt-Cooled, High-Temperature Reactors*. PhD thesis, UC Berkeley, 2015.

[115] D. de Wet, C. Poresky, and P. F. Peterson, "Designing frequency response tests for system identification in ciet," in *Proc. American Nuclear Society Winter Meeting 2018*, American Nuclear Society Orlando, Florida, 2018.

[116] P. M. Bardet and P. F. Peterson, "Options for scaled experiments for high temperature liquid salt and helium fluid mechanics and convective heat transfer," *Nuclear Technology*, vol. 163, no. 3, pp. 344–357, 2008.

[117] J. Hugo, J. Forester, D. Gertman, J. Joe, H. Medema, J. Persensky, and A. Whaley, "Draft function allocation framework and preliminary technical basis for advanced smr concepts of operations," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2013.

[118] C. Plott, T. Engh, and V. E. Barnes, *Technical basis for regulatory guidance for assessing exemption requests from the nuclear power plant licensed operator staffing requirements specified in 10 CFR 50.54 (m)*. Division of Systems Analysis and Regulatory Effectiveness, Office of Nuclear . . . , 2004.

[119] "Unified architecture," 2018.

[120] I. GmbH, "Opc ua," 2019.

[121] R. L. Boring, T. A. Ulrich, R. Lew, C. R. Kovesdi, and A. Al Rashdan, "A comparison study of operator preference and performance for analog versus digital turbine control systems in control room modernization," *Nuclear Technology*, vol. 205, no. 4, pp. 507–523, 2019.

[122] Marsh Risk Management Research, "Advanced cyber attacks on global energy facilities," tech. rep., Marsh, 2014.

[123] T. Ulrich, R. Lew, H. Medema, R. Boring, and K. Thomas, "A computerized operator support system prototype," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2015.

[124] T. A. Ulrich, R. Lew, C. M. Poresky, B. C. Rice, K. D. Thomas, and R. L. Boring, "Operator-in-the-loop study for a computerized operator support system (coss)–cross-system and system-independent evaluations," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2017.

[125] R. Lew, T. A. Ulrich, and R. L. Boring, "Nuclear reactor crew evaluation of a computerized operator support system hmi for chemical and volume control system," in *International Conference on Augmented Cognition*, pp. 501–513, Springer, 2017.

[126] H. Medema, K. Savchenko, R. Boring, and T. Ulrich, "Defining mutual awareness: Results of reactor operator surveys on the emergence of digital technology in main control rooms," in *International Conference on Applied Human Factors and Ergonomics*, pp. 58–67, Springer, 2018.

[127] C. Forsberg, "Improved heat transfer and volume scaling through novel heater design," in *Proc. of ANS Annual Meeting 2017*, 2017.

[128] A. C. Cilliers and E. J. Mulder, "Adapting plant measurement data to improve hardware fault detection performance in pressurised water reactors," *Annals of Nuclear Energy*, vol. 49, pp. 81–87, 2012.

[129] T. D. C. Company, "Dowtherm a heat transfer fluid product technical data," 1997.

[130] F. P. Incropera, A. S. Lavine, T. L. Bergman, and D. P. DeWitt, *Fundamentals of heat and mass transfer*. Wiley, 2007.

[131] R. Upadhya, "Ciet-mes-ts-003-01 fanex (fan-cooled heat exchangers) technical sheet," tech. rep., University of California, Berkeley, Thermal Hydraulics Laboratory, 2014.

[132] O. C. I. S. LLC, "Pipe and mechanical insulation pub. no. 10020231-c.," 2017.

Appendix A

Expanded Models

Structural Representation of Heater Model

- Variables: P_H, $CX101$, $CX102$, $CX103$, $CX104$, $CX111$, $CX112$, $CX113$, $CX114$, $WT10$, $BT11$, $ST14E$, $ST14W$, $ST14N$, $ST14S$, $ST12N$, $ST12SE$, $ST12SW$, $ST13$, $ST11$, $ST10$, $AT02$, $FM40$, $\dot{m}$, T_∞, $T_{in,H}$, $T_{out,H}$, $T_{S,H}$, $T_{F,H}$, $\dot{Q}_H$, $\dot{Q}_{\infty,H}$, $\frac{dT_{S,H}}{dt}$, $\frac{dT_{F,H}}{dt}$
- Faults: f_H
- Knowns: u_H, y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}, y_{12}, y_{13}, y_{14}, y_{15}, y_{16}, y_{17}, y_{18}, y_{19}, y_{20}, y_{21}, y_{22}
- Parameters: $c_{p,Dow}$, $h_{S,H}$, $A_{S,H}$, $h_{\infty,H}$, $A_{\infty,H}$, $M_{F,H}$, $c_{pF,H}$, $M_{S,H}$, $c_{pS,H}$

$$
\begin{aligned}
e_1 &: u_H = P_H + f_H & e_{12} &: y_{11} = ST14E \\
e_2 &: y_1 = CX101 & e_{13} &: y_{12} = ST14W \\
e_3 &: y_2 = CX102 & e_{14} &: y_{13} = ST14N \\
e_4 &: y_3 = CX103 & e_{15} &: y_{14} = ST14S \\
e_5 &: y_4 = CX104 & e_{16} &: y_{15} = ST12N \\
e_6 &: y_5 = CX111 & e_{17} &: y_{16} = ST12SE \\
e_7 &: y_6 = CX112 & e_{18} &: y_{17} = ST12SW \\
e_8 &: y_7 = CX113 & e_{19} &: y_{18} = ST13 \\
e_9 &: y_8 = CX114 & e_{20} &: y_{19} = ST11 \\
e_{10} &: y_9 = WT10 & e_{21} &: y_{20} = ST10 \\
e_{11} &: y_{10} = BT11 & e_{22} &: y_{21} = AT02
\end{aligned}
$$

$$e_{23} : y_{22} = FM40$$
$$e_{24} : \dot{m} = FM40$$
$$e_{25} : T_{\infty} = AT02$$

$$e_{26} : T_{in,H} = \frac{WT10 + BT11}{2}$$

$$e_{27} : T_{out,H} = \frac{CX101 + CX102 + CX103 + CX104 + CX111 + CX112 + CX113 + CX114}{8}$$

$$e_{28} : T_{S,H} = \frac{\frac{ST14E+ST14W+ST14N+ST14S}{4} + ST13 + \frac{ST12N+ST12SE+ST12SW}{3} + ST11 + ST10}{5}$$

$$e_{29} : \frac{dT_{S,H}}{dt} = \frac{d}{dt}(T_{S,H})$$
$$e_{30} : T_{F,H} = \frac{T_{in,H} + T_{out,H}}{2}$$

$$e_{31} : \frac{dT_{F,H}}{dt} = \frac{d}{dt}(T_{F,H})$$
$$e_{32} : \dot{Q}_H = \dot{m} c_{p,Dow}(T_{out,H} - T_{in,H})$$

$$e_{33} : \dot{Q}_H = (hA)_{S,H}(T_{S,H} - T_{F,H})$$

$$e_{34} : \dot{Q}_{\infty,H} = (hA)_{\infty,H}(T_{S,H} - T_{\infty,H})$$

$$e_{35} : P_H = \frac{dT_{S,H}}{dt}(Mc_p)_{S,H} + \frac{dT_{F,H}}{dt}(Mc_p)_{F,H} + \dot{Q}_H + \dot{Q}_{\infty}$$

Structural Representation of CTAH Model

- Variables: $WT40$, $BT41$, $WT42$, $BT43$, $AT01$, $AT02$, $FM40$, ω_C, $\dot{m}_{I,C}$, $\dot{m}_{F,C}$, $T_{Out,F,C}$, $T_{In,F,C}$, $T_{Out,I,C}$, $T_{In,I,C}$, P_C, $T_{F,C}$, $\frac{dT_{F,C}}{dt}$
- Faults: f_C
- Knowns: u_C, y_1, y_2, y_3, y_4, y_5, y_6, y_7
- Parameters: $f(\omega_C)$, $c_{p,F,C}$, $c_{p,I,C}$, $M_{F,C}$

$$
\begin{aligned}
e_1 &: y_1 = WT40 & e_{10} &: T_{Out,F,C} = \frac{BT41 + WT40}{2} \\
e_2 &: y_2 = BT41 & e_{11} &: T_{Out,I,C} = AT01 \\
e_3 &: y_3 = WT42 & e_{12} &: T_{In,I,C} = AT02 \\
e_4 &: y_4 = BT43 & e_{13} &: T_{F,C} = \frac{T_{Out,F,C} + T_{In,F,C}}{2} \\
e_5 &: y_5 = AT01 & e_{14} &: \frac{dT_{F,C}}{dt} = \frac{d}{dt}(T_{F,C}) \\
e_6 &: y_6 = AT02 & e_{15} &: u_C = \omega_C \\
e_7 &: y_7 = FM40 & e_{16} &: \dot{m}_{I,C} = f(\omega_C) + f_C \\
e_8 &: \dot{m}_{F,C} = FM40 & e_{17} &: P_C = \frac{dT_{F,C}}{dt}(Mc_p)_{F,C} + \dot{m}c_{p,F,C}(T_{In,F,C} - T_{Out,F,C}) \\
e_9 &: T_{In,F,C} = \frac{BT43 + WT42}{2} & e_{18} &: P_C = \dot{m}c_{p,I,C}(T_{In,I,C} - T_{Out,I,C})
\end{aligned}
$$

Structural Representation of Thermocouple Model

- Variables: $BT1$, $WT1$, $BT2$, $WT2$, AT, $\frac{dT_1}{dt}$, T_1, $\frac{dT_2}{dt}$, T_2, T_{av}, $\dot{Q}_{T,C}$, $T_{\infty,TC}$, $\dot{m}_{TC}$
- Faults: f_{T_1}, f_{T_2}
- Knowns: y_1, y_2, y_3, y_4, y_5, y_6
- Parameters: R_{TC}, $c_{p,TC}$, M_{TC}

$$e_1 : y_1 = BT1$$

$$e_2 : y_2 = WT1$$

$$e_3 : y_3 = BT2$$

$$e_4 : y_4 = WT2$$

$$e_5 : y_5 = AT$$

$$e_6 : y_6 = \dot{m}_{TC}$$

$$e_7 : T_{\infty,TC} = AT$$

$$e_8 : T_1 = \frac{WT1 + BT1}{2} + f_{T_1}$$

$$e_9 : \frac{dT_1}{dt} = \frac{d}{dt}(T_1)$$

$$e_{10} : T_2 = \frac{WT2 + BT2}{2} + f_{T_2}$$

$$e_{11} : \frac{dT_2}{dt} = \frac{d}{dt}(T_2)$$

$$e_{12} : T_{av,TC} = \frac{T_1 + T_2}{2}$$

$$e_{13} : \dot{Q}_{TC} = \dot{m}_{TC}(T_2 - T_1)$$

$$e_{14} : \dot{Q}_{TC} = \frac{T_{av} - T_{\infty,TC}}{R}$$

$$e_{15} : \frac{dT_1}{dt} = \frac{dT_2}{dt}$$

Appendix B

Model Data and References

Resources

- [129]: Dowtherm A Heat Transfer Fluid Product Technical Data, The Dow Chemical Company
- [127]: Improved Heat Transfer and Volume Scaling through Novel Heater Design, Lukas, Kendrick, and Peterson
- [130]: Fundamentals of Heat and Mass Transfer, Incropera and Dewitt
- [131]: CIET-MES-TS-003-01, FanEx (Fan-Cooled Heat Exchangers) Technical Sheet, Upadhya
- B1: Measurements by Raleigh Lukas
- [132]: Pipe and Mechanical Insulation, Owens Corning Insulation
- B2: Measurements by Dane de Wet

Heater model parameters

$c_{p,Dow}$

$$c_{p,Dow} = 1518 + 2.82T = 1785.9 \ (T = 90°C) \tag{B.1}$$

This equation for the specific heat of Dowtherm A comes from [129]. The average fluid temperature across the heater is calculated for an inlet of 80 ° C and outlet of 100 ° C with a simple average of the two. In reality, the temperature profile across the heater is non-linear and dynamic throughout power changes in operation. The temperature-dependence of Dowtherm A's thermophysical properties is one of the primary sources of error in the model.

Parameter	Value	Resource
$c_{p,Dow}$	1771.8 $[kg/m^3]$	[129]
$h_{S,H}$	469 $[W/m^2K]$	[127]
$A_{S,H}$	0.1915 $[m^2]$	B1
$h_{\infty,H}$	10.76 $[W/m^2K]$	[130]
$A_{\infty,H}$	0.2011 $[m^2]$	B1
$M_{F,H}$	3.4336 $[kg]$	B1
$c_{pF,H}$	1091.9 $[J/kgK]$	[129, 130]
$M_{S,H}$	5.9832 $[kg]$	B1
$c_{pS,H}$	500 $[J/kgK]$	[130]

Table B.1: Heater model parameter choices

$h_{S,H}$

$$h_{S,H} = 469\ W/m^2K \tag{B.2}$$

This empirical value comes from studies documented in [127].

$A_{S,H}$

$$A_{S,H} = 2\pi rL = 2\pi(1.5/2)(62.992)\left(\frac{(0.0254\ m}{1\ in}\right)^2 = 0.1915\ m^2 \tag{B.3}$$

The heat transfer surface between the shell and the fluid is the inside cylindrical surface of the shell. The shell's inner diameter is 1.5 inches and its heated length is 62.992 inches.

$h_{\infty,H}$

$$\begin{aligned} \bar{Nu}_D = \left\{0.825 + \frac{0.387Ra_D^{1/6}}{[1+(0.492/Pr)^{9/16}]^{8/27}}\right\}^2 = \\ \left\{0.825 + \frac{0.387(9.60\times10^5)^{1/6}}{[1+(0.492/0.707)^{9/16}]^{8/27}}\right\}^2 = 16.37 \end{aligned} \tag{B.4}$$

$$Ra = GrPr \tag{B.5}$$

$$\begin{aligned} Gr = \frac{g\beta(T_s - T_\infty)D^3}{\nu^2} = \\ \frac{(9.81\ m/s^2)(\frac{1}{298\ K})(140°C - 25°C)(1.575\ in\frac{0.0254\ m}{1\ in})^3}{(15.89\ \times\ 10^{-6})^2} = \\ 9.60\ \times 10^5 \end{aligned} \tag{B.6}$$

$$Pr = 0.707 \tag{B.7}$$

$$\bar{Nu}_D = \frac{\bar{h}D}{k} \rightarrow 16.37 = \frac{\bar{h}(1.575\ in\frac{0.0254\ m}{1\ in})}{26.3 \times 10^{-3}\ W/mK} \rightarrow h_{\infty,H} = 10.76\ W/m^2K \tag{B.8}$$

Here, the Churchill and Chu correlation for a vertical plate (an approximation of a long cylinder) and all air thermophysical properties come from [130]. A representative surface temperature of $T_s = 140°C$ and $T_\infty = 25°C$ come from quick inspection of test data and other values come from the heater geometry.

$A_{\infty,H}$

$$A_{\infty,H} = 2\pi rL = 2\pi(1.575/2)(62.992)\left(\frac{0.0254\ m}{1\ in}\right)^2 = 0.2011\ m^2 \tag{B.9}$$

The heat transfer surface between the shell and the ambient air is the outside cylindrical surface of the shell. The shell's outer diameter is 1.575 inches and its heated length is 62.992 inches.

$M_{F,H}$

$$\begin{aligned} m_{inner\ tube} = (m_{tube}\ +\ m_{tape})(fraction\ in\ control\ volume) = \\ (2.047\ kg\ +\ 0.430\ kg)(0.741) = \\ 1.84\ kg \end{aligned} \tag{B.10}$$

$$\begin{aligned} m_{fluid} = V_{fluid}\rho_{fluid} = (V_{shell} - V_{tube})(\rho_{fluid}) = \\ \big(\pi r_i^2 L - (V_{tube} + V_{tape})(fraction\ in\ control\ volume)\big)(\rho_{fluid}) = \\ \left(\pi\frac{1.5\ in}{2}^2(62.992\ in)\left(\frac{0.0254\ m}{1\ in}\right)^3 - \right. \\ \left.(255.8\ cm^3 + 56.1\ cm^3)\left(\frac{1\ m}{100\ cm}\right)^3(0.741)\right)(999.1\ kg/m^3) = 1.59\ kg \end{aligned} \tag{B.11}$$

$$M_{F,H} = m_{inner\ tube} + m_{fluid} = 1.84\ kg\ +\ 1.60\ kg = 3.43\ kg \tag{B.12}$$

$c_{pF,H}$

$$\begin{aligned} c_{pF,H} = \frac{c_{pS}m_{inner\ tube}\ +\ c_{pDow}m_{fluid}}{M_{F,H}} = \\ \frac{(500\ J/kgK)(1.84\ kg)\ +\ (1771.8\ J/kgK)(1.60\ kg)}{3.43\ kg} = \\ 1091.9\ J/kgK \end{aligned} \tag{B.13}$$

The average heater fluid mass for the simplified model that neglects the inner tube as an independent heat transfer actor is the combined mass of the inner tube and fluid.

$M_{S,H}$

$$M_{S,H} = 5.9832\ kg \tag{B.14}$$

$c_{pS,H}$

$$c_{pS,H} = 500\ J/kgK \tag{B.15}$$

CTAH model parameters

Parameter	Value	Resource
$f(\omega_C)$	0.0071 $[kg/rev]$	[131]
$c_{p,F,C}$	1771.8 $[J/kgK]$	[129]
$c_{p,I,C}$	1008 $[J/kgK]$	[130]
$M_{F,C}$	3.6817 $[kg]$	[131]

Table B.2: CTAH model parameter choices

$f(\omega_C)$

$$f(\omega_C) = (ft^3/min)/RPM)(RPM/Hz)(m^3/ft^3)(\rho_{air})(\frac{min}{sec}) = 0.464\ (ft^3/min)/RPM)(28.75\ RPM/Hz)\left(\frac{0.0283168\ m^3}{ft^3}\right)(1.123\ kg/m^3)\left(\frac{1\ min}{60\ sec}\right) = 0.0071\ kg/Hz \tag{B.16}$$

The operator enters a desired frequency as the CTAH control signal but this frequency does not describe the frequency of motor rotation; it describes the frequency of the electrical signal sent through a variable frequency drive. The above conversion uses data from [131].

$c_{p,F,C}$

$$c_{p,F,C} = 1518 + 2.82T = 1771.8\ (T = 90°C) \tag{B.17}$$

The average fluid temperature of the CTAH is similar to that of the heater because operators typically control for the outlet conditions that correspond to heater inlet and CTAH inlet is very close to the temperature of heater outlet. This value is, as in the heater, a source of uncertainty because the specific heat of Dowtherm A varies significantly with temperature.

$c_{p,I,C}$

$$c_{p,I,C} = 1008\ J/kgK\ (T = 40°C) \tag{B.18}$$

$M_{F,C}$

$$M_{F,C} = V_{CTAH}\rho_{fluid} = (3.67\ L)\left(\frac{0.001\ m^3}{1\ L}\right)(1003.2\ kg/m^3) = 3.68\ kg \tag{B.19}$$

This value comes from the vendor-specified CTAH tube volume in [131].

Thermocouple model parameters

Parameter	Value	Resource
R_{TC}	2.8292 $[K/W]$	[127, 130, 132], B1
$c_{p,TC}$	1814.1 $[J/kgK]$	[129]
M_{TC}	1.2214 $[kg]$	[129], B2

Table B.3: Hot leg thermocouple model parameter choices

Hot leg

R_{TC}

$$R_{TC} = \frac{1}{2\pi r_i h_F l} + \frac{ln(r_o/r_i)}{2\pi k_S l} + \frac{ln(r_I/r_o)}{2\pi k_I l} + \frac{1}{2\pi r_I h_\infty l} = \frac{1}{2\pi(0.014\ m)(16.54\ W/m^2K)(2.02\ m)} + \frac{ln(0.017\ m/0.014\ m)}{2\pi(16.2\ W/mK)(2.02\ m)} + \frac{ln(0.055\ m/0.017\ m)}{2\pi(0.04\ W/mK)(2.02\ m)} + \frac{1}{2\pi(0.055\ m)(9.18\ W/mK)(2.02\ m^2)} = 2.83\ K/W \tag{B.20}$$

$$Nu_D = 3.66 = \frac{hD}{k}$$
$$\rightarrow h_F = \frac{3.66(0.1259\ W/mK)}{(0.0139\ m)(2)} = 16.54\ W/m^2K \tag{B.21}$$

This correlation for laminar, fully developed flow with constant surface temperature comes from [130].

$$r_i = 0.014\ m \tag{B.22}$$

$$l = 2.02\ m \tag{B.23}$$

$$k_S = 16.2\ W/mK \tag{B.24}$$

$$r_o = 0.017\ m \tag{B.25}$$

$$k_I = 0.04\ W/mK \tag{B.26}$$

$$r_I = 0.055\ m \tag{B.27}$$

$$\begin{aligned} \bar{Nu}_D = \left\{0.825 + \frac{0.387 Ra_D^{1/6}}{[1+(0.492/Pr)^{9/16}]^{8/27}}\right\}^2 = \\ \left\{0.825 + \frac{0.387(1.73\times10^6)^{1/6}}{[1+(0.492/0.707)^{9/16}]^{8/27}}\right\}^2 = 19.16 \end{aligned} \tag{B.28}$$

$$Ra = GrPr \tag{B.29}$$

$$\begin{aligned} Gr = \frac{g\beta(T_s - T_\infty)D^3}{\nu^2} = \\ \frac{(9.81\ m/s^2)(\frac{1}{298\ K})(105°C - 25°C)(0.0549\ m)^3}{(15.89\ \times\ 10^{-6})^2} = \\ 1.73\ \times 10^6 \end{aligned} \tag{B.30}$$

$$Pr = 0.707 \tag{B.31}$$

$$\bar{Nu}_D = \frac{\bar{h}D}{k} \rightarrow 19.16 = \frac{\bar{h}(0.0549\ m)}{26.3\times10^{-3}\ W/mK} \rightarrow h_\infty = 9.18\ W/m^2K \tag{B.32}$$

$c_{p,TC}$

$$c_{p,F,C} = 1518 + 2.82T = 1814.1\ (T = 105°C) \tag{B.33}$$

M_{TC}

$$M_{TC} = \pi r^2 L\rho = \pi(0.014\ m)^2(2.02\ m)(990.7\ kg/m^3) = 1.22\ kg \tag{B.34}$$

DRACS

Parameter	**Value**	**Resource**
R_{TC}	1.5773 $[K/W]$	[127, 130, 132], B1
$c_{p,TC}$	1602.6 $[J/kgK]$	[129]
M_{TC}	2.4373 $[kg]$	[129], B2

Table B.4: DRACS thermocouple model parameter choices

R_{TC}

$$R_{TC} = \frac{1}{2\pi r_i h_F l} + \frac{ln(r_o/r_i)}{2\pi k_S l} + \frac{ln(r_I/r_o)}{2\pi k_I l} + \frac{1}{2\pi r_I h_\infty l} = \frac{1}{2\pi(0.014\ m)(18.01\ W/m^2K)(3.80\ m)} + \frac{ln(0.017\ m/0.014\ m)}{2\pi(16.2\ W/mK)(3.80\ m)} + \frac{ln(0.055/0.017\ m)}{2\pi(0.04\ W/mK)(3.80\ m)} + \frac{1}{2\pi(0.055\ m)(4.49\ W/mK)(3.80\ m)} = 1.58\ K/W \tag{B.35}$$

$$Nu_D = 3.66 = \frac{hD}{k} \rightarrow h = \frac{3.66(0.1371\ W/mK)}{(0.0139\ m)(2)} = 18.01\ W/m^2K \tag{B.36}$$

$$r_i = 0.014\ m \tag{B.37}$$

$$l = 3.80\ m \tag{B.38}$$

$$k_S = 16.2\ W/mK \tag{B.39}$$

$$r_o = 0.017\ m \tag{B.40}$$

$$k_I = 0.04\ W/mK \tag{B.41}$$

$$r_I = 0.055\ m \tag{B.42}$$

$$\bar{Nu}_D = \left\{0.825 + \frac{0.387Ra_D^{1/6}}{[1+(0.492/Pr)^{9/16}]^{8/27}}\right\}^2 = \left\{0.825 + \frac{0.387(1.08\times10^5)^{1/6}}{[1+(0.492/0.707)^{9/16}]^{8/27}}\right\}^2 = 9.38 \tag{B.43}$$

$$Ra = GrPr \tag{B.44}$$

$$Gr = \frac{g\beta(T_s - T_\infty)D^3}{\nu^2} = \frac{(9.81\ m/s^2)(\frac{1}{298\ K})(30°C - 25°C)(0.0549\ m)^3}{(15.89\ \times\ 10^{-6})^2} = 1.08\ \times 10^5 \tag{B.45}$$

$$Pr = 0.707 \tag{B.46}$$

$$N\bar{u}_D = \frac{\bar{h}D}{k} \rightarrow 9.38 = \frac{\bar{h}(0.0549\ m)}{26.3 \times 10^{-3}\ W/mK} \rightarrow h_\infty = 4.49\ W/m^2K \tag{B.47}$$

$c_{p,TC}$

$$c_{p,F,C} = 1518 + 2.82T = 1602.6\ (T = 30°C) \tag{B.48}$$

M_{TC}

$$M_{TC} = \pi r^2 L\rho = \pi(0.0139\ m)^2(3.80\ m)(1051.7\ kg/m^3) = 2.44\ kg \tag{B.49}$$