INL/RPT-23-73099

Light Water Reactor Sustainability Program

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis

June 2023

U.S. Department of Energy

Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/RPT-23-73099

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis

Jeffrey Joe, Larry Hettinger, Marvin Dainoff, Patrick Murray, and Yusuke Yamani

June 2023

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy

This page intentionally left blank

ABSTRACT

This report describes the interim progress for research supporting the design and optimization of information automation systems for nuclear power plants. Much of the domestic nuclear fleet is currently focused on modernizing technologies and processes, including transitioning toward digitalization in the control room and elsewhere throughout the plant, along with a greater use of automation, artificial intelligence, robotics, and other emerging technologies. While there are significant opportunities to apply these technologies toward greater plant safety, efficiency, and overall cost-effectiveness, optimizing their design and avoiding potential safety and performance risks depends on ensuring that human-performance-related organizational and technical design issues are identified and addressed. This report describes modeling tools and techniques, based on sociotechnical system theory, to support these design goals and their application in the current research effort. The report is intended for senior nuclear energy stakeholders, including regulators, corporate management, and senior plant management.

We have developed and employed a method to design an optimized information automation ecosystem (IAE) based on the systems-theoretic constructs underlying sociotechnical systems theory in general and the Systems-Theoretic Accident Modeling and Processes (STAMP) approach in particular. We argue that an IAE can be modeled as an interactive *information control system* whose behavior can be understood in terms of dynamic control and feedback relationships amongst the system’s technical and organizational components. Up to this point, we have employed a Causal Analysis based on STAMP (CAST) technique to examine a performance- and safety-related incident at an industry partner’s plant that involved the unintentional activation of an emergency diesel generator. This analysis provided insight into the behavior of the plant’s current information control structure within the context of a specific, significant event.

Our ongoing analysis is focused on identifying near-term process improvements and longer-term design requirements for an optimized IAE system. The latter analyses will employ a second STAMP-derived technique, System-Theoretic Process Analysis (STPA). STPA is a useful modeling tool for generating and analyzing actual or potential information control structures. Finally, we have begun modeling plantwide organizational relationships and processes. Organizational system modeling will supplement our CAST and STPA findings and provide a basis for mapping out a plantwide information control architecture.

CAST analysis findings indicate an important underlying contributor to the incident under investigation, and a significant risk to information automation system performance, was perceived schedule pressure, which exposed weaknesses in interdepartmental coordination between and within responsible plant organizations and challenged the resilience of established plant processes, until a human caused the initiating event. These findings are discussed in terms of their risk to overall system performance and their implications for information automation system resilience and brittleness.

We present two preliminary information automation models. The proactive issue resolution model is a test case of an information automation concept with significant near-term potential for application and subsequent reduction in

significant plant events. The IAE model is a more general representation of a broader, plantwide information automation system. From our results, we have generated a set of preliminary system-level requirements and safety constraints. These requirements will be further developed over the remainder of our project in collaboration with nuclear industry subject matter experts and specialists in the technical systems under consideration.

Additionally, we will continue to pursue the system analyses initiated in the first part of our effort, with a particular emphasis on STPA as the main tool to identify weak or weakening control structures that affect the resilience of organizations and programs. Our intent is to broaden the scope of the analysis from an individual use case to a related set of use cases (e.g., maintenance tasks, compliance tasks) with similar human-system performance challenges. This will enable more generalized findings to refine the Proactive Issue Resolution and IAE models, as well as their system-level requirements and safety constraints. We will use organizational system modeling analyses to supplement STPA findings and model development.

We conclude the report with a set of summary recommendations and an initial draft list of system-level requirements and safety constraints for optimized information automation systems.

This page intentionally left blank

CONTENTS

FIGURES

TABLES

ACRONYMS

AI	artificial intelligence
CAP	corrective action program
CAST	Causal Analysis Based on STAMP
CWA	cognitive work analysis
EDG	emergency diesel generator
EID	ecological interface design
HSI	human-systems integration
IAE	information automation ecosystem
ICS	information control structure
INL	Idaho National Laboratory
INPO	Institute of Nuclear Power Operations
LWR	light-water reactor
LWRS	Light Water Reactor Sustainability
ML	machine learning
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operations and maintenance
PIR	proactive issue resolution
R&D	research and development
SCS	safety control structure
SME	subject matter expert
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
U.S.	United States

This page intentionally left blank

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis

1. INTRODUCTION

This report describes the interim progress for a program of research supporting the design and optimization of information automation systems in nuclear power plants (NPPs). Much of the domestic fleet is currently focused on modernizing technologies and processes, including the digital transformation of the control room and elsewhere, as well as a greater use of automation, artificial intelligence, robotics, and other emerging technologies. There are significant opportunities to leverage these technologies for greater plant safety, efficiency, and overall cost-effectiveness. Optimizing their design (and avoiding potential risks) depends, in large part, on ensuring that potential sociotechnical system design weaknesses are identified and addressed as early as possible. This report describes modeling tools and techniques that support these design goals and their application in the current research.

We have developed and employed a method to support designing an optimized information automation ecosystem (IAE) based on the systems-theoretic constructs underlying sociotechnical systems theory in general and the Systems-Theoretic Accident Modeling and Processes (STAMP) approach in particular. We suggest that an IAE can be modeled as an interactive *information control system* whose behavior can be understood in terms of dynamic control and feedback relationships between a system's technical and organizational components. To date, we have employed the Causal Analysis based on STAMP (CAST) technique to examine an incident at an industry partner's plant that resulted in the unintended activation of an emergency diesel generator (EDG). This analysis provided insight into the behavior of the plant's current information control structure (ICS) within the context of a significant event. Our ongoing analysis is focused on identifying near-term process improvements and long-term design requirements for optimized information automation. The latter analyses will employ a second STAMP-derived technique, System-Theoretic Process Analysis (STPA). STPA is a useful modeling tool for analyzing actual or potential ICSs to proactively avoid unsafe events.

The programmatic goals of this research project are:

- Develop an accurate cost-effective issue resolution process that utilizes information automation and artificial intelligence (AI) to evaluate numerous sources of relevant internal and external plant data to identify adverse performance trends and weak signals that expose weakening or nonexistent control structures
- Employ a proactive analysis method such as STPA to analyze the performance data for precursors to significant events
- Develop a sociotechnical system model of an optimized IAE based on systems- and control-theoretic principles of feedback and control
- Apply sociotechnical systems analysis methods to identify the inadequate control structures that contribute to the weak organizational and programmatic causes responsible for adverse trends which, if uncorrected, lead to more significant events
- Develop means to recommend corrective actions to strengthen control structures before they can cause a significant event
- Evaluate the effectiveness of actions taken as a result of the system analysis by assessing its impact on the resultant control structure
- Ensure only accurate and validated information is disseminated to the rest of the nuclear industry.

The major principles and assumptions underlying the research project are:

1. A well-executed continuous improvement process drives nuclear plants to higher performance levels
2. The detection and prevention of events and issues is significantly less costly than their correction
3. A risk-informed focus on plant safety and reliability is the most effective way to drive improvements in plant safety and performance
4. Weak or nonexistent sociotechnical safety control structures (SCSs) are generally caused by organizational and programmatic weaknesses, which manifest themselves through events and issues at all significance levels within a nuclear utility
5. Significant events are caused by weak, weakening, or nonexistent SCSs embedded within a nuclear plant or utility
6. Low-level and near-miss events are caused by the same weak, weakening, or nonexistent SCSs as significant events but remained relatively nonconsequential due to the a constraint or barrier that mitigated a more significant event
7. Most significant events could have been prevented or mitigated if weak (or obvious) signals or adverse trends within relevant internal and external plant information (including operational experience) had been deciphered, evaluated, and corrected in a timely manner
8. There are many databases at an NPP for reporting issues that can be evaluated and trended to identify weak, weakening, or nonexistent SCSs
9. Information automation using AI (i.e., Machine Intelligence for Review and Analysis of Condition Logs and Entries [MIRACLE]) can accurately and simultaneously mine numerous sources of internal and external information looking for weak signals or adverse trends, which are predictive of potential incidents caused by indicative weak, weakening, or nonexistent control structures
10. Effectively mining all available data sources improves the statistical accuracy of problem identification and resolution
11. Sharing accurate information among utilities and plants is one of the most important elements in preventing issues.

The successful execution of this program will result in an overall reduction in unplanned significant events and, therefore, will have a profound impact on plant safety and the reduction of operating and maintenance (O&M) costs from those events.

This research is being conducted as part of the Department of Energy’s Light Water Reactor Sustainability (LWRS) Program and its efforts, in partnership with industry, to support NPP modernization through effective human-systems integration (HSI). It builds on prior work focused on the design and integration of new technologies into existing NPP processes (Kovesdi et al., 2021) as well as a prior STAMP-based analysis of a scram incident related to a new digital instrumentation and control system (Dainoff et al., 2022).

1.1 Socioeconomic Challenges Facing the Nuclear Industry

Much of the U.S.’ nuclear power industry is either considering or is actively engaged in a fundamental shift toward modernizing technologies and procedures. The transition from analog to digital technology, or digitalization, (e.g., Hunton et al., 2020) and from other increasingly obsolete to emerging technologies (e.g., Kovesdi et al., 2021) is at the center of many of these efforts. Technologies such as automation, AI, machine learning (ML), robotics, and virtual systems are all under consideration to increase NPP safety, efficiency, and operational cost-effectiveness.

There are numerous factors impacting the industry's drive toward modernization. Some are socioeconomic while others represent a response to the possibilities afforded by emerging technologies. In many cases, modernization is being driven by a desire to extend the operational lifespan of the existing NPP fleet (Thomas and Hunton, 2019). This lifespan extension requires an effective integration of technologies, personnel, work procedures, and corresponding governance to achieve a fully modernized and effective *system.* Achieving the long-term modernization and economic viability of the industry also requires achieving greater cost-effectiveness in overall operations to effectively compete with other forms of energy generation.

Nuclear energy, like much of the industry in general, is also coping with emerging demographic issues that could impact future operations, particularly with regard to staffing as there is an aging workforce, due in part to a shrinking labor pool driven by retirement (and associated loss of expertise) and fewer qualified individuals in the replacement pool. This issue has been recognized as a potential problem for the industry for quite some time (e.g., Wahlstrom, 2004) and remains an area of concern. The relevance of this issue for the design and implementation of future NPP systems lies in the possibility that these systems will likely need to be operated by fewer workers called upon to accomplish more (e.g., Alcover et al., 2021).

There are several constraints operating on the industry that complicate addressing the issues described above. For instance, for much of the industry, there will be a need to modernize technologies and associated processes, staffing, and governance on the fly. That is, modifications may need to be implemented while the plant cycles through normal online and offline conditions. While this is more of a logistical challenge and less a socioeconomic one, it nevertheless challenges system design and, especially, implementation.

Additionally, significant changes of the sort under consideration within the industry can only be pursued within the context of a heavily regulated environment. The U.S. Nuclear Regulatory Commission (NRC) closely monitors NPP modernization plans and processes, working with the nuclear industry to ensure the safety of significant modifications. For example, NUREG-0711 provides the NRC with the means to monitor and "review the human factors engineering (HFE) programs of applicants for construction permits, operating licenses, standard design certifications, combined operating licenses, and license amendments" (NRC, 2012).

The LWRS Program has been performing research and development (R&D) within the economic and regulatory constraints described above to modernize the existing fleet of commercial light-water reactors (LWRs) because these NPPs play a foundational role for the United States in terms of both energy security and economic prosperity. To successfully modernize existing NPPs, the LWRS Plant Modernization Pathway has conducted R&D, used that R&D to provide guidance on the full-scale implementation of digital modernization, and communicated the results to other nuclear power stakeholders to significantly reduce the technical and financial risks of digitalization. The LWRS Plant Modernization Pathway follows this process of researching, developing, demonstrating, and deploying R&D solutions in order to achieve its R&D objectives of developing modernization solutions that improve reliability and economic performance, while addressing the U.S. nuclear industry's aging and obsolescence challenges, and its goals of extending the life and improving the performance of the existing fleet of NPPs through modernized technologies and improved processes for plant operation and power generation.

Additionally, the Department of Energy determined that the LWRS Program needed to provide a vision and strategy to fundamentally transformation NPPs. Developing a transformation strategy that revolutionizes the operating paradigm of NPPs, as opposed to incremental upgrades, is vitally important because this is the approach needed to make commercial NPPs competitive with other electrical generating sources. As such, the LWRS Plant Modernization Pathway has developed a strategy to achieve the safe and economical long-term operation of the nation's commercial NPPs that entails a fundamental transformation of the concepts of operation, maintenance, support, and governance for commercial NPPs. Our research summarized in this report supports this LWRS Program goal by addressing the sociotechnical gaps often overlooked when highly complex engineered systems undergo significant upgrades. It is often the case that the unintended consequences of large-scale transformations on people, work processes, and the organization are minimized or not even considered.

Effectively integrating humans with the technical and organizational systems that define the workplace is essential to fully leverage the capabilities of any new technology or process introduced into a new or existing sociotechnical system. The technologies we mentioned above have promising applications for NPP performance and safety, but their potential can only be realized if they also adequately complement human performance by, for instance, leveraging the advantages of users' perceptual, cognitive, and physical capabilities while compensating for corresponding limitations.

The current research effort is focused on the *joint optimization* of NPP technical, human, and organizational assets and processes. The likelihood of a new or redesigned sociotechnical system achieving its operational objectives is greatly reduced if insufficient attention is paid to human-system performance and social and organizational issues at the expense of technical innovation. The latter condition has been referred to as the asynchronous evolution of technical and personnel resources and can result, for instance, in expensive technical "fixes" that do not coordinate well with the skillsets and work practices of the intended users.

Joint optimization also applies to designing overall systems and their subsystems such that the safety, efficiency, and effectiveness of system operation are optimally counterbalanced (see Figure 1). For example, it is possible to design a system with an outsized emphasis on efficiency at the expense of operational effectiveness and safety by, for instance, emphasizing worker speed over accuracy, corner-cutting to save time and resources, etc. Similarly, designs might significantly emphasize safety over efficiency and effectiveness, perhaps resulting in operational procedures, work processes, etc. that are slower and more costly than necessary, negatively impacting overall system performance.

We suggest that the joint optimization of these three key elements of successful system performance can be achieved through a similar joint optimization of people, technology, related processes, and governance. Sociotechnical systems theory and its associated methods are an effective means of supporting the modeling, design, and implementation of such systems through knowledge representation (i.e., the identification and representation of key information supporting the user's system knowledge), knowledge elicitation (i.e., extracting system knowledge, expertise, and experience from users and stakeholders to ensure the design is relevant to their needs) and, most importantly, cross-functional integration. Cross-functional integration refers to the process of multidisciplinary design in which stakeholders participate in a system design that includes hardware, software, human factors engineering, training and personnel selection, and management and others participate jointly in all aspects of the design process.

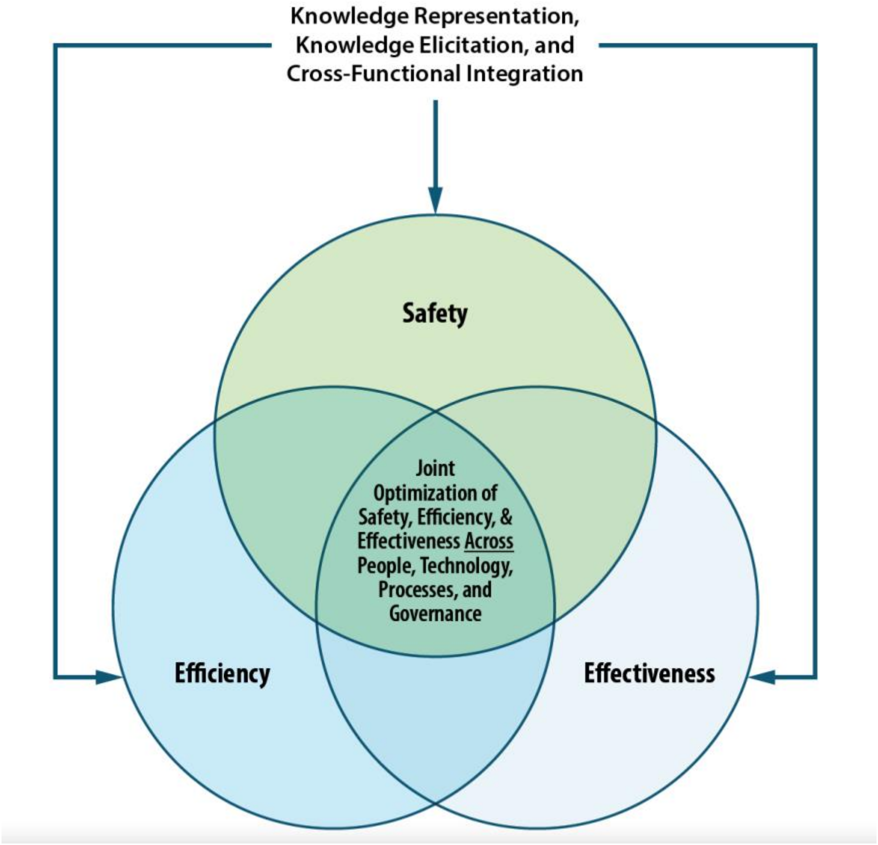
Knowledge Representation, Knowledge Elicitation, and Cross-Functional Integration
Safety
Joint Optimization of Safety, Efficiency, & Effectiveness Across People, Technology, Processes, and Governance
Efficiency
Effectiveness

Figure 1. Joint optimization of safety, efficiency, and effectiveness.

It is important to note that, while successfully addressing economic challenges to industry viability is critical to support the future of nuclear energy, safety is and must always remain the industry's highest priority. Any long-term cost savings associated with transitioning the current system to one with a greater dependence on advanced technologies can only be accomplished if it can be shown to be done so safely. A key advantage of the STAMP approach, described in Section 3.2.1, is that it provides a means of assessing specific sociotechnical risks in a design early enough in the process to allow for correction to avoid any further development of a faulty design. For this reason, we have chosen it as an analytic approach to support the design of an optimized information automation system.

1.2 Performance and Safety Challenges Associated with System Monitoring

The NPPs currently in operation within the United States as well as most of the other nuclear plants in the world operate under high-stakes conditions. The naïve notion of nuclear power being "too cheap to meter" is long gone. When operating well, NPPs can produce a lot of power due to their high-power output, and a utility can profit greatly when a plant performs well. However, NPPs are always one severe event at any plant in the world away from either having to implement expensive compensatory actions to prevent a similar event or being shut down. For example, as of April 2023, Germany permanently shut down its nuclear plants, even though they were some of the best performing plants in the world. The catalyst for this was a quicker transition to renewable energy than originally planned, in part as a result of the catastrophe at the Japanese Fukushima Daichi nuclear plants, due to poor reactor safety system management, which was exposed by an unexpected tsunami. The catastrophe could have been prevented if the utility was aware of programmatic similarities between the Japanese plants and the potential vulnerability their plants had to flooding and those of the Blayais French nuclear plant flooding event, which occurred in December 1999 when a storm surge at high tide exceeded the design-basis flood scenario causing a loss of power and jeopardizing reactor safety systems from being able to perform their design-basis functions.

In order for an NPP or nuclear utility to stay in operation, it must try to maintain the optimal balance between nuclear safety and production. As seen in Figure 2, the further a plant operates from this optimal line of performance, the more costly it is to return the plant to this optimal performance.

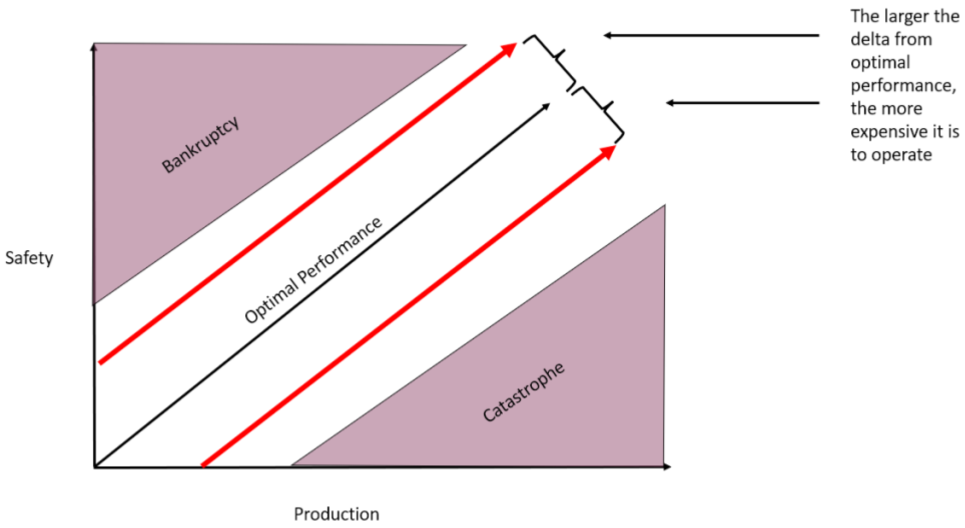
The larger the delta from optimal performance, the more expensive it is to operate
Bankruptcy
Safety
Optimal Performance
Catastrophe
Production

Figure 2. Optimal plant performance.

If a plant deviates too far from optimal performance, it is permanently shut down, and depending on why it is shut down, other plants may also be affected, further reducing the economic viability of the other NPPs. One solution to achieve optimal performance is to develop a more effective proactive issue resolution process than is currently in use that capitalizes on recent developments in the use of information automation and AI.

1.3 Information Automation to Support System Performance

U.S. nuclear regulations as well as those in most other countries require the reporting and correction of conditions adverse to quality. Regulators perform periodic audits of NPP’s problem identification and resolution programs to ensure compliance with regulations. When a plant’s ability to identify and correct its own issues is recognized by the regulator as inadequate, the regulator increases their presence and intensity of enforcement until the plant meets (or exceeds) the required level of performance. As Figure 2 shows, returning to a satisfactory level of performance is very costly to the plant and utility. Although regulatory compliance is a minimum expected outcome of a performance improvement program, achieving optimal performance is driven by plant or utility profitability. As previously noted, when a plant deviates too far from the optimal performance line in either direction, it becomes costly to return to it.

NPPs utilize performance improvement processes to help drive continuous improvement. These processes are commonly made up of several subprograms, each designed to collect and evaluate data from different sources of information. Figure 3 illustrates the characteristics of a typical performance improvement program and the different processes that comprise it.

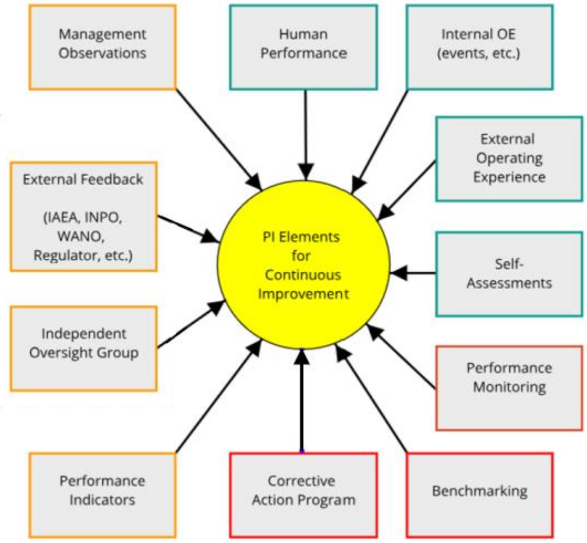
Management Observations
Human Performance
Internal OE (events, etc.)
External Operating Experience
External Feedback
(IAEA, INPO, WANO, Regulator, etc.)
PI Elements for Continuous Improvement
Self-Assessments
Independent Oversight Group
Performance Monitoring
Performance Indicators
Corrective Action Program
Benchmarking

Figure 3. Characteristics of a typical performance improvement program.

By design, the current performance improvement process in use at most NPPs attempts to employ many leading and real-time performance evaluation processes to concentrate on issue prevention and detection. In most cases the data from these programs are distilled and eventually captured in the corrective action program (CAP). As the focus on most investigation methods has been on self-revealing events, the tools for trending and evaluating the low-level trends are limited to common cause analysis, and this process is limited in its ability to identify and correct organizational and programmatic weaknesses because it is biased towards lagging sources of data. However, it is widely known within the industry that the root causes of low-level events and trends are the same as the root causes of significant events, without a contributing cause to exacerbate the problem. As previously noted, apparent root causes of issues at all significance levels are at least partially attributable to organizational and programmatic weaknesses, and these weaknesses are due to weak, weakening, or nonexistent SCSs. The more proficient an organization is at identifying these weak control structures, the more cost effective and higher performing a plant is going to be.

Identifying weak SCSs after a significant event is relatively easy, and most utilities have become adept at investigating significant events and identifying the organizational and programmatic weaknesses that contributed to them. However, being able to proactively prevent significant events is much more difficult. Until recently, all plant issues and events were captured in the CAP, and CAP data were trended and analyzed to detect and correct weak SCSs. However, with CAP as the only source of data, it takes more time for trends to develop, be detected, be analyzed, and have the causes corrected. Statistically, with more data sources, adverse trends will become apparent more quickly and the time to correct the programmatic causes is decreased.

Evaluating all of the available plant data sources to detect weak or weakening control structures and subsequently prevent significant issues has proven to be difficult, time consuming, and costly, with most utilities having limited success performing this evaluation effectively. We suggest that the solution is to develop a cost-effective issue resolution process that utilizes information automation and AI to identify trends and a proactive analysis method, such as STPA, to continually analyze the data in search of sociotechnical precursors to significant events.

Figure 4 illustrates an initial proactive issue resolution (PIR) model and process structured around information automation, AI, and STPA. In support of the current research program’s objectives, we have pursued developing a PIR model, whose application is meant to address near-term needs in the nuclear industry (i.e., proactively identifying potential issues and signs of weak or weakening SCSs), while also serving as a prototype use case for developing a more general IAE. We intend IAE to model a plant's entire information automation system, within which the PIR and other related utilities will reside.

A major reason information automation is a relatively new development for industry in general, including the nuclear energy industry, is simply that previous technology did not afford the means for its widespread, effective adoption. In light of the significant increase in the development and use of critical IAE-enabling technologies, particularly automation, AI, ML, and large language models, the technical risks associated with their application in the nuclear energy domain are not the barriers they once were.

A well-designed IAE (i.e., the system comprising users, information technology, and associated processes and governance) will benefit plant performance in a number of ways. AI can be used to search for, detect, and process weak (or strong) signals indicating potential weaknesses in the plant's technical systems, schedules, and processes. Distilling and presenting that information in an intuitive and actionable manner to individuals on a need-to-know basis will enable a more rapid and well-informed response to issues of concern than is possible with current analytic techniques. Tracking actions associated with issues and assessing their effectiveness is desirable to ensure an issue has been addressed, but also to promote lessons learned for in-plant purposes and, ideally, sharing with other nuclear utilities.

There are many R&D issues to address in developing an optimized information automation system, and many extend beyond the realm of HSI, the focus of the current work. Our major research concerns are to identify those parts of the system that "touch the human" in some way, to identify current and potential risks associated with those interactions, and to model a system in which those interactions are optimized. This necessarily involves questions of human-automation interaction, human-AI interaction including such issues as trust (e.g., Hoff and Bashir, 2015) and system transparency (e.g., Larsson and Heintz, 2020), and information presentation and interface design. Simply put, our focus is on identifying the means to provide the right information to the right people at the right time and in the right way.

We propose that information automation can be modeled as an ICS. Similar in many respects to a SCSs, an ICS is a model of the system based on control- and systems-theoretic concepts of control and feedback. It includes all the system's sociotechnical components (people and technology) and maps the control and feedback relationships between them as they relate to information transmission, reception, and processing. The utility of such a model is that it provides a functional map of the system that can be used to assess and identify actual and potential weaknesses in the system design and to identify opportunities for the introduction of automation and AI/ML technologies.

Our approach to the current research is based on systems theory in general (Checkland, 1981; von Bertalanfy, 1968) and sociotechnical system theory in particular (e.g., Whitworth, 2009; Wilson, 2014). The many variations of systems theory currently in use in science, engineering, medicine, and other domains, including sociotechnical system analysis and design, share the following core concepts:

- Systems are made up of components, typically arranged in a hierarchical fashion and characterized by complex control and feedback relationships amongst themselves
- System behavior is considered an *emergent property* of the activity within that system in its current state; however, emergent properties are not simply a linear function of the combined behavior of individual system components but are also heavily influenced by the various interactions between components.

Sociotechnical system theory shares all the above characteristics of general systems theory but is specialized for the analysis and design of complex human-machine systems, particularly those involving multiple humans, technical systems, and associated processes.

1.4 A Preliminary Information Automation Model of Proactive Issue Resolution

Figure 4 illustrates a PIR process that uses information automation, AI, and STPA to provide information regarding emerging, adverse trends within the plant.

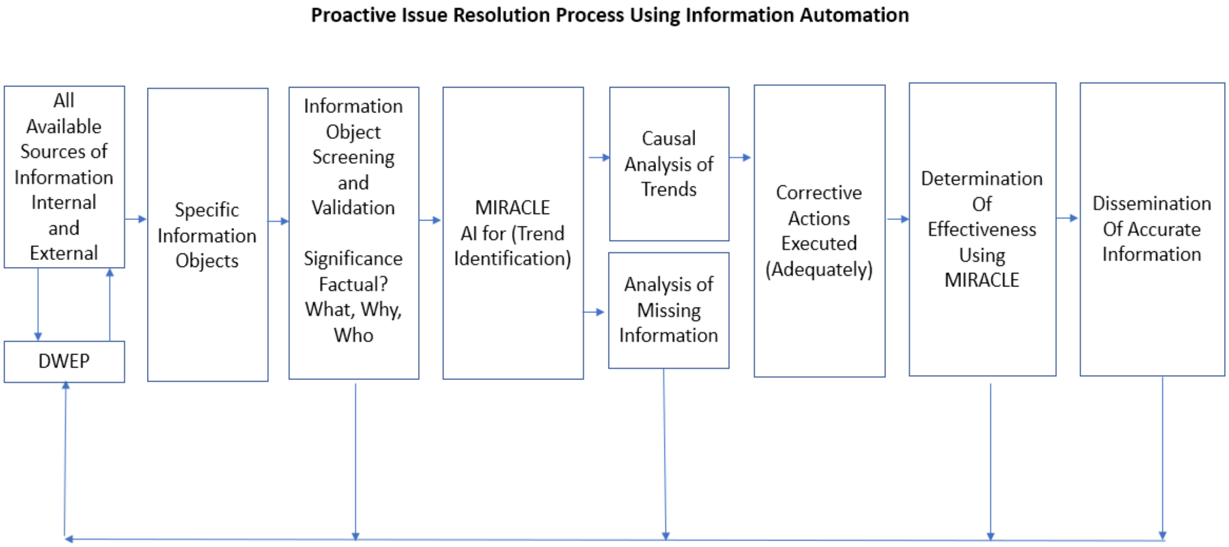
Proactive Issue Resolution Process Using Information Automation
All Available Sources of Information Internal and External
DWEP
Specific Information Objects
Information Object Screening and Validation
Significance Factual? What, Why, Who
MIRACLE AI for (Trend Identification)
Causal Analysis of Trends
Analysis of Missing Information
Corrective Actions Executed (Adequately)
Determination Of Effectiveness Using MIRACLE
Dissemination Of Accurate Information

Figure 4. PIR process using information automation.

The PIR process, as shown above, utilizes information automation and AI to gather, screen, and evaluate data for indications of weak, weakening, or nonexistent SCSs. STPA is used to perform an in-depth evaluation of the control structures and to support recommended corrective actions to strengthen the control structures. Finally, AI is used to evaluate plant data once again to determine the effectiveness of actions taken.

A more detailed overview of the process includes:

- All available data sources are considered process inputs, including all internal plant databases (human and equipment related), inputs into a dynamic work execution platform (DWEP; see Section 1.4.2), equipment and process sensors, and external sources.
- Information automation is used to gather and convert these data sources into specific information objects, which are distinct usable records once they are subsequently screened and validated.
- Screening information objects includes determining the significance of the information to the plant as well as other information that will facilitate the data trend in many different dimensions. Note, if the significance or other attributes of the information objects cannot be determined, they are fed back through the DWEP for clarification and update.
- Once the information objects have been successfully screened, an AI application, such as Idaho National Laboratory's (INL's) MIRACLE (see Section 1.4.1), which was specifically designed to evaluate NPP information, evaluates and places the information objects into logical groupings, such as potential trends and event precursors.
- STPA is then used to evaluate the groupings to identify weak and weakening control structures and to recommend actions that can improve the organizational and programmatic weaknesses resulting from these structures.

- When there is inadequate or limited data to evaluate or improve the statistical accuracy of the trend, the process can direct the DWEP to acquire the data it needs.
- The STPA recommends corrective actions to strengthen the technical, organizational, or programmatic weaknesses identified through the analysis.
- Once corrective actions are complete, actions are evaluated for effectiveness by utilizing MIRACLE to look for similar weaknesses in data after corrective actions have been taken.
- If weaknesses still exist, a further STPA is performed to identify why the recommended actions were ineffective, and further corrective actions are taken.
- If effectiveness has been validated, information is disseminated to external stakeholders to also benefit from this process, so that not only can the plant using this process operate more safely and efficiently but all light-water reactors can improve as well, as long as they utilize this information properly as an input to their PIR process.

1.4.1 Machine Intelligence for Condition Log Review and Analysis

Every day nuclear plants collect information from many different sources and processes. Some of these involve human interaction and others are automatically produced by process equipment. All of this information helps drive the safe and reliable performance of the nuclear plant through immediate action or analysis, which is provided to senior leadership to support decision-making. U.S. nuclear regulations require that conditions adverse to quality are identified and resolved at the lowest level possible to prevent more significant events.

CAP is the process at a nuclear plant to identify and correct conditions adverse to quality. The current reactor oversight process requires that the NRC perform a biannual inspection of all U.S. nuclear plants' CAP processes. However, effectively evaluating two years' worth of data for each plant is a large task for the NRC. Therefore, the NRC reached out to INL for assistance in making problem identification and resolution inspections more effective. As a result, INL created a data-driven information automation program, MIRACLE.

MIRACLE maps data from various NPP data sources into intelligent groupings and attempts to determine the impact of these groupings on the plant. The automated identification and screening of these groupings allows the NRC to evaluate the plant's CAP program execution against these intelligent groupings to determine if the issues have been effectively reported, screened, and corrected. Currently, INL is developing various processes that utilize MIRACLE's information automation capabilities to help drive plant performance to higher levels of safety and reliability while reducing the overall cost of NPP operation.

1.4.2 Dynamic Work Execution Platform

One of the integral parts of improving plant safety and performance while reducing operating costs is automating work previously performed manually, and performing that work in a more flexible and intuitive digital environment is a DWEP. NPPs generate a lot of data for several reasons, including requirements to retain documentation from most processes affecting reactor safety as a condition of the plant license. Another reason is to analyze the output of work performed within the plant to review it for errors or opportunities for improvement. Performing work in a DWEP environment can improve work performance because this platform can not only emulate a manual process but improve it incrementally while the actual work is being performed.

The DWEP improves itself and the user experience through continuously improving the data that feed it and introducing an improved human-system interface to reduce errors while improving work efficiency. This is accomplished through intuitive AI that helps guide the end user through the work evolution while improving the very work process that is in use, in real time. One important element of the PIR model we discussed earlier is the locus of the intuitive insights that are fed into the DWEP process, which enable it to continuously improve the model. This is accomplished through near real-time STPAs and subsequent identification of factors impacting weak, weakening, or nonexistent SCSs. These issues can result in inefficiencies or even error precursors that can affect the plant evolutions, which provide data for analysis, and once identified, alter the DWEP by adding additional specific informational and procedural barriers to mitigate the effects of those inadequate control structures. The DWEP we utilized in this process was designed and implemented by NextAxiom® and has been integrated into many programs under development by INL.

1.5 The Information Automation Ecosystem

An IAE can be defined as a dynamic communications, process, and decision support system comprising a complex network of technology, humans, and the interfaces between them. In the current work, we are modeling the IAE as a control structure similar to those derived from STAMP or system dynamics modeling (e.g., Martinez-Moyano and Richardson, 2013). However, whereas STAMP deals primarily with SCSs, we suggest that an IAE should be considered a dynamic ICS whose function is to support the safety and performance of the plant.

With regard to plant data acquisition and processing, the IAE is sensitive to signals indicating emerging performance and safety issues and adverse trends within the plant. It should also (for system resilience purposes) be sensitive to signals indicating potential stressors on its own performance and reconfiguring itself as needed. The IAE system conveys information to appropriate, need-to-know personnel in an intuitive and actionable fashion through a process of ecological interface design (Bennett and Flach, 2011), providing alerts, trend information, and other support for decision-making. It facilitates critical lines of communication during both normal operations and system disturbances, supports the decision maker in assigning actions stemming from the issue, and tracks their progress, providing updates and reminders as necessary.

The information ecosystem concept itself is well known in information science and is defined as all structures, entities, and agents involved in transmitting information relevant to a particular domain, including the information itself (Keuhn, 2023). This definition corresponds well with a sociotechnical systems perspective, the latter emphasizing the importance of understanding the nature of the control and feedback relationships between the structures, entities, and agents that comprise any given system.

Figure 5 provides a high-level depiction of the IAE model as currently envisioned, which has much in common with the PIR model illustrated in Figure 4 above, including an emphasis on near real-time STPA as a means of identifying safety and ICS weaknesses.

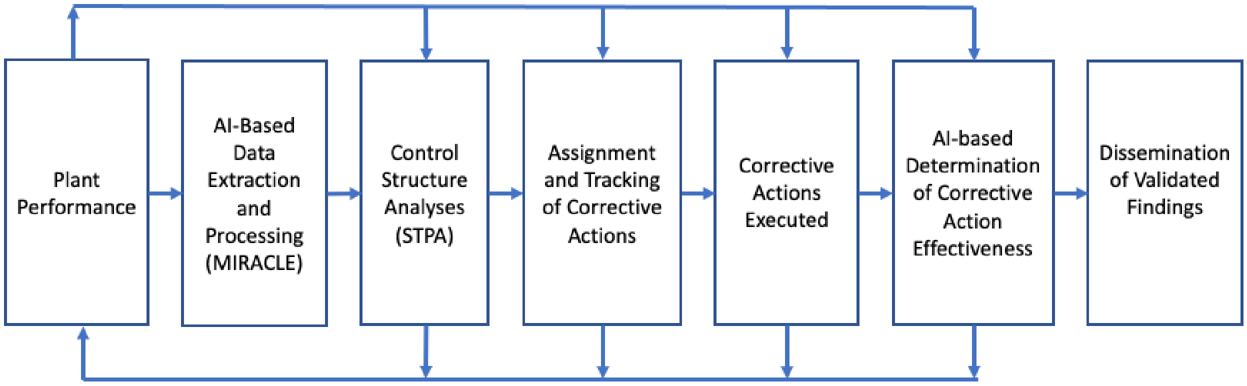
Plant Performance
AI-Based Data Extraction and Processing (MIRACLE)
Control Structure Analyses (STPA)
Assignment and Tracking of Corrective Actions
Corrective Actions Executed
AI-based Determination of Corrective Action Effectiveness
Dissemination of Validated Findings

Figure 5. Preliminary IAE model.

Within the context of NPP operations, a plantwide information automation system would:

- Continually process plant system and component performance data

- Perform data reduction and processing
- Analyze relevant safety and ICS trends to identify potential areas of concern
- Assign and track corrective actions, determine their effectiveness, and disseminate validated findings to appropriate personnel.

Assigning actions is an area where automation and AI may be of value in providing the user with suggested actions and approaches to address a particular problem.

1.5.1 Optimizing Information Automation

The principal goal of the current research effort is to support the development of an optimized information automation system. When using "optimized," we refer to the following suggested set of information automation system characteristics. These characteristics can be viewed as preliminary criteria for an optimized IAE, with particular attention to critical issues for effective human-system integration.

- *Accurate, reliable, and actionable information*. The quality and reliability of information provided to system users is foundational to any human-computer-machine system. Information reliability, transparency, and trustworthiness are particularly relevant when advanced automation and AI are introduced to a system. Finally, information output should also provide users with clear means for executing potential actions.
- *Timely information delivery*. Timing in information delivery can be a very critical factor impacting the quality of users' decision-making and responses. Since delayed decision-making and responses can extend system risk, it is important for information to be delivered in an appropriately timely fashion.
- *Continuous data extraction and processing.* As previously noted, there are multiple sources of relevant information within an NPP that, if continuously sampled and appropriately processed, can provide the basis for meaningful information about emerging trends, weak or strong signals, etc. An optimized IAE should be continuously sampling and processing plant data in search of potential areas of concern, which will also help determine the effectiveness of previously performed actions.
- *Targeted information delivery.* The system should deliver information in a timely fashion to individuals with a need to know. Typically, this would include individuals whose decisions and actions are required in response to an emerging condition within the plant, as well as relevant program and project managers and other requisite, need-to-know authorities within management.
- *Intuitive and easily usable human-system interface.* The quality and timeliness of decision-making and acting in response to emerging conditions is a direct function of the quality of the user interface. As has been shown repeatedly across multiple industries and applications, the interface must present information in an intuitive and easily understandable fashion, while also providing clear affordances for effective action.
- *Action tracking and notification.* The system may suggest recommended actions to the user who, in turn, makes decisions regarding actions in response to an emerging condition. Once assigned, the system tracks the status of individual actions and provides regular progress updates to the decision maker.
- *Ability to adapt to changing and challenging conditions (i.e., system resilience).* The system behavior is largely dependent on the situation and context within which it functions. When situational or contextual conditions change (e.g., schedules change, processes stall, unanticipated outages occur), the system should have the ability to detect such changes, identify potential stresses on relevant SCSs as well as its own information control system, and recommend potential actions to the appropriate decision makers.

- *Tailorable to individual plant requirements.* As different plants may have different physical and organizational infrastructures, a general IAE model should be modifiable to meet the requirements of individual utilities and plants.

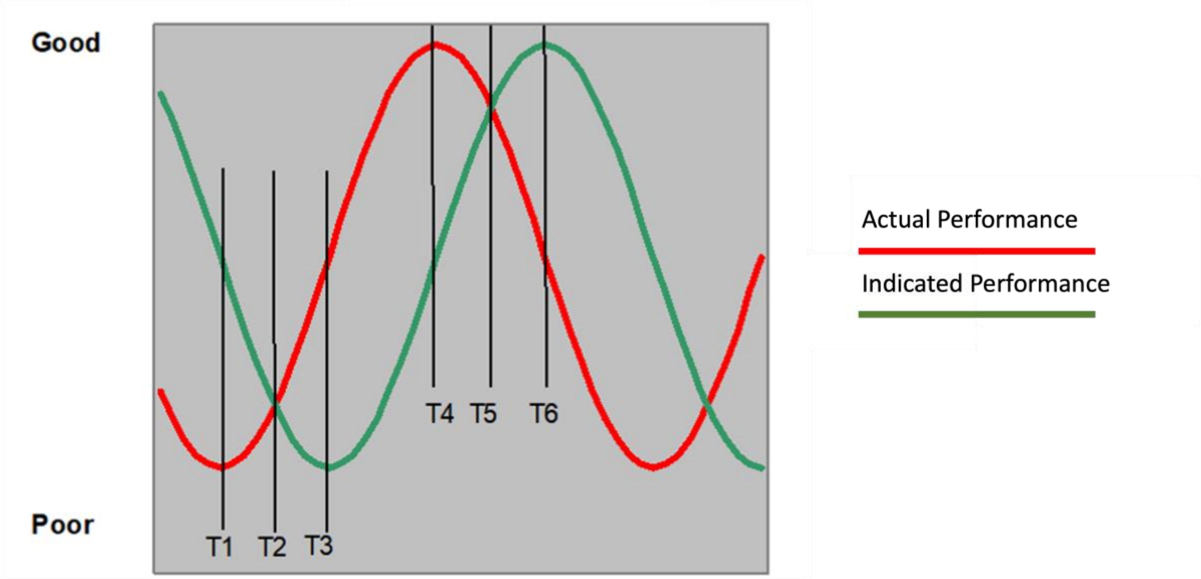

Figure 6. Time differences between indicated and actual plant performance.

Figure 6 illustrates the potential consequences of delayed information delivery. Specifically, if information is delayed in reaching the appropriate decision makers, the plant (or subsystem) status has likely already changed. Decisions and subsequent actions might be made in response to conditions that no longer exist and could even undo corrective actions that were beginning to make positive improvements. Eliminating or reducing this delay in information processing and transmission is an important aspect of an optimized information automation system.

1.6 The Role of Human-Systems Integration

A major goal of this research project is to support effective information automation design through the joint optimization of people, technology, processes, and governance, that is, to assure effective human integration with technical and organizational systems. Within the context of the current work, HSI has two meanings. The first refers to the systems engineering discipline of the same name (Booher, 2003) in which HSI coordinates and conducts the activities of the “human-related” disciplines in system design, such as human factors and ergonomics, training, personnel selection, safety, organizational design, and interface design and user experience. HSI, at this level, describes a cross-functional discipline within the systems engineering structure, essentially advocating for the user across the full breadth of a design. It is viewed as a key risk reduction approach during system design and development, based largely on the military’s experience with expensive and time-consuming system retrofits necessitated by a lack of attention to integrating the system with the humans for whom it was intended. HSI is as concerned with the design and implementation of organizational systems as it is with technical systems, as these also directly impact the human-system performance quality. As the current effort evolves from the conceptual, research phase to the system development phase, this meaning of HSI will become increasingly important.

HSI can also be thought of more narrowly as a research and design discipline focused on optimizing the relationship between humans and the sociotechnical systems within which they function. The work reported herein is an example of this sense of the term. Specifically, our goal is to understand the possibilities and limitations of current technologies and processes as they impact plant activities related to information transmission, model these sociotechnical systems and activities, and use that knowledge to impact both near- and long-term system improvements centered around optimizing information automation.

Both HSI domains were successfully applied in the design of the U.S. Navy's *Zumwalt* class of destroyers, the first major Department of Defense procurement to require HSI as a part of the design and testing process (Quintana, Howells & Hettinger, 2007; Tate, Estes & Hettinger, 2005). *Zumwalt's* design included a substantial amount of automation as it was intended to operate with approximately one-third the crew size of legacy destroyers while achieving higher levels of tactical performance. In these respects, the constraints on the *Zumwalt* design and incorporation of advanced technologies are quite similar to those confronting the nuclear energy industry today.

1.6.1 Sociotechnical Issues in Information Automation

With respect to the design and implementation of complex systems, such as information automation, sociotechnical refers to those aspects of the design that impact human performance and, by extension, broader system performance. While this encompasses traditional human factors and ergonomic concerns, such as interface design, it also extends into areas such as organizational design, job design, and managerial governance. In other words, any system aspect, defined as an interactive set of human and technical components, that has the potential to impact human performance is a possible area of concern and analysis.

Information automation systems present a number of potential sociotechnical system issues, many of which relate to the use of automation and AI. In addition to issues involving incorporating "expert systems" of this type into interface design, there are broader issues related to factors such as the number and type of people involved in operating the system, the manner in which their work is to be managed, and the nature of users' information and control requirements. Automation and AI introduce user trust and transparency issues, the latter referring to the user's ability to gain insight into AI activities and the basis for its actions and recommendations.

The sociotechnical methods applied in the current work support the design of optimized information automation systems by addressing potential issues such as those described above. Using a combination of analysis and modeling based on sociotechnical systems theory in general, and STAMP in particular, our goal is to identify human-performance-related shortcomings in current designs (the purpose of the CAST analysis) and in proposed future designs (the purpose of the STPA and organizational systems modeling [OSM] analyses).

1.6.2 Modeling the Information Automation Ecosystem

In Section 1.5, we define an IAE as a dynamic information and decision support system—one that can be modeled as a complex control system operating under the general principles of systems theory. One of the principal goals of the current effort is to analyze and, especially, model existing and potential ICSs for supporting information automation design.

There are two major functions served by modeling a complex sociotechnical system such as this, including:

- *Achieving a consistent mental model of the system.* People working within the same operational environment, such as an NPP, can often have very different mental models of the status of systems they are required to operate, maintain, etc., particularly under unusual conditions. Also, individuals involved in developing or deploying new systems may also have differing mental models of their designs, functions, etc. These differences often manifest in organizational confusion or loss of coordination in conducting activities. When analyzing and designing a complex sociotechnical system, developing a consensus model helps ensure stakeholders and users have a common understanding of the system under consideration.

- *Identifying system weaknesses.* Modeling is an efficient and effective way to identify potential weaknesses in an existing or proposed design. Static models, such as STAMP and System Dynamics Modeling are useful, relatively easy-to-use screening tools early in a design process, for instance. More dynamic, computer-based modeling methods, such as event- and agent-based modeling, are more time and resource intensive and are typically used later in a design process (Hettinger et al., 2015).

1.6.2.1 Identifying Existing and Potential Areas of Safety and Performance Risk

There are areas of potential risk in any complex sociotechnical system of the sort exemplified by NPPs. One of the main functions of modeling such systems is to support the identification and analysis of risk areas in current operations and in future system designs. CAST is a tool specialized for current operations while STPA is more directly useful in future system designs.

There are two major risk areas of concern in the development of the PIR and IAE models, safety and performance. The safety risk is concerned with the models' abilities to identify and adequately address safety risks to personnel and processes across the plant but also to guard against introducing unintended risk due to an inadequate information automation system design. Performance risk is concerned with the impact of information automation across measures of plant performance, particularly the introduction of unanticipated negative side effects. There are also performance risks associated with a system's ability to adequately support human-system performance and to meet its system-level and detailed requirements.

As noted above, modeling in general and STAMP in particular are useful for identifying existing or potential weaknesses in a design that can pose risks to safety and system performance. For instance, nonexistent, weak, or otherwise dysfunctional control and feedback links between key components of the sociotechnical system (people, technology, processes, and governance) are common red flags for introducing a potential risk to system performance.

1.6.2.2 Identifying Near-Term Opportunities for Performance Improvement

The primary objective of modeling the IAE using STAMP is to develop an ICS to support future system development. However, examining existing and proposed ICSs also aids in identifying opportunities for near-term system and process improvement. For instance, identifying organizational process bottlenecks in an existing system, one focus of the CAST analysis presented in Sections 3 and 4, can help inform near-term process changes while, in parallel, supporting future IAE development.

Areas for performance improvement are identified primarily by expert review groups who, once familiar with the control structure under discussion, examine its system components and linkages (i.e., control and feedback relationships between organizational and technical components of a sociotechnical system) for potential problem areas and potential solutions or approaches. It is not uncommon in these sorts of reviews to discover missing or dysfunctional feedback links between components as when, for instance, senior management is separated by several layers of communication and technology from frontline workers. This latter condition can contribute to a loss of "ground truth" awareness in senior management, resulting in nonoptimal decision-making based on incomplete, erroneous, or missing information.

1.6.2.3 Identifying Opportunities for Automation and Artificial Intelligence

Modeling the IAE also affords a means of identifying system areas that could potentially benefit from the introduction of automation or an AI/ML-based process. For example, process bottlenecks in the system involving communications are a common issue preceding and during unusual or emergency conditions in many industrial and process settings (e.g., Butts et al., 2007). An optimized IAE can identify the occurrence of such bottlenecks, providing the user with suggested or recommended courses of action to resolve the issue.

In short, an examination of control and feedback linkages within the overall ICS helps to uncover issues such as delayed communications, insufficient or inaccurate information, information delivered too late or at the wrong time to be useful, etc. Each of these common control structure weaknesses is potentially addressable with well-designed automation and AI/ML.

1.7 Return on Investment Considerations

The main goal of the LWRS Program is to enhance the safe, efficient, and economical performance of our nation's nuclear fleet through deploying innovative approaches to improving the economics and competitiveness of our LWRs in both near-term and future energy markets.

All complex systems such as NPPs realize events and issues at all levels of significance that directly affect operating costs—mainly in replacement power, investigation, and recovery actions. However, there are other costs that LWRs incur that are unique to the nuclear industry. Nuclear power is one of the most regulated industries in the world, for good reason—because of the inherent impact a beyond design-basis accident can have on the environment, population, other nuclear plants, and electricity infrastructure. Therefore, preventing significant events can have an immediate and long-term payoff.

In all cases, even these costs, although latent or more difficult to measure, can be monetized. They become manifest in the costs of the actions taken to address the issue, to react to violation of the regulations, and in the performance of the mandated causal analysis to prevent recurrence of similar events. As illustrated in Figure 7, we anticipate that developing an effective PIR process will result in a future distribution of O&M costs that would be considerably more favorable to the industry than is currently the case.

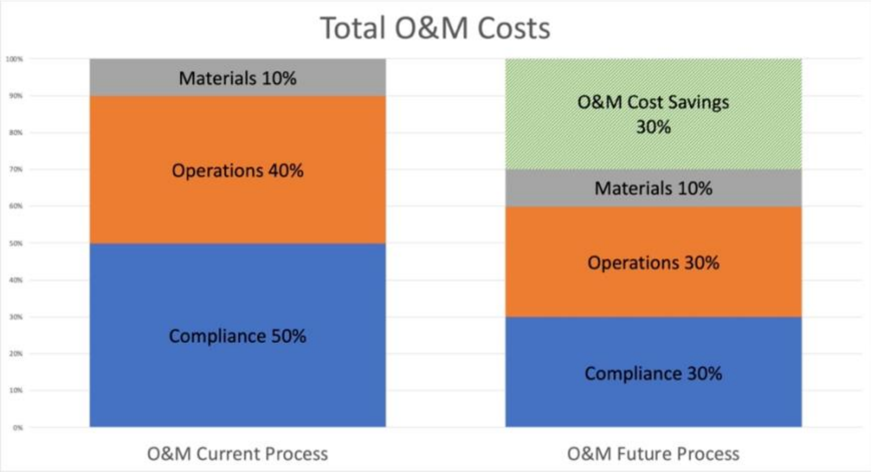

Figure 7. Projected impact of effective PIR on total O&M costs.

Sociotechnical system methods of the sort used in this program of research, notably those derived from STAMP and other HSI approaches, have also been shown to help control costs associated with complex system development and deployment (Rouse, 2011), thereby providing a positive return on investment in the earliest phases of the system lifespan. These analysis and modeling techniques provide an efficient and effective way of identifying and mitigating potential flaws in the system design and use early enough in system lifecycle to help defray later costs associated with retrofits or other fixes.

Industry experience has shown that the underlying organizational and programmatic causes of low-level events are the same as significant events and that, because of the high costs of significant events, the detection and proactive prevention of events at all levels is much more cost effective than correcting significant events.

2. OBJECTIVES

The major goals of the current research effort are to improve nuclear safety and reduce operating and compliance costs through proactive and real-time correction of technical, organizational, and programmatic factors that are precursors to human- and equipment-related events. A proposed means to this end is the development and application of an IAE sociotechnical systems model. Supporting the development of this dynamic network, comprising multiple technical and organizational components and supported by AI (i.e., MIRACLE) and advanced automation (i.e., DWEP), is the long-term objective of this work.

We selected the near-term objectives (Sections 2.1-2.3 below) both as logical follow-ons to work conducted in Fiscal Year 2022 (Dainoff et al., 2022), which demonstrated the utility of a CAST analysis in support of incident and event investigation, and as necessary steps in the early IAE development.

2.1 Objective 1: Apply Sociotechnical Systems Analysis Methods to Industry Use Cases

Over the course of this research effort, we will make use of several different sociotechnical system analysis and modeling tools to better understand existing safety and ICSs and to support the design of advanced models, such as PIR and IAE. The methods we will use include two based on STAMP—CAST and STPA. CAST analyses are very useful in describing and modeling existing safety and ICSs, as described in the current report and in previous, related work by Dainoff et al. (2022). STPA focuses on broader analyses of existing and potential systems, looking beyond the sociotechnical interactions that characterize specific events to examine broader system design and usage issues. STPAs in support of PIR and IAE model development will be the major focus of the remainder of the current year's effort. Finally, organizational system modeling will focus on mapping out plantwide ICSs.

2.2 Objective 2: Develop a Preliminary System-Theoretic Model of Information Automation

A second major objective of the current effort is to develop a systems-theory-based model of information automation, specifically one primarily based on sociotechnical systems theory. To this end, we have focused on modeling a near-term application PIR model and a long-term application, general IAE model.

The major focus of a sociotechnical systems-based model of information automation is to identify areas of potential concern with regard to human and broader system performance, as well as to identify opportunities for emerging technologies to effectively leverage human capabilities and compensate for associated limitations. This type of systems-theoretic model comprises information regarding people, technology, processes, and government and supports design by specifying and illustrating the relations between them.

2.3 Objective 3: Develop Preliminary Requirements for Human-System Interface Software and Display Design

The ultimate purpose of the current research is to support the development of an optimized IAE comprising utilities that enable rapid and reliable organizational communication and coordination. The PIR and IAE models that have been the focus of much of the current work are ultimately meant to provide a basis for system design and implementation.

System development relies on specific requirements at various levels of design specificity. In a typical systems engineering setting, the starting point for this process involves creating system-level requirements. This level of requirement is specifically concerned with what functionality the system needs. Subsequent finer-grained requirements are more concerned with increasing specification of how system-level requirements will be met.

We will create a set of preliminary system-level requirements in conjunction with technical expertise from MIRACLE and DWEP, as well as subject matter expertise from our industry partner. Additionally, we will create a set of preliminary system safety constraints that can be thought of as system-level requirements for what the system must not do and what it must be able to prevent from occurring.

3. APPROACH

Figure 8 provides an illustration of the current research effort's approach. The principal analyses we will perform include CAST, STPA, and OSM. Each of these relies on the availability of information such as incident reports (particularly important for CAST), knowledge elicitation sessions with industry technical and subject matter experts (SMEs), and documentation related to plant processes, procedures, and communications.

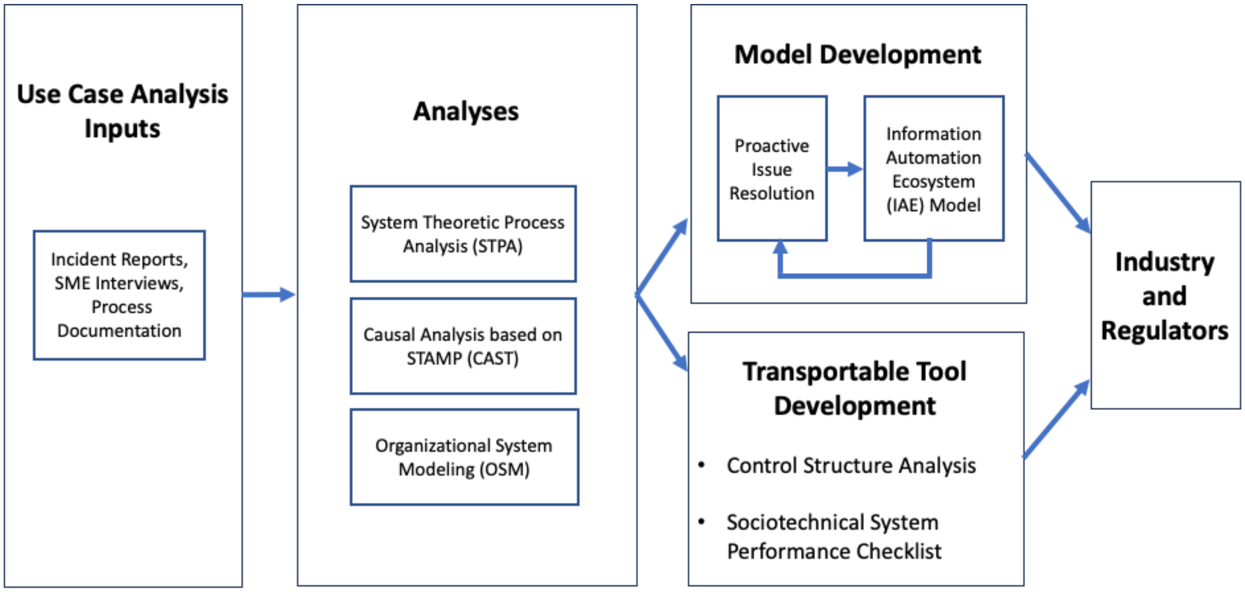
Use Case Analysis Inputs
Incident Reports, SME Interviews, Process Documentation
Analyses
System Theoretic Process Analysis (STPA)
Causal Analysis based on STAMP (CAST)
Organizational System Modeling (OSM)
Model Development
Proactive Issue Resolution
Information Automation Ecosystem (IAE) Model
Transportable Tool Development
• Control Structure Analysis
• Sociotechnical System Performance Checklist
Industry and Regulators

Figure 8. Research analysis and design approach.

The output of these analyses is intended to support two objectives. First, the development of safety and ICSs will support the development of the PIR and IAE models, as previously discussed. Second, the results will support the development of transportable tools for industry and regulators (i.e., simplified control structure analytic tools and checklists). Finally, all results along with models and tools will be disseminated as broadly as possible within the industry and regulator communities.

3.1 Use Case Selection and Description

The team considered several factors when determining the first use case to evaluate for this project, including: relevance to the nuclear industry, regulatory-related, complexity, cross-functional area interactions, a human element affected by known human error precursors that impacted the outcome, access to technical SMEs and investigators, and whether there was a common theme with other similar events that have occurred in the nuclear industry within the past few years. All of these factors will provide a great opportunity to identify event precursors and allow for the evaluation of causal factors at many different levels.

The goal of this project was not to reperform any investigation or challenge the approved result, but to analyze the incident from a different perspective, looking for opportunities to use the knowledge from thoroughly investigated and reviewed evolutions, to help build a fairly simple, transportable robust process that integrates information automation with a system theoretical process analysis so that end users can proactively identify and correct control structure problems from other low-level events. Analyzing thoroughly investigated breakthrough events gives a greater understanding of how the various control structures, including governance and oversight, interact within the plant and utility, as well as how they interact with the regulator. A thorough evaluation will require access to some of their procedures, investigations, and CAP data, as well as interacting with internal SMEs, to help the team to challenge conclusions and effectively develop this process.

3.1.1 Event Description

The first event that was evaluated by the team was an unexpected start of an emergency diesel generator (EDG), initiated by a human error during planned online maintenance that was originally planned as outage work. As it was an unplanned emergency safety function actuation, it was also reportable to the NRC. A review of the root cause investigation identified numerous departmental interactions not only with the modification approval, but during the planning, clearance activities, and work execution, all impacted by the implicit pressure of completing the work by a regulatory deadline.

Contracted groups were also involved in developing the modification and executing the work. Utilizing contractors throughout this evolution challenged the resilience of the established control structures, as it was one of the contracted groups that caused the initiating event. The fact that this is a common scenario for a work-schedule-adherence-centric plant influenced our selection of this event, as this situation in controlling the work management scope is common for all NPPs attempting to balance nuclear safety with plant production.

3.2 Use Case Analysis

3.2.1 Systems-Theoretic Accident and Modeling Processes

The techniques we used here to analyze the above use case are methods derived from a more general model of causality (i.e., STAMP) developed by Leveson and her colleagues (Leveson, 2011). This model changes the emphasis in system safety from preventing failures to enhancing sociotechnical system safety constraints. Accident causality is extended to the interaction among components, and the focus is on control rather than reliability. Leveson considers her work an extension of the groundbreaking work in cognitive work analysis (CWA) by Rasmussen, Pejterson, and Goodstein (1994).

3.2.1.1 Causal Analysis Based on Systems-Theoretic Accident Modeling and Processes

CAST is, as the title indicates, a STAMP-based method specifically aimed at accident analysis. It does not look for single causes but rather examines the entire sociotechnical system to identify weaknesses in the SCS. Its goal is to "… get away from assigning blame and instead shift the focus to why the accident occurred to prevent losses in the future" (Leveson, 2011, p. 345). In traditional accident analysis, it is difficult to avoid hindsight bias. Leveson (2011) makes the fundamental assumption that most individuals involved in accidents do not come to work planning to create a problem. Instead, actions that result in what looks like human error or failure to the observer examining the situation in hindsight must have seemed reasonable at the time. CAST attempts to find out why the actions might have seemed reasonable.

Unlike STPA, which examines the entire domain of interest, CAST focuses on event-relevant components. The CAST process is necessarily iterative, since examining weaknesses in the SCS may require analyzing additional components.

3.2.1.1.1 Major Components of Causal Analysis Based on Systems-Theoretic Accident Modeling and Processes

Figure 9 depicts the major components of a CAST analysis. This figure is modified from the CAST Handbook (Leveson, 2019). Additional information on CAST can be found in a tutorial (Leveson, Malmquist, and Wong, 2020) and in an example of an analysis of a radiation therapy accident (Silvis-Cividjian, 2022.)

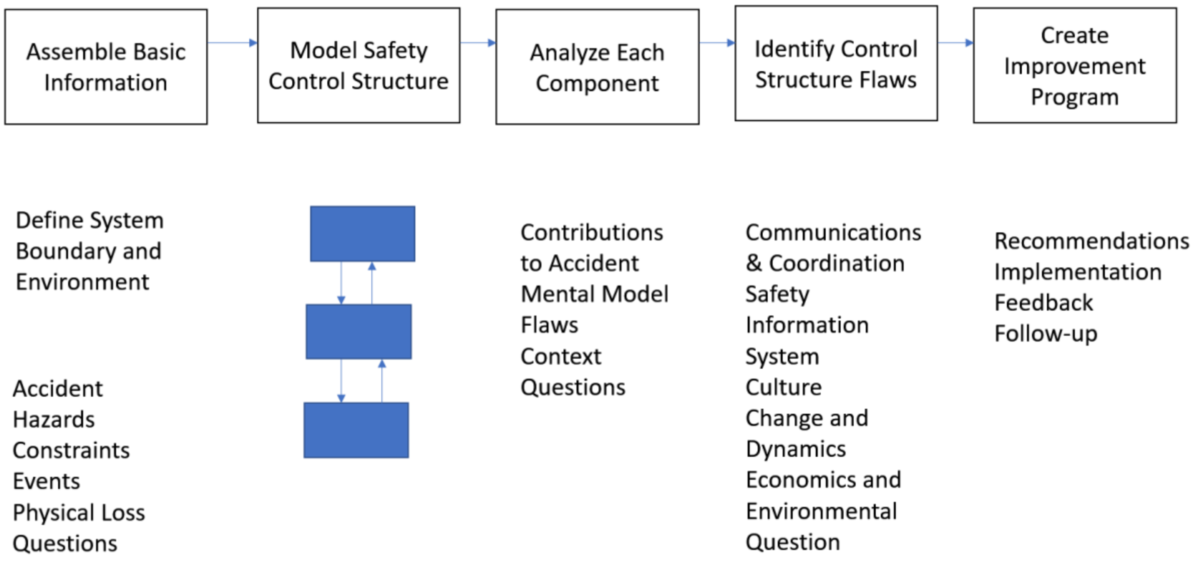
Assemble Basic Information
Model Safety Control Structure
Analyze Each Component
Identify Control Structure Flaws
Create Improvement Program
Define System Boundary and Environment
Accident
Hazards
Constraints
Events
Physical Loss
Questions
Contributions to Accident
Mental Model Flaws
Context
Questions
Communications & Coordination
Safety Information System
Culture
Change and Dynamics
Economics and Environmental
Question
Recommendations
Implementation
Feedback
Follow-up

Figure 9. Major components of CAST analysis (Modified from Leveson, 2019, p. 34).

3.2.1.1.2 Modifications Based on a Discussion by Leveson: Intent Specification and Means-Ends Abstraction Hierarchy

The following procedural modifications to CAST are based on a more recent discussion by Leveson (2020). Specifically, in the first section of the CAST procedure—Assemble Basic Information—an important step is to identify high-level hazards and safety constraints. Inherent in the STAMP model, relevant to both STPAs and CAST, are the relationships among hazards, constraints, and the SCS.

> Controls are used to enforce constraints on the behavior of the system components and the system as a whole and the identification of the inadequate controls will assist in refining the high-level system hazards and the safety constraints needed to prevent the hazards. (Leveson 2019, p. 44).

Leveson (2020) has suggested embedding a more formal representation of hazards and constraints within a means-end abstraction hierarchy—a concept taken from the work domain analysis approach of Rasmussen et al. (1994). Leveson prefers to call this representation an intent abstraction, reflecting the necessity to link lower level physical and operational details with the original intention—the “why”—found in the designer’s intention. These intentions are expressed in the representation of the systems hazards and constraints.

3.2.1.1.3. Modification Based on Johnson’s Coordination Model.

Johnson (2017) has identified the problem of coordination as a common issue arising in STPAs and CAST analyses and has proposed a modification of the basic CAST and STPA methodology to reflect this perspective. An examination of the content of the material comprising the EDG case study has led to the conclusion that the coordination perspective might be most effective in understanding the problem. This is primarily based on the observation that a significant contribution to the incident under study was a loss of evolution coordination affected by delays and perceived schedule pressure. Another contributor to the event was the plant mode in which the work was performed, which was originally planned for execution during an outage, but was switched to online, which introduced additional risks to the successful performance of the work.

Figure 10 depicts Johnson's models for fundamental coordination relationships in sociotechnical systems. Model C, in the lower left-hand section of the figure, seems to best reflect the situation in the current case study. Specifically, multiple independent decision systems and processes needed to be coordinated to yield a single outcome.

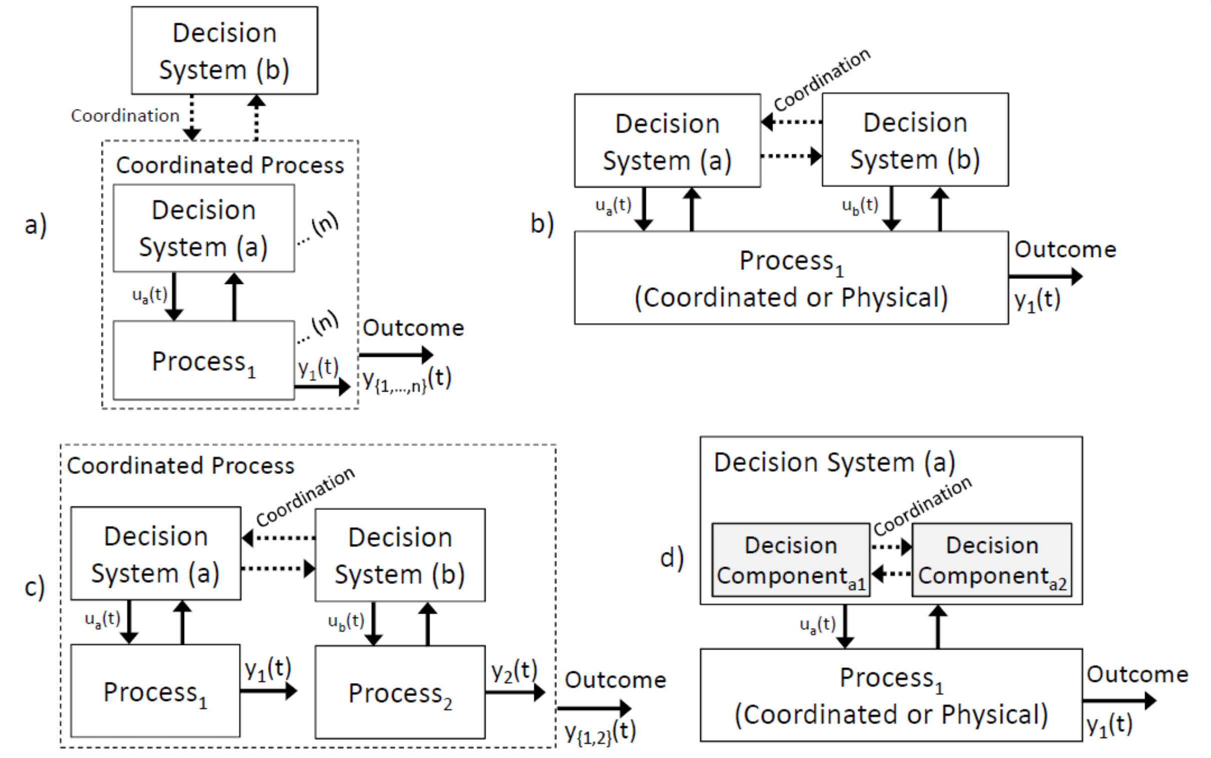

Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

$u_a(t)$: control action as a function of time
n: additional
y(t): output or outcome as a function of time

Figure 10. Fundamental coordination relationships in sociotechnical systems. (Johnson, 2017, Figure 12; Used by permission of author).

Figure 11 (Johnson, 2017, Fig. 11) presents a conceptual framework for coordination. There are three main sets of conditions and categories and nine coordination elements. This figure defines a spectrum of coordination.

According to Johnson, this spectrum can be characterized as:

- *None. The coordination elements that indicate coordination exists or is occurring are missing, in particular coordination goals, coordination strategy, and group decision-making.*
- *Partial coordination. One or more of the nine coordination elements is missing or inadequate.*
- *Holistic coordination. Coordination has the nine necessary elements in this framework.*

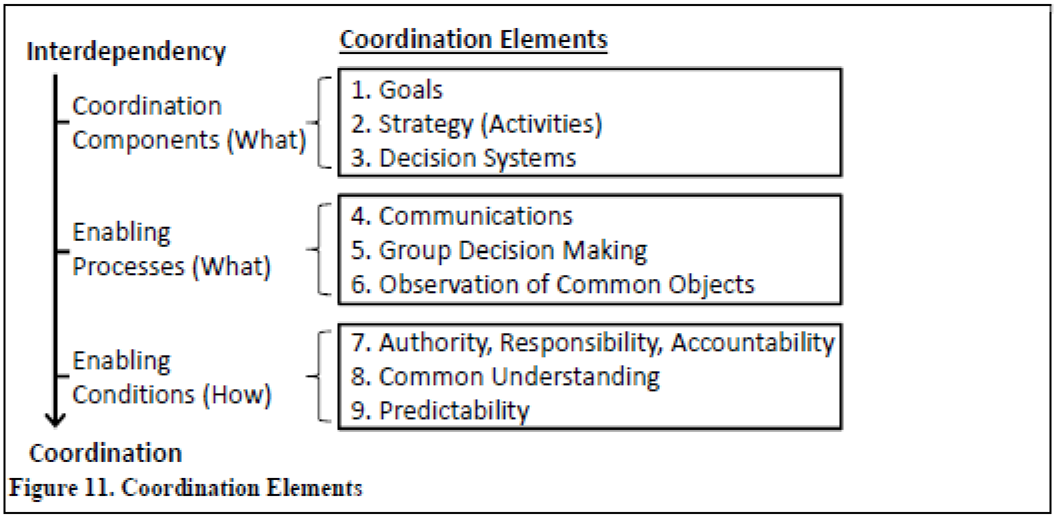
Interdependency
Coordination Elements
Coordination Components (What)
1. Goals
2. Strategy (Activities)
3. Decision Systems
Enabling Processes (What)
4. Communications
5. Group Decision Making
6. Observation of Common Objects
Enabling Conditions (How)
7. Authority, Responsibility, Accountability
8. Common Understanding
9. Predictability
Coordination
Figure 11. Coordination Elements

Figure 11. Element of coordination (redrawn from Johnson, 2017, Figure 11; Used by permission of author).

Figure 12 indicates how this framework can be used to modify the control structures used in CAST and STPA. This framework includes the same components of the traditional control structure, except that they are organized in a hierarchy-by-time plot.

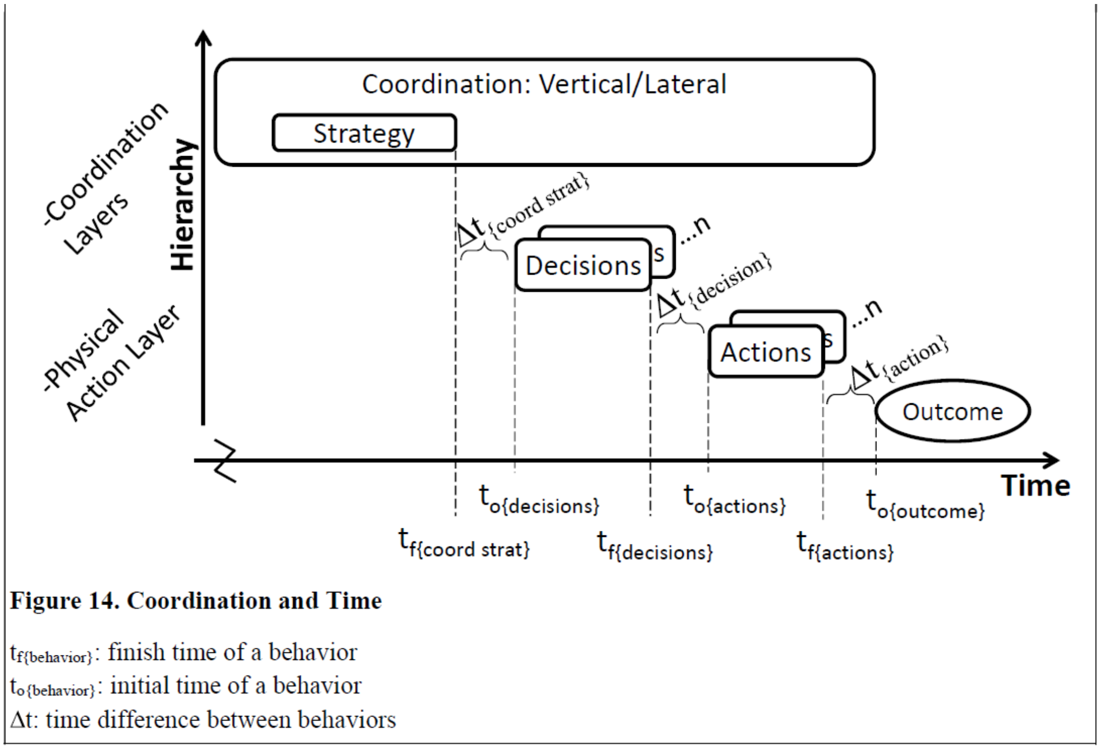

Figure 12. Modified SCS (from Johnson, 2017, Figure 14; Used by permission of author).

Hierarchy, displayed on the y-axis, consists of two basic levels: the required layers of coordination are on top and physical actions that emerge are below. These physical actions also include the production of key documents. In the situation depicted in this diagram, which reflects holistic coordination (see Figure 12), there is a linear relationship between the hierarchical progress downward of strategy, decision-making, actions, and outcome and time increments between each of these elements. However, when coordination is inadequate, strategic information relevant to decision-making arrives too late or not at all.

3.2.2 Organizational Systems Modeling

To supplement STPAs and CAST analyses, and to develop a means of gaining a plantwide perspective on organizational communications, processes, and documentation, we are developing a method we call OSM. OSM models and analyzes these dimensions of organizational activity to identify existing issues in current systems and potential issues in the design of future systems. Issues of this sort could include communication and decision-making bottlenecks, nonexistent or dysfunctional control and feedback links between system components, etc.

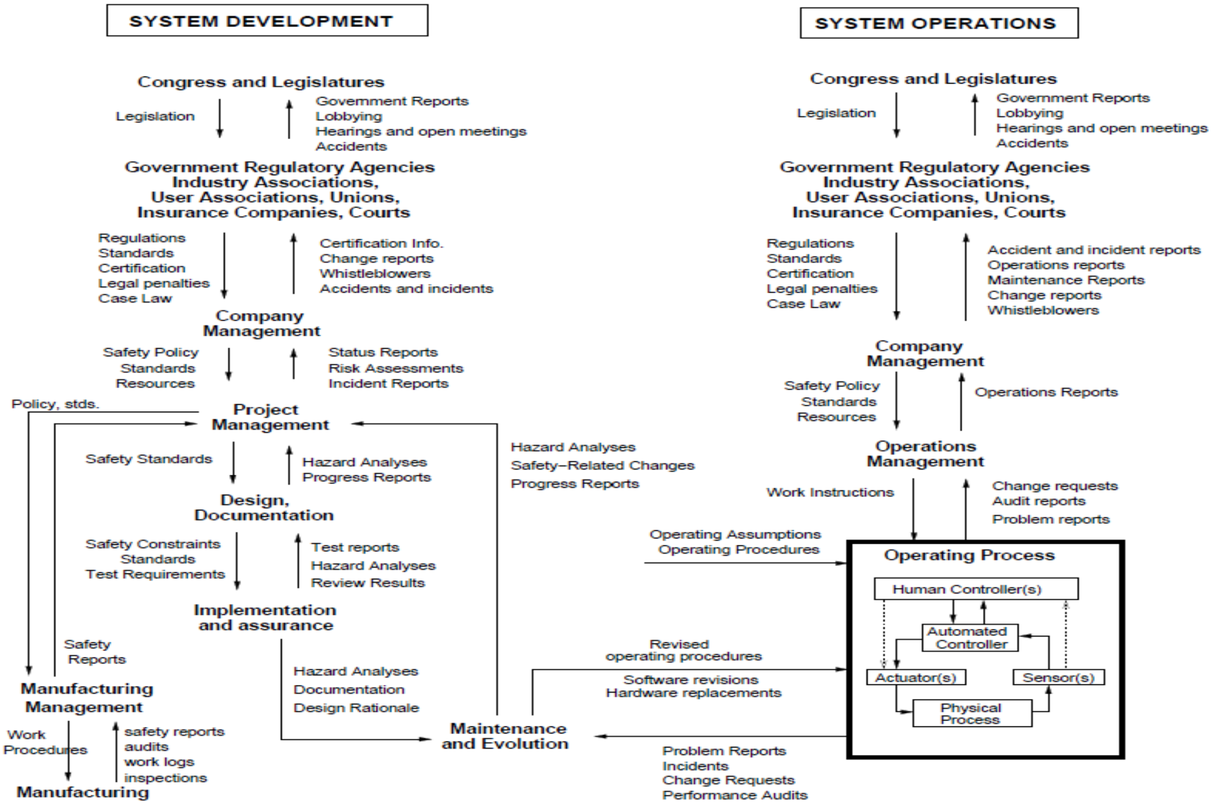

Figure 13. Sociotechnical system model incorporating organizational relationships based on STAMP and Systems Theory (from Leveson, 2011; Used by permission of author).

Figure 13 presents a generic organizational systems model based on Leveson’s (2011) STAMP approach. Illustrating the control and feedback relationships between organizational entities regarding safety in systems development and operations, this figure provides examples of the types of processes and documentation that constitute the control and feedback relationships within a given system.

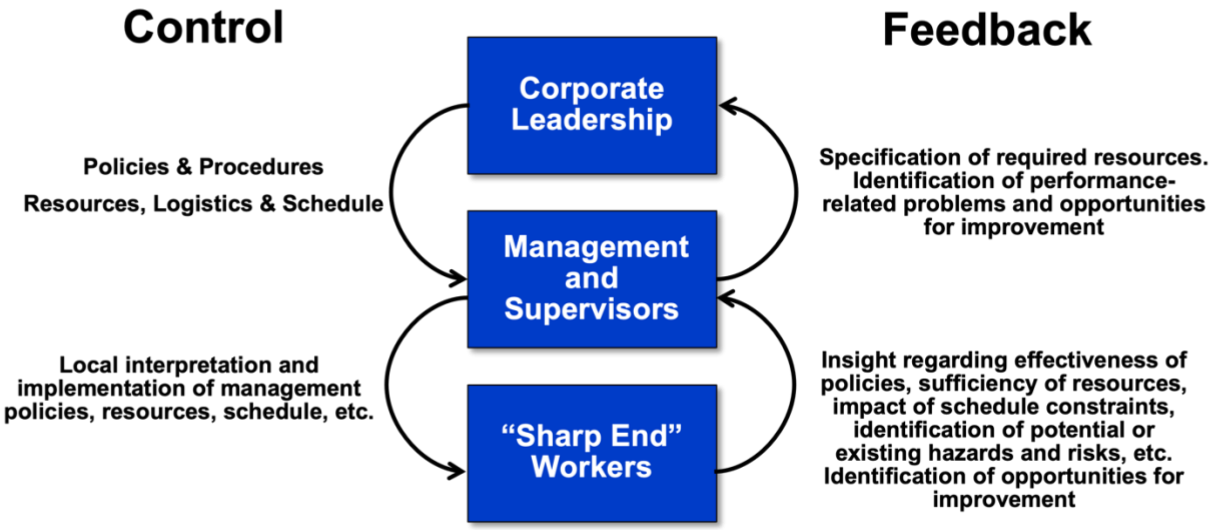
Control
Feedback
Corporate Leadership
Management and Supervisors
"Sharp End" Workers
Policies & Procedures
Resources, Logistics & Schedule
Local interpretation and implementation of management policies, resources, schedule, etc.
Specification of required resources. Identification of performance-related problems and opportunities for improvement
Insight regarding effectiveness of policies, sufficiency of resources, impact of schedule constraints, identification of potential or existing hazards and risks, etc. Identification of opportunities for improvement

Figure 14. Simplified organizational systems model.

Figure 14 presents a model of a generic organizational system at its simplest level (i.e., at the senior management, middle-management, and "sharp-end" worker level). As with all complex systems, whether biological or human-made, there is a hierarchical relationship between system components, with higher-level entities responsible for the control of lower-level entities which, in turn, reciprocate with feedback in performance, information, etc. Problems with insufficient or nonexistent feedback channels from lower to higher organizational levels, for example, are commonly observed and can result in poor senior-level decision-making due to missing, insufficient, or erroneous system feedback.

In the current work we have begun to examine the communication relationships within and between organizational layers, using our industry partner as an example, to identify current performance issues and opportunities for improvement in future control structure design. In combination with STPA and modeling, OSM will help provide a holistic perspective on the sociotechnical relationships comprising an optimized IAE.

3.2.3 Ecological Interface Design

Ultimately, users will interact with information automation systems through one or more human-system interfaces. One of our objectives is to support interface design using a user-centered, multidisciplinary team approach while applying relevant sociotechnical system analyses results. The interfaces themselves could take a number of possible forms, including digital, multisensory, and virtual displays. Regarding the latter, with enough proper sensors placed in key locations throughout the plant, a virtual presence could enable effective information transmission while also addressing reduced staffing concerns (Kovesdi et al., 2021). For instance, should a troubling signal occur indicating a potential issue somewhere in the plant, the proper user, upon being notified, could "go there" right away, even if the plant was in another state.

Ecological interface design (EID) (Bennett & Flach, 2011) is an approach to human-system interface design that is a logical outgrowth of CWA, building on its results in a manner that is very useful to developing prototype HSI concepts. One of the key outcomes of CWA is a description of constraints on the safe and effective system performance (e.g., information, control, and communication requirements). EID translates those descriptions of system constraints into representations and specifications for HSI prototyping and design. As such, it is a very useful tool for extending the results of CWA and other relevant, prior analyses into the candidate prototype designs.

EID focuses on developing HSIs that use visual and auditory methods to provide users with an intuitive understanding of underlying system activities and processes, freeing up the operator to focus on more complex decision-making tasks. EID is similar to other user-centered design approaches in that knowledge elicited from representative users and experts in earlier analyses support later HSI designs. However, EID's focus is primarily on the work space, as opposed to the end user, and seeks to effectively represent to the user all relevant possibilities for interaction with it.

The nuclear power industry is one of the contexts in which EID has been successfully applied (e.g., Vicente, 2002; Vicente & Rasmussen, 1992). As a natural extension of CWA, it is a particularly useful activity that can support designing prototype HSIs for later user testing and analysis.

3.3 Information Automation Model Development

One of the major objectives of this research effort is to develop information automation system models to support the design and development of useful applications for the nuclear industry. To that end we have begun developing the PIR and IAE models. The PIR model will support the near-term development of a proactive issue resolution utility that can also serve as a use case and model for developing the broader IAE system. This section provides descriptions of each model along with our approach to model development.

3.3.1 Proactive Issue Resolution Model Development

Control structures provide the constructs that dictate how an organization behaves both as a whole system and each component individually. When an NPP is licensed, the NRC evaluates the plant's design basis and eventually licenses the plant for power operations after approving all elements of the plant's ultimate control structure. Periodically, the NRC evaluates the compliance to these design bases, and the control structure is altered when improvements are warranted. This in itself is a continuous improvement process. Regulatory compliance is a mandated condition of plant operation—for good reason—and is considered the price of admission for the lowest level of acceptable performance. According to one utility, the cost of compliance to all regulatory requirements can be as high as half of the utility's operating costs. Figure 15 shows the breakdown of the most significant contributors to this utility's operating costs.

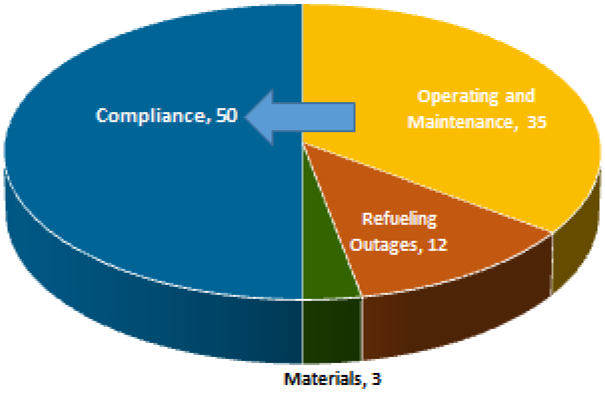

Figure 15. An estimate of one utility's operating costs.

Although compliance is the largest contributor to O&M costs, excellent plant production can offset the compliance costs as long as a high plant performance is sustained. Once plant performance begins to decline, operating costs increase, and if plant safety systems are not maintained properly, regulatory compliance also become more difficult—and costly. Failure to achieve an adequate level of regulatory compliance eventually results in a high level of regulatory enforcement, which, if not corrected in a timely manner, can cause a plant's operational costs to skyrocket to the point where a decision has to be made by the plant's financer as to whether they want to continue to operate or shut the plant down. Table 1, provided by the Congressional Research Service, shows nuclear plants that shut down as a result of their inability to economically comply with their licensing basis or operating costs that have become too high to compete with other more economical sources of generation without financial intervention by their respective state.

Table 1. U.S. nuclear reactor shutdowns: 2013–2021.

Reactor	**State**	**Shutdown Date**	**Generating Capacity (Megawatts)**	**Start-Up Year**	**Major Factor(s) Contributing to Shutdown**
Crystal River 3	Florida	February, 2013	860	1977	Cost of major repairs to reactor containment
Kewaunee	Wisconsin	May, 2013	566	1974	Operating losses
San Onofre 2	California	June, 2013	1,070	1983	Cost of replacing defective steam generators
San Onofre 3	California	June, 2013	1,080	1984	Cost of replacing defective steam generators
Vermont Yankee	Vermont	December, 2014	620	1972	Operating losses
Fort Calhoun	Nebraska	October, 2016	479	1973	Operating losses
Oyster Creek	New Jersey	September, 2018	614	1969	Agreement with state to avoid building cooling towers
Pilgrim	Massachusetts	May, 2019	685	1972	Operating losses, rising capital expenditures
Three Mile Island 1	Pennsylvania	October, 2019	803	1974	Operating losses
Indian Point 2	New York	April, 2020	1,020	1974	Low electricity prices; settlement with state
Duane Arnold	Iowa	August, 2020	601	1975	Lower-cost alternative power purchases
Indian Point 3	New York	April, 2021	1,038	1976	Low electricity prices; settlement with state
		TOTAL	9,436		

As noted in Section 1.2, a plant must always be vigilant to maintain optimal performance between safety and production. Higher performing nuclear plants that are able to remain in operation build upon the regulatory control structure by implementing a performance improvement process that effectively reduces unexpected compliance and operating costs through the continuous improvement of plant performance. However, even successfully operating nuclear plants are operating on relatively thin profit margins and are only one severe accident away from an event at any plant in the U.S. before it become too costly to operate.

Each significant event, especially those that reduce generation output or incur additional regulatory oversight can have a large negative financial impact on a utility, especially when there are sustained generation losses during recovery. Reducing significant events by even a small number can have a large impact on safety and production. It is generally accepted that detecting and preventing significant events is much cheaper than recovering from them. In 1735, Benjamin Franklin noted in an article printed in the Pennsylvania Gazette that "an ounce of prevention is worth a pound of cure." Although this was in reference to the impact of house fires on towns and was more than 200 years before the invention of commercial nuclear power, it still accurately pertains to the best way to reduce the impact of significant events on NPPs. Figure 16 represents the widely accepted concept.

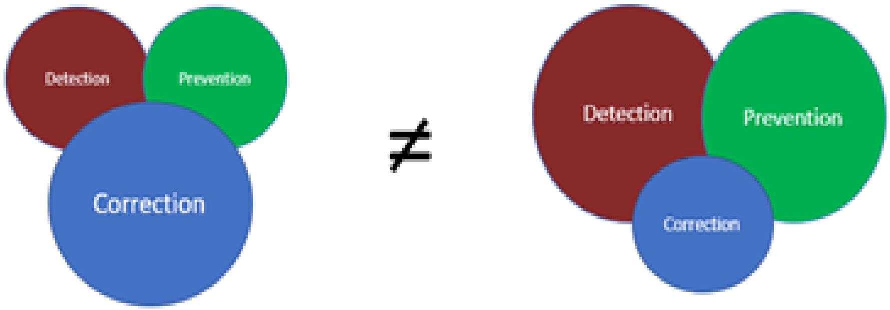

Figure 16. Impact of reduction of plant significant events.

Performance improvement programs employ various methods to retrieve and analyze sources of leading and real-time information to drive the detection and subsequent prevention of event precursors so that they correct these precursors before they can cause or contribute to more significant events. However, this process can be costly and cumbersome to manage with the return on investment often perceived as not worth the effort. In 2016, the Nuclear Energy Institute published Efficiency Bulletin 16-10 stating that "other alternatives should be considered to trending all issues through the Corrective Action Program," and that nuclear utilities should "adopt a philosophy of accruing a number of low-level issues through trending programs and then conducting common cause analyses on aggregate performance rather than individual event investigations."

There are two problems that would need to be overcome to be successful in this regard. First of all, nuclear plants have an entire formalized control structure for performing root cause investigations that include training, qualification, and several layers of review and approval. By design and to meet regulatory requirements regarding significant conditions adverse to quality, a plant's CAP needs to ensure that "the cause of the condition is determined, and corrective action taken to preclude repetition." However, aside from common cause analysis, there are relatively few methods that proactively and successfully identify organizational or programmatic causes, especially in low-level events or near misses. Secondly, CAP data is thoroughly screened and reviewed by collegial groups, and the control structure that was created to manage the CAP was established in the 1990s.

With advances in digitizing information, AI, and information automation established and improved by organizations such as INL, NPPs have capabilities that were not available to them in the past. Programs such as MIRACLE can quickly sort through data sources looking for groupings that constitute potential adverse trends and can automatically determine the significance of such groupings with fewer human resources than was previously possible. These capabilities have enabled this team to conceptualize a PIR model that utilizes a DWEP along with the information automation and proactive analysis method of STPA to improve prevention and detection capabilities.

The heart of the PIR model is identifying weak, weakening, or nonexistent control structures. The first part of this method is to understand how the various control structures are working at a nuclear plant utilizing analysis methods such as CAST and STPA to analyze the control structures at various levels within the nuclear plant. The most accurate way to do this is to evaluate previous significant events, such as the unplanned EDG start discussed at length within this report. Once the control structures have been evaluated, information automation can compile and validate various sources of plant information. It can then feed them into MIRACLE to identify adverse trends and potentially weak signals that are indicative of inadequate control structures. Further analysis is then performed and validated within information automation by being fed back into the plant processes through the DWEP. Once the process has validated that the organizational or programmatic causes being exposed are the result of weak or nonexistent control structures, corrective actions can be proposed, performed, and evaluated for effectiveness by examining the plant data output for indications that the problem has either disappeared altogether or is still evident and that additional analysis and actions will need to be taken through the DWEP until the issue has been fully eradicated or, if full elimination of the issues is not realistic, until it has been mitigated to a level acceptable to plant senior management and the regulator as validated through the reactor oversight process.

4. RESULTS

This section provides a description of the results of our analyses performed to date. These results should be considered preliminary until we can analyze further use cases and events over the rest of the fiscal year.

Results are provided for the CAST analyses performed on the unintended EDG activation use case, and for subsequent STPAs building off the CAST findings. For example, the issue of process coordination, particularly as a result of a significant schedule change, was identified as a key area of concern in the incident itself and, therefore, a potentially useful area for improvement. Subsequent STPA modeling focused on developing a potential ICS to address this and other issues.

We have provided interim results for organizational system modeling. This effort is geared toward the broader IAE modeling and analysis effort scheduled for the remainder of the current fiscal year. Its intent is to model, in control structure terms, the network of organizational entities and processes (information control and feedback relationships) that describe the broader organization.

We have also provided a set of preliminary, system-level requirements for developing a functional PIR and IAE system. These are expressed both as safety constraints (i.e., what the system must not do or what it must prevent) and more traditional system-level requirements as used in systems engineering approaches (what the system must do).

Finally, we have provided preliminary results from the return-on-investment analyses conducted to date. These focus on the near- and long-term cost benefits of conducting the types of analyses described in this report and on the potential cost benefits of supplementing these processes with automation and AI.

4.1 Causal Analysis Based on Systems-Theoretic Accident Modeling and Processes

The CAST analysis results are described below, including the suggested modifications proposed by Leveson and Johnson, as discussed in Sections 3.2.1.1.2 and 3. In the current case, it appears that the relevant coordination layers involved in the EDG incident include four functional areas: governance, design, clearance and risk management, and work process. We will use these functional areas to organize the analysis results, as appropriate.

4.1.1 System Part A: Assemble Basic Information

4.1.1.1 Define System: Model Hazards and Constraint Using Means-End Abstraction Hierarchy

The first step in assembling basic information is to characterize the system being investigated. In this situation, while the case study is investigating an incident in which an EDG was unexpectedly activated, the system is defined as one of unanticipated consequences of incomplete planning transitioning work from offline to online. Leveson (2020) has suggested the use of a means-end abstraction hierarchy to visualize the work domain under investigation. Embedded in the work domain is a table of hazards and constraints.

Inherent in the STAMP model, relevant to both STPA and CAST, are the relationships among the hazards, constraints, and SCS.

> Controls are used to enforce constraints on the behavior of the system components and the system as a whole and the identification of the inadequate controls will assist in refining the high-level system hazards and the safety constraints needed to prevent the hazards. (Leveson 2019, p. 44).

Figure 17 is a skeleton version of the hierarchy. In this particular case, as discussed in Section 4.1, the preliminary analysis of the available data led to the conclusion that coordination issues were most likely involved in this incident. The basic incident involved work originally scheduled for completion during the outage, when the affected work areas were offline, and execution of work during an outage posed less risk to the workers and plant. However, due to delays, the project needed to be transitioned from offline work to online. It was in this transition that coordination issues seemed to affect the final outcome of the event.

Accordingly, we used a levels of coordination approach, following the suggestion of Johnson (2017, Figure 17). The specific levels identified with each of the three aspects of project work were governance, clearance, design, and work processes.

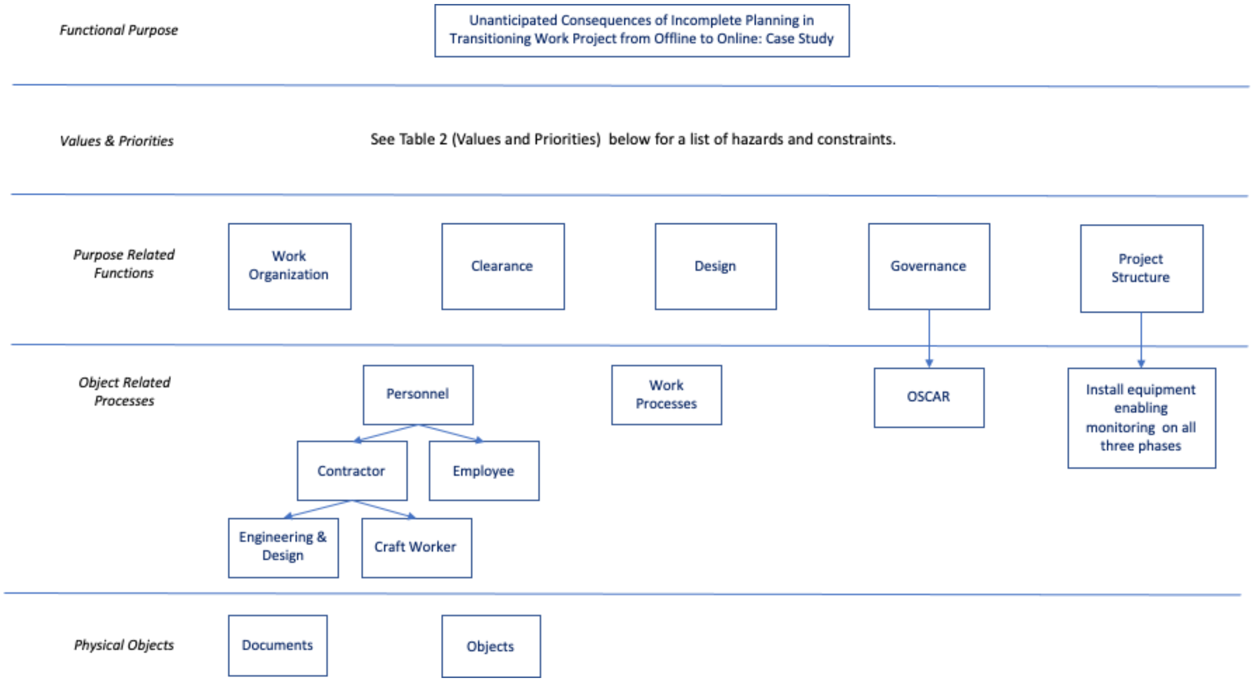
Functional Purpose
Unanticipated Consequences of Incomplete Planning in Transitioning Work Project from Offline to Online: Case Study
Values & Priorities
See Table 2 (Values and Priorities) below for a list of hazards and constraints.
Purpose Related Functions
Work Organization
Clearance
Design
Governance
Project Structure
Object Related Processes
Personnel
Work Processes
OSCAR
Install equipment enabling monitoring on all three phases
Contractor
Employee
Engineering & Design
Craft Worker
Physical Objects
Documents
Objects

Figure 17. Skeleton means-end abstraction hierarchy.

Table 2 depicts an expanded version of the values and priorities level of the hierarchy containing the hazard and constraints. These are meant to represent the designer's original intention. In this way, specific functional processes and physical objects can be traced back to these intentions.

Table 2. Values and priorities.

System Hazard #1: Loss of Power to Nuclear Safety Power Sources
Safety Constraints:
Power must always be available to nuclear safety-related equipment to ensure that the reactor core is always protected
Work on safety-related power sources must be carefully planned and executed to reduce impact on important systems needed to protect the reactor core
Plant design bases rely on the maximum availability of nuclear safety-related power sources
System Hazard #2: EDG Unavailability
Safety Constraints:
EDGs must be available to provide backup power to safety-related equipment
When normal power is lost to nuclear safety-related equipment, EDGs must be able to provide power
Backup EDGs are required by the plant design bases
When NPP EDGs are actuated due to a loss of normal power sources, core damage probabilities increase
System Hazard #3: Extended Safety Bus and MCC Outage
Safety Constraints:
Online work management uses probabilistic risk assessment to minimize the risk to the reactor core when working on nuclear safety-related power sources
Modifications to nuclear safety-related power sources should ensure minimum impact on nuclear core damage probabilities
Unanticipated events on nuclear safety power sources delay restoration of optimal nuclear safety plant configurations
System Hazard #4: Injury to Workers
Safety Constraints:
Unexpected, energized equipment at all voltage levels poses risks to workers
Work management processes and procedures need to ensure that workers are protected from injury
Supervisory oversight is designed to increase safety of plant workers
Walkdowns by planning and work execution workers should identify safety risks to workers
System Hazard #5: Addressing Regulatory Compliance
Safety Constraints:
Plant licensing process by the regulator is designed to ensure maximum nuclear safety is achieved
Reduced regulatory margin at one nuclear plant results in captivation of regulator resources that could be performing proactive identification of other nuclear plants' reduced regulatory margins
Reduced regulatory margin can impact the viability of all NPPs

4.1.1.2 Construct Proximal Events Table

A major step in the analysis is collecting information about the event. The goal is to be comprehensive, seeking as many contributing factors as possible to avoid similar events in the future. A typical procedure is to construct a proximate events table. Table 3 presents proximal events leading to the inadvertent activation of the EDG. In constructing this table, the focus should not be on selecting one or two causes. Instead, the purpose of the table is to generate questions for the investigation and be the primary input to the investigation. In this particular case, because of the levels of coordination focus, the proximal events table has already been organized according to these levels.

Table 3. Proximal events table.

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
1	Byron modification project approved	—	—	—	Corporate review board approved modification project	High/low side joint project approval. Did project size hide complexity?	Initiating event
2	Contracting engineer (CE) walkdown not fully effective because Bus 3 Cubicle 318 was covered	CE was required to conduct a project walkdown to identify possible interferences with running cables needed to complete the project and was unable to fully identify the drawer in the Bus 318 cubicle because the back of the cubicle was inaccessible.	—	—	—	Done after mod was issued. Why was the back of the bus covered such that the Engineer of Choice couldn't see it? Why didn't someone use their stop work authority here and declare this was an inadequate walkdown? Why wasn't the CE accompanied by a supplemental worker (who would be doing the actual "wrench" work) during the walkdown? When the decision was to move this work to when the NPP was still online, why wasn't this walkdown performed again to evaluate the impacts of opening this bus drawer while the	The Potential Transformer (PT) drawer was potentially visible to the CE during the project walkdown because the cubicle door was opened during the walkdown, and the PT drawer should have been visible when the cubicle door was open. However, the personnel conducting the walkdown did not consider that the drawer would need to be opened to complete the mod since entry was from the back of the bus cubicle for the other cubicles that were completed. Note, the PTs would not be energized when the work was scheduled as outage work, and even during the online work, the high voltage side of the PTs would be dead; however, other circuits (load

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
						plant is online? There appear to be two different and disjointed processes running in parallel, the design review process and the outage review (OR) process. When the OR decision was made, why wasn't there feedback to the design review process to direct it to go back and redo several steps?	sequencers) within this unique cubicle would not be dead because the work was performed online with the assumption that the workers would not need to open the drawer
3	Bus de-energization plan for outage complete	—	—	—	Outage electrical bus de-energization plan complete	—	Important to note because there would be no risk of an EDG starting if Bus 3 is fully de-energized (which would be alright during an outage because other live buses not mentioned would cover diesel safety functionality)
4	OR to perform project online approved	—	Design is still incomplete	—	OR to perform Bus 3 PT installation and testing online approved by operations manager and plant manager and the scope of work and risk assessment did not discuss new PT	Previous efforts to address the Byron open phase vulnerability were performed when the NPP was offline (during outages). Why not by the maintenance or	No real discussion as to why the OR process did not recognize and evaluate why the PT drawer (load sequencer relay) would still be energized in this configuration. If the OR process included engineering for

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
					cable interference or recognize Bus PT drawer in Cubicle 318	engineering manager?	approval, this may have caught or identified this risk.
5	Clearance request submitted for Cubicle 318 work order	—	—	Clearance Request submitted in plant (electronic clearance program/system) for WO 360. Does not recognize Fuse B318 in Cubicle 318 and does not request isolation of this fuse. Clearance request does not support the work to install the cables because it lacked details on hazards specific to the evolution of this work activity.	—	—	Clearance request does not recognize two things, 1) that the workers could be exposed to dangerous voltage contained somewhere within the cubicle (in the drawer), and 2) that actions in the cubicle could result in the start of the EDG.
6	Work order walkdown	Work order 360 walkdown signed off as completed by construction contractor general foreman. Personnel actually involved in construction (construction subcontractor)	—	—	—	Construction workers were not involved in walkdown (significant issue).	Individuals installing the cables should have performed each cubicle walkdown as its own entity, each with its own inherent risk. However, workers that would be actually performing the work were not involved in this walkdown.

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
		were not involved in this walkdown.					
7	Clearance for work prepared	—	—	Planner prepared Clearance 108 for work order 360.	—	Clearance boundaries are protection zones—like lockout/tagout to isolate a part of the system to work on.	Planning should have treated Cubicle 318 as special, not the same as the others—this was complacency. There were four cubicles and this one was different from the others.
9	Independent review of clearance 2EA performed	—	—	Planner performed independent review of Clearance 108 but did not recognize that individuals would be working in the vicinity of Cubicle 318 drawer with 4 kV present.	—	Although an independent review was performed, the original and independent reviews both failed to recognize that individuals would be in the vicinity of the Bus PT drawer—so far, all walkdowns failed to identify this risk.	The independent reviewer should have recognized the risk to workers and the plant; however, it is unclear how “independent” this review was. The Human Performance tool of independent verification failed here.
10	Stop work order	—	—	—	Stop work order issued by shift manager due to delays in schedule	Project was having trouble meeting deadlines.	Final design was completed only 3 months earlier.
11	SRO verified actual clearance for work on Bus 3 Cubicle 318	—	—	SRO verified Clearance 108. Did not identify a clearance issue associated with working in vicinity of Bus 318 PT drawer with 4 kV present.	—	The Senior Reactor Operator (SRO) is a senior licensed operator. Were appropriate drawings available at that time?	The SRO is actually a field supervisor and did not identify the risks specific to Cubicle 318, most likely because this clearance was used for all Bus 3 work, and it was not considered that individuals would need to open the PT drawer

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
							on this specific cubicle. Note, this is another verification as a barrier to errors that failed.
12	Review board addresses stop work	—	—	—	Review board to address project stop work held with plant manager, quality control (QC) engineering, construction contractor, operations, planning, and project management	Why was the unique nature of Cubicle 318 not identified?	This meeting should have identified the unique issue with Cubicle 318 and added additional barriers to prevent the worker safety issue and the possibility that load sequencer work in Cubicle 318 could result in an auto start of the EDG.
13	Additional table top meeting held to address the stop work	Table top meeting held to address the stop work with project manager, engineering, construction contractor, production planning, QC, and planning for remaining cubicle work, cubicle tie-in work, and load sequencer tie-in work. Discussed lessons learned and durations for work, corrections, and	—	—	—	Why was the unique nature of Cubicle 318 not identified?	This meeting should have identified the unique issue with Cubicle 318 and added additional barriers to prevent the worker safety issue and the possibility that load sequencer work in Cubicle 318 could result in an auto start of the EDG.

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
		changes to work plans made.					
14	Final review board for project	Restart work authorized	—	—	Final review board to address the project stop work held with plant manager, QC, engineering, construction contractor, operations, planning, and project management	Why was the unique nature of Cubicle 318 not identified?	This meeting should have identified the unique issue with Cubicle 310 and added additional barriers to prevent the worker safety issue and the possibility that load sequencer work in Cubicle 310 could result in danger to installers and an automatic start of the diesel.
15	Work commenced on Cubicle 318	(2) Pre-job briefing with the construction general foreman. (3) Subcontractor construction crew signed on to Clearance 108 and performed a 2 minute drill. (5) Subcontractor construction crew examined the sign on the door of Cubicle 318 that indicated the drawer was not to be opened. They checked the isolation sheet	—	(1) The operations SRO authorized tags placement for Clearance 108.	(4) The project manager met the subcontractor construction crew in Cubicle 318 to observe opening the rear panel and determining the work required for connections	Cubicle 318 contained the Bus 3 PTs, which was different than the other three cubicles. Two of the three other cubicles contained PTs for the source, while the third did not contain an existing PT.	Because the workers had successfully completed previous operations with PT interferences, they were preconditioned to believe it was acceptable to open the PT drawer in this cubicle. The workers did not experience adverse effects with previous work as the respective PTs were included in the isolation. Terminating event

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
		from their work package and saw the number 318 in the tagout list. They had previously successfully completed tasks in different cubicles in which open drawers were necessary. Believing the fuse was isolated for Cubicle 318, they opened the drawer containing Fuse B318. This action resulted in the activation of the EDG					

4.1.2 System Part B: Model Safety Control Structure

Figure 18 depicts the control structures reflecting events through and including the terminal event in which the EDG was triggered and follows the format used by Johnson (2017, Figure 14) as discussed in Section 4.1. As in traditional control structures, the elements consist of controllers, controlled processes and objects, control and information links (arrows), and feedback links (arrows).

The y-axis contains the four functional areas described above as well as the physical actions layer. For reasons that will become clear, the y-axis space devoted to governance and physical action is larger than the space for the other functions. The x-axis depicts time, in this case the approximate number of workdays into the project at which each controlled action occurred.

Regarding Figure 18, we should clarify that we have been limited to details that were publicly available in the published analysis. This implies that, in many cases, we would be able to identify problem areas with the control structure but would not have enough specific organizational detail to propose more specific solutions.

Accordingly, some components of the control structure are depicted with dashed lines. These components were not actually present in the proximal events table but are implied by their presence. Thus, the first event is the approval of the basic project comprising the case study—the Byron Modification Project. This is approved by a corporate review board, which is depicted at the governance level. However, the members of the review board are not identified. The approval is also reflected in the governance level as a controlled process. However, this level also acts as a controller, depositing a document reflecting the approval of Byron Modification Project at the physical action layer. Note that information from this document will later become part of a larger collection of project design documents and that this analysis focuses on a single incident at a specific location. Therefore, the activity at the physical action level is, until the very end, characterized by changes in document status and the addition of new documents (e.g., clearance and stop work order). The very last physical event is the unexpected automatic start of the EDG.

Since this CAST analysis is, by definition, limited, the control structure ignores other physical work successfully completed on this project.

The first three steps, from Day 1 through 660, reflect events that occurred while the project was still expected to be completed offline during the next planned outage. On Day 700, realizing that the final design specifications and drawings had not yet been completed, a formal outage review process designated the project be scheduled for completion while the plant was online. Unfortunately, the available documentation provides no details of how this review was accomplished. As a matter of completion, there were a number of other design and work process steps accomplished during this period, but they are not listed because these steps assumed that the work would be accomplished offline when the risk was much lower.

From Day 770 through 1,031, the project proceeded through various approval steps. There were basically two items relevant to analyzing the incident: clearances (i.e., ensuring that the workers could safely perform the task and that appropriate lockout tags were provided) and coping with a stop work order due to problems meeting schedules. Not shown in Figure 18 is the final completion of design details on Day 827. This is 70 days before the stop work order. Finally, the major events of the terminal event are depicted on Day 1,061.

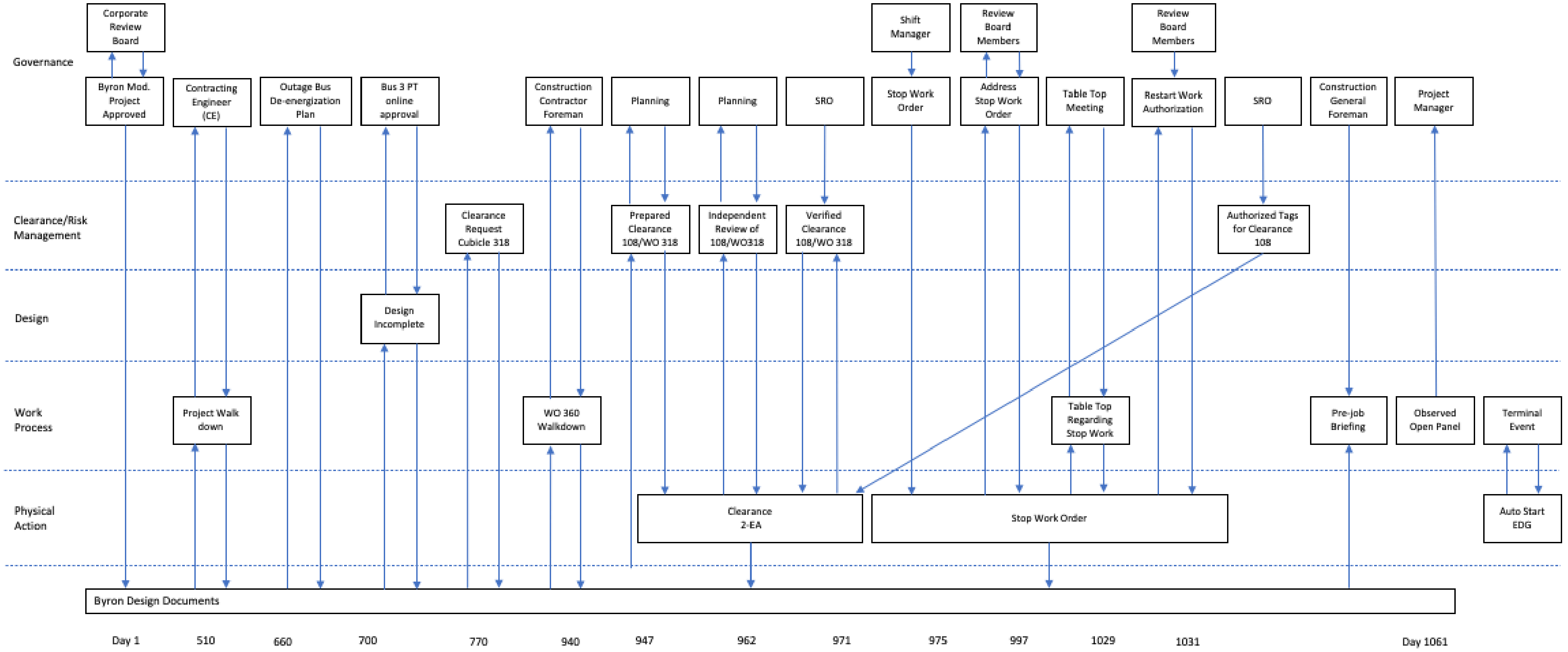

Figure 18. SCS using the format by Johnson (2017).

4.1.3 System Part C: Analysis of Individual Components of the Control Structure

Table 4 summarizes the results of this analysis and indicates each controller's responsibility within the SCS. Contributions reflect the extent to which actions, lack of actions, and decisions contributed to the hazardous state. Process flaws refer to either individual mental models or procedural flaws. Context refers to environmental or behavior-shaping factors that influence a controller or controlled process.

In some cases, we have inferred some of the information in this table from published material but have not been able to directly verify it. This should not detract from the conclusions.

Table 4. EDG autoactivation SCS individual controllers.

Controller or Controlled Process	**Responsibility**	**Contribution**	**Process Flaws**	**Context**
Corporate Review Board Day 1	Approve Byron Station Modification Project	Approval of entire project for one outage whereas other NPPs used two outages: one for the high voltage side and one for the low voltage side	Decision-making under time constraints.	Previous progress had been slow in meeting the NRC deadline. Note that 510 days elapsed between the approval and project walkdown
CE Day 510	Project walkdown for interferences with potentiometer cable runs	The back of Cubicle 318, which housed load-balancing relays for the EDG, was covered so that photographs could not be taken	The CE did not seem to be aware of the role of Cubicle 318 in the plant's safety systems, where a drawer contained the voltage source of the Bus 3 load sequencer voltage relays. An interruption in the load sequencer would have activated the EDG. Moreover, opening this drawer would have put workers in the vicinity of 4 kV. According to the PRA safety constraint described above, the EDG is the second most critical element in plant protection.	Given that the work was scheduled for offline completion, the risk associated with the autoactivation of the EDG would have been lower.
Bus Modification Planner Day 660	Bus modification plan approved for offline work during the upcoming outage.	Plan was approved before the design process and associated drawings were completed.	The risk associated with Cubicle 310, as described above, was not identified.	The risk continued to be considered low since the work was scheduled for completion during the outage.
Outage Review	Transition procedures for projects originally	No indication of the risk associated	There is no indication in the available	The final design, with applicable drawings

Controller or Controlled Process	Responsibility	Contribution	Process Flaws	Context
Day 700	scheduled to be accomplished during the outage but now are to be done online.	with the Bus 3 PT drawer in Cubicle 318 was provided. Nevertheless, the plant manager and the operations manager signed off on the transition package.	documentation of what the review process was or who carried it out. It is interesting that neither the engineering manager nor maintenance manager is listed as signing off on the transition package. It can be surmised that the appropriate transition procedures were not followed.	and calculations, was still 127 days from being completed when this decision was made. The outage was scheduled to begin in 152 days.
Clearance Requester Day 770	A clearance order request was submitted for work order 360. representatives sign off on the overall project.	The requester did not recognize Fuse B318 was in Cubicle 318 and did not request the isolation of this fuse, which was in the pathway of the safety-critical EDG.	The clearance request supports the work to install the cables, but it lacks controls on other hazards specific to this work activity.	This request seems to be a revision of a previous clearance request created in an earlier version of an online work management system. However, the earlier clearance also did not have the required warnings. At about the same time as the plant was switching over to the new version, it was also transitioning to a different work management system. Thus, there were two versions of work management systems running in parallel.
Construction Contractor Foreman Walkdown Day 940	According to procedure, this is a craft walkdown to determine if clearance is adequate for work.	Foreman did not recognize Fuse B318 was in Cubicle 318 and did not request the isolation of this fuse, which was in the pathway of the safety-critical EDG.	Although this is supposed to be a craft walkdown, none of the craft personnel from the subcontracting construction company were involved. Rather the supervisor performed the walkdown. However, the supervisor would not have the requisite knowledge of any	A subcontractor was hired to do the actual work as they would have detailed knowledge regarding cable runs. However, the foreman of the company who hired the subcontractors did the walkdown without any of the crew members.

Controller or Controlled Process	**Responsibility**	**Contribution**	**Process Flaws**	**Context**
			other components within the bus, just as the implementing crew would not.	
Planning Prepared Clearance 108 Day 947	Prepare Clearance 108 for work order 318 to ensure no hazards exist for the work process.	Clearance boundaries were inadequate for the job scope.	The planner did not recognize Fuse B318 was in Cubicle 318 and did not request the isolation of this fuse, which was in the pathway of the safety-critical EDG, or recognize that workers would be in the vicinity of 4 KV.	There is some suggestion that there was confusion because different work processes were logged in two different work management systems. However, the basic information regarding the importance of Cubicle 318 to the EDG safety system was still missing.
Planning Independent Review of Clearance 108 Day 947	Review Clearance 108	Did not recognize that boundaries were inadequate for the job scope.	The reviewer did not recognize Fuse B318 was in Cubicle 318 and did not request isolation of this fuse, which was in the pathway of the safety-critical EDG, or recognize that workers would be in the vicinity of 4 KV.	Importance of Cubicle 318 to EDG safety system is still missing.
Shift Manager Issue Stop Work Order Day 971	Stop work order was issued because the project was falling behind schedule.	Opportunity to review the project to determine the reason for delay.	n/a	Final design completed only 3 months earlier.
SRO Verify Clearance Day 975	Senior reactor operator verification of clearance boundaries.	Did not recognize that boundaries were inadequate for the job scope	The SRO would be expected to understand the importance of Cubicle 310 in the EDG's safety system.	Time pressure, as the project is behind schedule.
Review Board address Stop Work Order Day 997	Review board addresses stop work. Members include plant manager, QC, engineering, construction contractor, production planning, operations, and project management. Discussed lessons learned and durations	Did not detect the potential problem with Bus 3 Cubicle 310	The Bus 3 Cubicle 310 problem is not part of the review.	Focus on schedule delay. Note that the Cubicle 310 problem has not been previously identified as an issue so it is unlikely that it would emerge, particularly in the face of schedule delays.

Controller or Controlled Process	**Responsibility**	**Contribution**	**Process Flaws**	**Context**
	for work corrections and changes to work plans.			
Table Top Meeting to Address Stop Work Day 1,029	Table top meeting to address stop work with project manager, engineering, construction contractor, production planning, QC, and planning for remaining cubicle work, cubicle tie-in work, and load sequencer tie-in work. Discussed lessons learned and durations for work, corrections, and changes to work plans made.	Did not detect the potential problem with Bus 3 Cubicle 310	Reviewers did not review work order 360. It should be noted that, although the load sequencer tie-in is explicitly mentioned as a review goal, the work order containing the load sequencer breakers and fuses was not discussed.	Focus on schedule delay. Note that the Cubicle 310 problem has not been previously identified as an issue so it is unlikely that it would emerge, particularly in the face of schedule delays.
Review Board Issue Restart Work Authorization Day 1,031	Final review of project provides basis for restart work authorization. Approved by shift manager with concurrence from plant manager.	Did not detect the potential problem with Bus 3 Cubicle 318	The Bus 3 Cubicle 318 problem is not part of the review.	Focus on schedule delays.
SRO Authorizes Tags for Clearance Day 1,061	The SRO authorizes tags providing clearance boundaries, allowing work crews to proceed with their task in Cubicle 318.	Did not detect the potential problem with Bus 3 Cubicle 318	The SRO would be expected to understand the importance of Cubicle 318 in the safety system of the EDG.	Time pressure.
Construction General Foreman Gives Pre-Job Briefing Day 1,061	Foreman gives a pre-job briefing to subcontractor installation crew.	Did not discuss the problem of the drawer containing Fuse B318.	Foreman did not have the training to understand the details of the installation job.	Time pressure.
Project Manager Observed Opening of Cubicle 310	Project manager observed the work crew opening Cubicle 318.	Project manager did not watch how the crew responded to the situation, which had safety-	Unclear what the project manager’s mental model of the crew’s task was with respect to the drawer containing Fuse B318	Time pressure.

Controller or Controlled Process	**Responsibility**	**Contribution**	**Process Flaws**	**Context**
Day 1,061		critical implications.		
Terminal Event Autostart of EDG Day 1,061	The crew opened the drawer in Cubicle 301 containing Fuse B318 to allow the cable run.	Opening the drawer affected the load sequencer, which caused the EDG to autostart, resulting in a reactor shutdown.	The crew observed a sign warning not to open the drawer. However, they observed the number 318 on a list of fuses that had been tagged out. Unfortunately, that number referred to a fuse from a different cubicle. Thus, they thought they had been cleared.	The crew had successfully performed the same operation before, including opening the fuse drawer, and had not been informed that Cubicle 318 was different.

4.1.4 Identify Control Structure Flaws

This section provides an opportunity to look for systemic structural flaws that might occur across the SCS, reflecting interactions among components. Leveson (2019) provides the following suggested categories: communication and coordination, safety information systems, changes, and dynamics over time in the system, environment, organizational climate, and economic and environmental factors.

As indicated previously, coordination was a particular issue in this case study. Therefore, we will use the conceptual framework for coordination proposed by Johnson (2017). As seen in Figure 19, there are three major sets of conditions and nine coordination elements that we will use to discuss the observed interactions that hampered coordination:

- Coordination Components
    - Goals: There was a long gap between the initial approval of the Byron Modification Project and activity. The NRC’s time requirements for completing this activity seems to have imparted a degree of time pressure. For example, the project was planned to be completed in one outage period whereas other NPPs were able to utilize two outage periods.
    - Strategy Activities: The unique role of Cubicle 318 in the plant’s safety structure does not seem to have been addressed, despite the explicit mention of load-balancing in the project objectives. There were two aspects of this failure: the actual triggering event—an autostart of the EDG—(System Hazard 1.2: Work on Safety-Related Power Sources) and danger to workers exposed to dangerous voltage levels (System Hazard 4.1: Unexpected Energized Equipment). System hazards are described in detail in Table 4.1 of Section 4.1.1.1.
    - Decision Systems: Figure 19 depicts the generic pattern of relationships among decision systems characterizing this case. This figure is Part C of Figure 19, which depicts Johnson’s conception of fundamental coordination relationships. Thus, this case involved multiple decision systems—each with its own process—which needed to be coordinated to achieve a single final outcome.

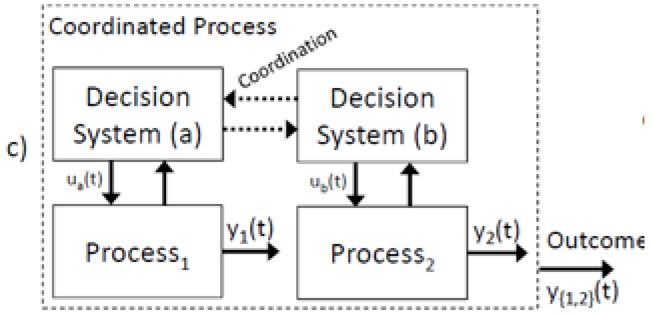

Figure 19. Generic fundamental coordination relationship applicable to the present case (Johnson 2017, Figure 12; Used by permission of author).

- Enabling Processes
  - Communications: The risk associated with Cubicle 318 did not appear to be communicated among the several decision systems involved.
  - Group Decision-Making: As seen in the control structure, there were numerous independent opportunities for calling attention to the hazards defined above. It seems as if a diffusion of responsibility had taken place where each decision maker assumed that someone else would take charge.
  - Observation of Common Objects: The central role of Cubicle 318 in the plant's safety structure was missed by individuals, such as the plant manager, shift manager, and SRO, who would be expected to be sensitive to such issues.
- Enabling Conditions
  - Authority, Responsibility, Accountability: See the comment above regarding the diffusion of responsibility.
  - Common Understanding: See the comment above regarding the observation of common objects.
  - Predictability: There were assumptions that craft workers, with a limited understanding of the overall project goals, could proceed with supervision by individuals from a different organization without detailed operational knowledge of the task.

One of the main issues in the current use case is that no one treated the one cubicle as special—not the modification workers, maintenance planners, or operations. This is one of the major contributing factors to the event. Each of the processes discussed in the control structure (Figure 15) was a missed opportunity to set that special cubicle aside and put in additional precautions. It should be noted that the people doing the modification would, with the exception of the walkdowns, likely be working offsite. It is likely that the drawings they were using depicted the load sequencer equipment, but this would not be considered a problem because the work was going to be offline and it is not the responsibility of the modification engineer to worry about what happens if a maintenance worker opens a drawer that has nothing to do with the equipment being modified.

Regular plant maintenance personnel (not contractors) would have probably observed the warning sign and not opened the drawer without talking to their supervisor. Thus, if they were doing the work, the event most likely would not have happened.

Operations would most likely be the only group that could have known about the risk to the plant by opening the drawer; however, they were also hyper focused on the modification work and not the load sequencer equipment because it had nothing to do with the modification.

Operations should have noted that this cubicle was unique and been concerned about adding additional barriers "just in case" someone came in contact with the other circuitry in the cubicle. This should have been the case even when the work was not expected to be performed with the plant online. Personnel safety should have driven this decision if not for any other reason, yet all independent reviews failed to even raise the issue.

4.2 Organizational System Modeling

Organizational system modeling is underway to provide a plantwide perspective on organizational communications, processes, and documentation. CAST analyses, such as that described above, are generally limited to examining organizational systems to the extent that they exert influence on the particular incident under examination. This fully supports their use in incident investigations and related control structure analysis. STPAs map a broader array of organizational (and technical) entities but typically do not attempt to model entire communication networks.

Therefore, to supplement CAST and STPA processes and provide a more complete model of our industry partner's ICS across a variety of contexts, we initiated an effort to model organizational communications, processes, and documentation as an ICS. Specifically, we were interested in mapping communication control and feedback relationships both across and within organizational levels of the company, regulators, and plant.

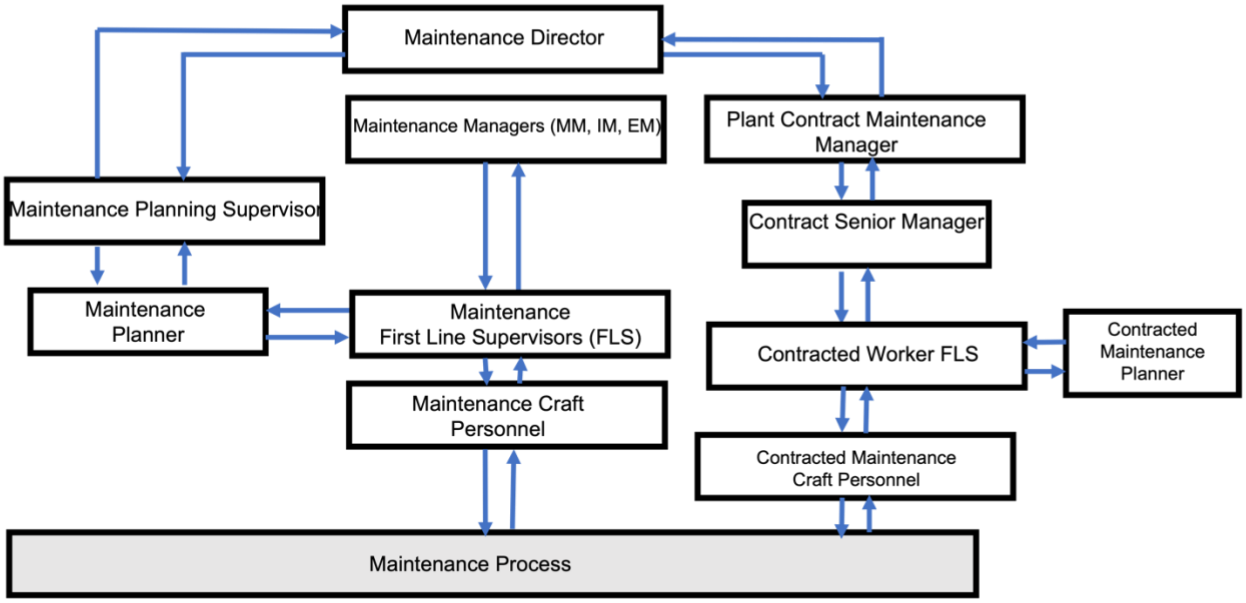
Maintenance Director
Maintenance Managers (MM, IM, EM)
Plant Contract Maintenance Manager
Maintenance Planning Supervisor
Contract Senior Manager
Maintenance Planner
Maintenance First Line Supervisors (FLS)
Contracted Worker FLS
Contracted Maintenance Planner
Maintenance Craft Personnel
Contracted Maintenance Craft Personnel
Maintenance Process

Figure 20. Organizational system model of the maintenance communication process.

Figure 20 illustrates an example of the organizational system modeling conducted to date, specifically with respect to communication control and feedback relationships related to maintenance activities of the sort exemplified by the current use case. While these models are still under development, it is interesting to note that Figure 20 illustrates a situation in which the use of contracted maintenance (as was the case in the current analysis) introduces a number of potentially problematic alterations to the ICS when compared to using experienced plant workers. Specifically, additional layers of management come into play whenever contracted labor is used, introducing a potential diffusion of responsibility and confusion with respect to the responsibility for worker and system safety. Additionally, there is typically little to no communication between contracted and full-time maintenance personnel, depriving the former of the expertise possessed by the latter.

OSM activities will continue over the remainder of the fiscal year to specify the nature of organizational interconnections more fully as they impact communication effectiveness and, ultimately, plant safety. These analyses will support STPA modeling by providing details of relevant organizational control structures and PIR and IAE model development by modeling the full breadth of organizational communications, processes, and documentation required for optimized information automation.

4.3 Preliminary Human-System Design Requirements and Safety Constraints

As a result of the current work, and although there are further analyses to complete (see Section 5.5), we feel that we can initiate developing preliminary system-level requirements and safety constraints for a revised, near-term design and operational approach related to the current use case as well as that examined by Dainoff et al. (2022). With a subsequent STPA, these system-level requirements will evolve to include issues associated with both near and long term (i.e., IAE development) information automation system design and optimization. Stated simply, at the system level, it is critical know what information needs to be delivered to whom, when, and in what form. Similarly, it is important to specify system safety constraints (i.e., what the information automation must not do and what it must prevent from happening). While much valuable information will be derived from the remaining analyses to support software and human-system interface development, these will be the focus of more detailed requirements definition than occurs at the system level.

Table 5 presents a set of preliminary system-level requirements for an optimized information automation system. Table 6 presents a set of preliminary system-level safety constraints for the same system.

Table 5. Preliminary system-level requirements.

1	The system shall detect and process data specific to anomalous conditions in power plant components and subsystems in near real time without a loss of information accuracy.
2	The system shall route information about anomalous conditions to appropriate[a] plant personnel as soon as possible.
3	The system shall provide appropriate plant personnel with suggested actions for addressing the anomalous conditions.
4	The system shall track the status of open actions related to the anomalous conditions.
5	The system shall notify appropriate plant personnel about the status of open actions related to the anomalous conditions.
6	The system shall provide an intuitive and easily usable human-system interface for information display, retrieval, and submission.
7	The system shall track all plant operational, maintenance, design, and outage schedules and processes, including (but not limited to) information such as objectives, start and stop dates, current status, dependencies on other schedules and processes, action status, etc.
8	The system shall detect change in plant operational, maintenance, design and outage schedules, and processes related to the anomalous conditions.
9	The system shall detect all plant schedule and process changes, determine the impact on related schedules and processes and the likelihood of resulting safety or performance risks, and inform appropriate plant personnel.

Table 6. Preliminary system-level safety constraints for PIR system.

1	The system shall not alert on anomalous signals or conditions until appropriate signal thresholds are met.
2	The system shall not provide excessive or extraneous information to users.
3	The system shall not require sustained, excessive cognitive or physical workload on the part of the user.

[a] Defined as those with a need to know to avoid a diffusion of responsibility, noise in the system, etc.

Further development of system-level requirements and safety constraints will take place over the remainder of the research effort. Progress on this aspect of the work will be heavily reliant on access to technical expertise related to MIRACLE and DWEP, as well as NPP subject matter expertise from our industry partner. A multidisciplinary approach to the requirements definition is an efficient way to arrive at requirements to jointly optimize the technology and its impact on human performance.

5. DISCUSSION

The primary purpose of the research described in this report is to support the promotion of safety and cost-efficiency in NPP design and operation. The current work was based on a prior, initial application of CAST to a representative NPP use case (Dainoff et al., 2022). In this report, we have expanded the CAST method used in the prior analysis to include models of process coordination based on STAMP and sociotechnical systems theory in general.

5.1 Summary of Findings

This section provides of summary of interim findings with regard to each of the three major objectives described in Section 2 and examines the findings in light of resilience theory (e.g., Woods, 2015) and their implications for designing information automation systems. The relevance of the findings for developing the PIR and IAE models is also provided, along with a discussion of the research planned for the remainder of the current effort.

5.1.1 Objective 1: Apply Sociotechnical Systems Analysis Methods to Industry Use Cases

To date, we have conducted a CAST analysis on an industry use case involving the accidental activation of an EDG. This use case was suggested by a nuclear utility partner who supplied some of the documentation used in the analysis. Over the remainder of the fiscal year, we will conduct an STPA, a sociotechnical analysis method useful in complex system design as opposed to CAST's application for accident analyses.

A major finding of the CAST analysis involves the problematic matter of plant schedule and process coordination. Given the inherent complexity of an NPP and the fact that multiple activities are ongoing at any given point in time, it is hardly surprising that schedules and processes can sometimes transition from a coordinated state to a less functional, uncoordinated state. The CAST analysis demonstrated that the loss of schedule and process coordination was a major contributor to the EDG incident and suggests that this is likely to remain a general concern until means are developed for the real-time identification that factors negatively impacting coordination exist and could have an increased possibility of error.

A prior CAST analysis examined a detailed root cause analysis of a scram incident related to a new digital instrumentation and control system, the digital electrohydraulic controller. Conflicting mental models regarding process activities and their status was revealed as a causal element in this event. Additionally, the digital electrohydraulic controller and EDG events shared a number of common themes. First, time pressure played an important role in both events, and the pressure and error precursors inherent with an increased time pressure to meet a deadline were a factor. Second, there appeared to be an overreliance on contracted work (i.e., maintenance support) to help each of the two organizations meet a deadline. Third, the consequences of poor performance in each case included a greatly increased regulatory presence at the respective plants, begging the question of why critical maintenance evolutions were entrusted to contracted work.

Over the remainder of the fiscal year, we will supplement these findings with results from an STPA of a generalized set of similar use cases. The utility of STPA for design lies in its ability to analyze existing and proposed systems to identify sociotechnical and system performance risks. Our intent is to identify these risks in current control structures, to better understand the dynamic nature of control structures (their tendency to strengthen or weaken in response to conditions), and to further develop the control structures underlying the PIR and IAE models.

5.1.2 Objective 2: Develop a Preliminary System-Theoretic Model of Information Automation

As part of this effort, we developed two preliminary information automation models. The PIR model supports the near-term development of an information automation utility for proactive issue resolution, while the IAE model supports the development of the broader information automation ecosystem. Each model has been developed to the point where additional expertise related to enabling technologies (i.e., MIRACLE and DWEP) and operational demands (i.e., nuclear industry SMEs) is required for further maturation.

5.1.3 Objective 3: Develop Preliminary Requirements for Human-System Interface Software and Display Design

In order to provide useful support to system design efforts, it is important to translate findings such as those from the current work and from related, relevant human-systems performance research into specific requirements. We have initiated this process with an initial, preliminary set of system-level requirements and safety constraints focused primarily on those design aspects with most direct relevance for human performance.

Requirements development will continue throughout the remainder of the effort to provide a more complete set of system-level requirements and safety constraints. Specifying requirements for human-system interfaces associated with the PIR and IAE models will be an area of principal interest.

5.2 Process Coordination

In complex systems, such as those within NPPs, process coordination is an essential component of operational effectiveness. However, while coordination is an implicit and explicit requirement of such systems, the specific mechanism for accomplishing and enhancing coordination are rarely provided or specified. This is particularly the case under time pressure. Johnson (2017) has pointed out that coordination failures are a frequent contributing component of accident analysis during CAST.

It is frequently observed in organizations that, when there is an urgent timeline, standard procedures are bypassed. In some cases, there is a rational basis for doing so. For example, during the Cuban Missile Crisis, warships had supplies of training ammunition for larger caliber guns. This ammunition was expensive, and during normal training operations, detailed operational experience procedures were required to document the firing of each round. However, during the crisis, it was necessary to quickly remove training ammunition to allow live ammunition to replace it. The fastest way to accomplish this was to simply fire all of the training ammunition. During this process, the documentation requirement was appropriately suspended (Dainoff, personal experience).

However, in many other situations, safety barriers are bypassed under a time pressure. This was the finding of the case study examined in this report. The phenomenon of “work to rule” is a fundamental demonstration of this problem. If operating procedures are so complicated that normal work would be slowed down by complying with every procedure, there must be an issue with the procedures. In reality, organizations count on the tacit (tribal) knowledge of operators who know which procedures to follow, and which can be bypassed.

The information automation approaches discussed in this report provide potential solutions for this problem. An information display that allows relevant operators to visualize the system—as provided by an ecological interface display—would give an operator the confidence that a given procedure could be safely bypassed without threat to the system’s integrity. Underlying this display philosophy is the intent specification approach by Leveson (2020). That is, each safety-critical procedure should, in principle, be transparently linked to a specific potential system hazard and the safety constraint that mitigates that hazard. These should be identifiable with the system control structure. See Section 5.4 for further elaboration.

5.3 Resilience in Scheduling and Process Coordination

Resilience, as applied to the design and operation of sociotechnical systems, refers to “the ability of a system to extend its capacity to adapt when surprise events challenge its boundaries” (Woods, 2015, p.4), where boundaries refer to the limits of safe, effective, and economically viable operations. It is the opposite of system brittleness, defined as “a rapid fall off or collapse of performance that occurs when events push a system beyond its boundaries for handling changing disturbances and variations” (Woods, 2016, p.1).

One of the more influential approaches to resilience is the stress-strain model. Proposed by Woods and Wreathall (2006), it models sociotechnical system resilience and brittleness by employing a metaphor borrowed from materials science in which stress is equated with the varying loads placed on a system and strain is equated with how the system stretches in response (Woods and Wreathall, 2016). As stress on a sociotechnical system increases, the subsequent strain can be evenly distributed across the system, according to the type and level of strain the system is designed and positioned to accommodate (see Figure 21). As the level of stress increases beyond the system design basis, the system continues to strain to accommodate, perhaps successfully for a while, until weaknesses, disruptions, failures, etc. begin to appear. System performance and its ability to further adapt can fall off dramatically at that point.

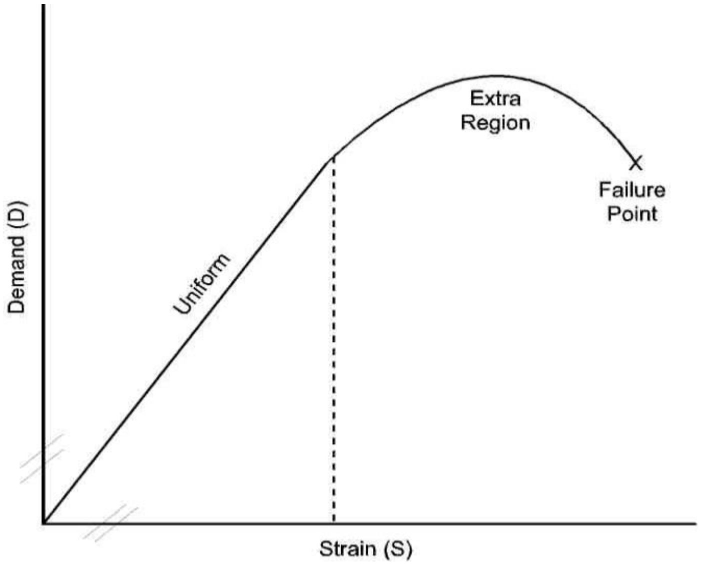

Figure 21. Stress-strain model of resilience (taken from Woods and Wreathall, 2016).

Within the context of the current CAST analysis, the sociotechnical system supporting the planning and execution of maintenance work exhibited signs of brittleness with respect to its ability to adjust to complications caused by design and work schedule changes. It is likely that other, similar disruptions—such as changes in the nature and scope of maintenance activities—will result in similar negative impacts if not adequately addressed.

Resilience issues have already drawn the attention of enterprise information system designers and researchers (e.g., Liu et al., 2010; Zhang and Lin, 2010). While a good deal of this work deals with resilience against cyberattacks, the concept applies equally to understanding and addressing situations in which system brittleness is more directly a function of design shortcomings than an external attack.

STPAs over the remainder of the summer should provide further information regarding PIR and IAE system resilience requirements.

5.4 Implications of Findings for Proactive Issue Resolution Model Development

There are many sources of data captured on a daily basis at NPPs. Previously, we were mainly limited to only using CAP data for analyses that would uncover organizational or programmatic issues. The plant would have to realize a significant event in order to be able to perform a good CAST analysis, because the amount of organizational and programmatic information needed to perform a good CAST analysis was only present in more complex investigations, such as the EDG event analyzed in this report. The only other viable option was performing an intrusive deep dive looking for areas of weakness to evaluate, which is both costly and time consuming and would only be performed if senior leadership felt that plant performance was declining significantly.

However, through collaborating with other INL research projects, we have learned that we can now analyze more data than ever before. These new abilities will help the team proactively identify and, using STPAs, evaluate control structures for weaknesses. Then, \information automation and MIRACLE will enable us to seek out the signals indicative of potentially negative impacts resulting from these weak control structures at a much lower consequence level, allowing us to either make recommendations to the plant on how to strengthen the suspect control structure or to use the DWEP to "solicit" additional information during related evolutions, so that we can validate whether our analysis is accurate, which will then result in more effective corrective actions.

5.5 Next Steps

This report has provided a description of our work to support developing an optimized information automation system. The CAST analyses have provided sufficient insight into challenges associated with existing systems to begin developing system-level requirements and safety constraints. Over the remainder of our current effort, we will focus on shifting from analyzing existing systems toward designing a potential optimized design.

5.5.1 System-Theoretic Process Analysis and Organizational System Modeling Analyses

STPAs and OSMs over the remainder of the fiscal year will support further developing the PIR and IAE models. Specifically, we will conduct an STPA on the communications process underlying a general class of activities, such as maintenance activities in general or responses to equipment failures. With a broader scope than CAST, an STPA will support identifying other potential weaknesses in current ICSs and opportunities for improvement and the potential introduction of automation and AI.

An OSM will support the STPA by modeling the organizational communications, processes, and documentation associated with the class of events under examination. It will also support developing the PIR and IAE models, as both involve numerous organizational entities whose communication-based processes will rely on close coordination in an optimized system.

5.5.2 Maturation of Proactive Issue Resolution and Information Automation Ecosystem Models

The STPAs, OSMs, and modeling efforts described above support the further development and maturation of the PIR and IAE models. Specifically, our intent is to further specify the major components of each model and the interactions between them in conjunction with MIRACLE and DWEP technical expertise and industry partner subject matter expertise. The end-of-year objective is to provide as complete a set of system-level requirements and safety constraints as possible. This will support follow-on efforts to develop more detailed requirements and prototyping of key system features such as the human-system interface.

At this point, it is particularly important to involve MIRACLE and DWEP technical expertise to a much greater extent. Their input is required to refine the design of the PIR and IAE models and to ensure that system design and implementation issues relevant to their systems are raised as part of analysis and modeling. Both technologies are key enablers of the systems under consideration, and as the team's work proceeds toward requirements and design, it will be increasingly important to understand their capabilities and limitations.

We propose accomplishing this by involving MIRACLE and DWEP technical experts in our analysis and design activities, particularly those involving industry partner SMEs. A multidisciplinary perspective in these types of knowledge acquisition processes is an important aspect of user-centered design.

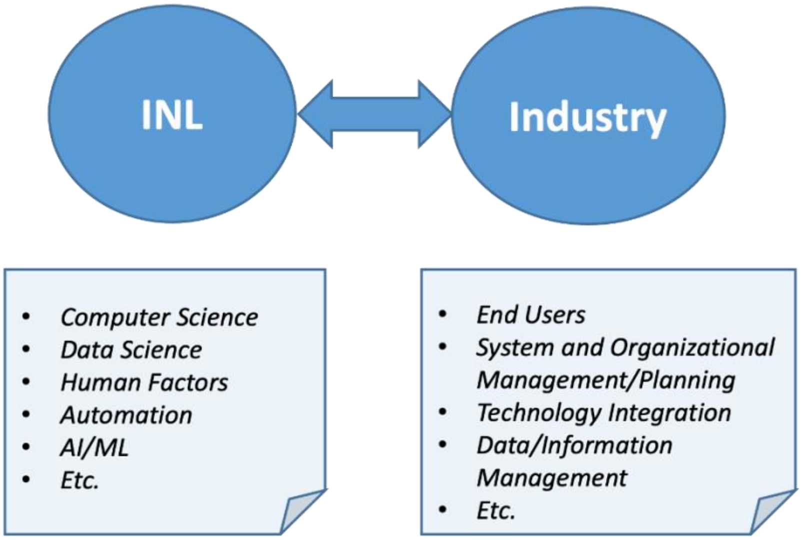

Figure 22. Elements of a multidisciplinary, user-centered design.

Figure 22 illustrates the nature of the recommended collaboration between INL and industry. INL possesses significant expertise in system analysis and design related to technical and HSI aspects of the system, while industry possesses the operational and experiential expertise required to ensure the design's relevance and usability. A multidisciplinary team approach to designing complex sociotechnical systems is significantly more efficient and effective than traditional stovepiped approaches (e.g., Booher, 2003; Tate et al., 2005). It is more efficient in the sense that design stakeholders (users, developers, etc.) maintain a continuous presence in the design and implementation presence. Simultaneous information transmission, decision-making regarding the system's design, etc. helps to eliminate long feedback loops between organizational components. It is more effective in the sense that multidisciplinary discussions of system design and implementation issues are far more likely to result in synthetic, cross-disciplinary approaches.

5.5.3 Process Transportability

Our objective with respect to process transportability is to provide the nuclear industry with intuitive, easily understood, and readily usable tools and techniques for assessing sociotechnical issues of the type discussed above in existing or planned systems. These tools must be designed to minimize demands on training and should be usable by personnel of varying qualification and experience levels.

For example, two of the authors (LH and MD) have worked with the trucking and rail industries, instructing workers on developing simplified SCSs. While simply generating a control structure is not the same as conducting a full STPA or CAST analysis, it has nevertheless revealed significant organizational communication, control, and feedback issues. It should certainly be possible to do the same for nuclear industry personnel and regulators.

To this end we will pursue a parallel focus on developing transportable tools and techniques in conjunction with STPA and OSM analyses.

6. CONCLUSIONS AND RECOMMENDATIONS

The following sections describe interim conclusions and recommendations, including a discussion of the implications of the current findings for nuclear modernization and a summary of preliminary system-level requirements and system safety constraints. Of primary interest are the implications of the findings for optimizing the design and implementation of information automation systems.

6.1 Information Automation System Design and Optimization

At this stage of the research process, we have identified a number of preliminary system-level design requirements and safety constraints for an optimized information automation system. We expect the current lists to significantly expand over the remainder of the effort, particularly as a result of our interactions with technical experts and nuclear industry SMEs. In summary, we conclude the following:

- The system must be able to reliably relay useful, situation-specific, and actionable information to users, possibly on a need-to-know basis, to avoid potential confusion and diffusion of responsibility and clearly specify possible actions and their results.
- While an AI system could potentially suggest or assign actions based on the above information, until that technical capability has been developed and demonstrated to be useful, we suggest the user continue to assign actions. However, to maintain coordinated schedules and processes, it is important that the system have the ability to track actions and assess their effectiveness once completed.
- System resilience with respect to schedule and process disruptions is essential. The results of the current CAST analysis, as well as the analysis performed by Dainoff et al. (2022), clearly demonstrate the potentially disruptive effects of time pressure and schedule and process changes. Therefore, an optimized IAE system must have the means to detect such an occurrence, notify appropriate users of the issue, identify the locus of the issue, and suggest potential solutions.

Having conducted a CAST analysis of the accidental EDG activation use case, our first priority over the remainder of this effort will be to conduct a corresponding STPA. Since STPA is a system design tool, whereas CAST is an accident analysis tool, we have decided to broaden the scope of its analysis beyond the specifics of the EDG use case to include similar types of potential incidents. This will enable the development of a more generalized control structure model and therefore be a step toward the development of a generalized IAE model.

Generalizing the model from the PIR to IAE use cases will require a much broader and more detailed understanding of organizational structure and processes. This is the purpose of the OSM, the results of which will also support the development of a corresponding, plantwide ICS.

6.2 System Performance and Safety

In industry Institute of Nuclear Power Operations (INPO) Industry Reporting and Information System (IRIS) data, there are many issues and events reported by most U.S. nuclear plants. There are factors that tie all nuclear plants together, such as common regulations and regulators, including the NRC and INPO. Based on our research so far, we have seen some common themes that appear to impact the performance of unrelated plants from different utilities. Reviewing events from one utility and comparing them to others from different plants as well as reviewing all events reported to the NRC and through the INPO IRIS process starts to validate that there are common sociotechnical design issue flaws impacting plants. This brings about a couple questions: Are current nuclear regulatory enforcement methods inadvertently causing utilities to design sociotechnical flaws into their plants' highest level SCSs? Did utilities respond by creating highly cumbersome performance improvement programs to ensure regulatory compliance would be met?

With the advances in information automation, and with this new proactive information automation model, we feel that both the regulators and nuclear plants can utilize this process to both improve the resilience of SCSs and reduce compliance costs, helping to simultaneously improve safety margin and performance.

6.3 Implications of Findings for Nuclear Modernization

As described in the introduction to this report, the goals of the current research program are to improve nuclear safety and reduce costs through the proactive and real-time correction of technical, organizational, and programmatic factors that are precursors to human- and equipment-related events. By initiating a set of analyses of recent events from several U.S. nuclear utilities, the research reported herein supports the following nuclear modernization objectives:

- CAST findings have identified and described sociotechnical factors involved in an EDG activation event. More importantly, as described in Section 4.1, in doing so it has identified weak linkages between organizational system components, primarily with respect to process and decision-making coordination. Identifying systemic issues of this sort can support near-term modernization efforts by illuminating areas of weakness in the current system.

- The reassignment of the work from being conducted during an outage period to being conducted while the plant was online resulted in a number of issues that were related to a disruption in the coordination of processes involved. Clearly, one characteristic of an optimized, future information automation system will be resilience. Resilience in enterprise information systems is currently a R&D topic (e.g., Liu et al., 2010; Zhang and Lin, 2010) to develop information systems that can dynamically realign in response to changing conditions and context.

These findings and, we anticipate, those from upcoming STPA and OSM analyses will directly support nuclear modernization by providing the foundational components of any future information automation system. Specifically, the nature of the interactions between components of complex sociotechnical systems, particularly those considering the introduction of new technologies, such as automation and AI, is critical for development and implementation. Furthermore, the development of specific utilities, such as PIR or the more general IAE, relies on a clear understanding of the needs, capabilities, and limitations of the end user. A sociotechnical approach of the type illustrated in the current work can support the accomplishment of numerous design objectives, including the joint optimization of people, technology, process, and governance.

7. REFERENCES

Alcover, C., Guglielmi, D., Depolo, M., and Mazzeti, G. 2021. "Aging and tech job vulnerability: A proposed framework on the dual impact of aging and AI, robotics and automation among older workers." Organizational Psychology Review 11(2): 175–201. https://doi.org/10.1177/2041386621992105.

Bennett, K. and Flach, J. 2011. *Display and Interface Design*. Boca Raton, FL: CRC Press. https://doi.org/10.1201/b10774.

Booher, H. 2003. *Handbook of Human Systems Integration*. New York City, NY: Wiley. https://doi.org/10.1002/0471721174.

Butts, C.T., Petrescu-Prahova, M., and Cross, B. 2007. "Responder communication networks in the World Trade Center disaster: Implications for modeling of communication within emergency settings." The Journal of Mathematical Sociology 31(2): 121–147. https://doi.org/10.1080/00222500601188056.

Checkland, P. 1981. *Systems Thinking, Systems Practice*. New York City, NY: John Wiley and Sons.

Dainoff, M., Hettinger, L., Hanes, L., and Joe. J. 2020. "Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology." INL/EXT-20-57908, Idaho National Laboratory. https://doi.org/10.2172/1615671.

Dainoff, M., Hettinger, L., Hanes, L., and Joe, J. 2021. "Addressing Human and Organizational Factors in Nuclear Industry Modernization: A Sociotechnically-Based Strategic Framework." Proceedings of the 12th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2021), 162-170, (virtual) Providence, RI. https://doi.org/10.1080/00295450.2022.2138065.

Dainoff, M., Hettinger, L, and Joe, J. 2022. "Using Information Automation and Human Technology Integration to Implement Integrated Operations for Nuclear." INL/RPT-22-68076, Idaho National Laboratory. https://doi.org/10.2172/1879683.

Dainoff, M. Murray, P., Joe, J., Hall, A., Oxstrand, J., Hettinger., L., Yamani, Y., and Primer, C. 2022. "Using Systems Theoretic Process Analysis and Causal Analysis to Map and Manage Organizational Information to Enable Digitalization and Information Automation." INL/RPT-22-69058, Idaho National Laboratory. https://doi.org/10.2172/1894897.

Hettinger, L., Kirlik, A., Goh, Y. and Buckle, P. 2015. "Modeling and simulation of complex sociotechnical systems: Envisioning and analysing work environments." Ergonomics 58(4): 600–614. https://doi.org/10.1080/00140139.2015.1008586.

Hettinger, L., Dainoff, M., Hanes, L., and Joe, J. 2020. "Guidance on Including Social, Organizational, and Technical Influences in Nuclear Utility and Plant Modernization Plans." INL/EXT-20-60264, Idaho National Laboratory. https://doi.org/10.2172/1696804.

Hoff, K. A., & Bashir, M. 2015. "Trust in automation: Integrating empirical evidence on factors that influence trust." Human Factors 57(3): 407–434. https://doi.org/10.1177/0018720814547570.

Hunton, P., England, R., Lawrie, S., Kerrigan, M., Niedermuller, J., and Jessup, W. 2020. "Business case analysis for digital safety-related instrumentation & control system modernizations." INL/EXT-20-59371, Idaho National Laboratory. https://doi.org/10.2172/1660976.

Johnson, K. 2017. *Extending Systems-Theoretic Safety Analyses for Coordination*. MIT PhD Dissertation.

Kovesdi, C., Mohon, J., Thomas, K., Remer, J., Joe, J., Hanes, L., Dainoff, M, and Hettinger, L. 2021. "Nuclear Work Function Innovation Tool Set Development for Performance Improvement and Human Systems Integration." INL/EXT-21-64428, Idaho National Laboratory.

Kuehn, E. F. 2023. "The information ecosystem concept in information literacy: A theoretical approach and definition." Journal of the Association for Information Science and Technology 74(4): 434–443. https://doi.org/10.1002/asi.24733.

Larsson, S., & Heintz, F. 2020. "Transparency in artificial intelligence." Internet Policy Review 9(2). DOI: 10.14763/2020.2.1469

Leveson, N. 2011. *Engineering a Safer World*. Cambridge, MA: MIT Press.

Leveson, N. 2019. "CAST Handbook: How to Learn More from Incidents and Accidents." http://psas.scripts.mit.edu/home/get_file4.php?name=CAST_handbook.pdf

Leveson, N. 2020. "An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture." http://sunnyday.mit.edu/

Leveson, L., Malmquist, S., and Wong, L. 2020. "CAST Tutorial: How to Learn More from Accidents." http://psas.scripts.mit.edu/home/wp-content/uploads/2020/07/Leveson-CAST-Tutorial.pdf

Leveson, N. and Thomas, J. 2018. "STPA Handbook." http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.

Liu, D., Deters, R., and Zhang, W. 2010. "Architectural design for resilience." Enterprise Information Systems 4(2): 137–152. https://doi.org/10.1080/17517570903067751.

Martinez-Moyano, I. J., & Richardson, G. P. 2013. "Best practices in system dynamics modeling." System Dynamics Review 29(2): 102–123. https://doi.org/10.1002/sdr.1495.

Quintana, V., Howells, R.A., and Hettinger L. 2007. "User-centered design in a large-scale naval ship design program: Usability testing of complex military systems – DDG 1000." Naval Engineering Journal, 1, 25-33. https://doi.org/10.1111/j.0028-1425.2007.00001.x.

Rasmussen, J., Pejtersen, A., and Goodstein, L. 1994. *Cognitive Systems Engineering*. New York City, NY: Wiley.

Rouse, W. 2010. *The economics of human system integration.* Hoboken, NJ: Wiley. http://doi.org/10.1002/9780470642627.

Silvis-Cividjian, N. 2022. "Using Stamp-CAST to Analyze an Incident in Radiation Therapy." http://psas.scripts.mit.edu/home/wp-content/uploads/2022/2022-06-07-1130__Natalia%20Silvis-Cividjian__PUB.pdf.

Tate, C., Estes, T., and Hettinger, L. 2005. "Lessons learned from integrating user-centered design into a large-scale defense procurement." Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49. https://doi.org/10.1177/154193120504902309.

Thomas, K. and Hunton, P. 2019. "Nuclear Power Plant Modernization Strategy and Action Plan." INL/EXT-19-55852, Idaho National Laboratory.

von Bertalanffy, L. 1968. *General Systems Theory: Foundations, Development and Applications*. New York: G. Braziler.

Wahlstrom, B. 2004. "Challenges in the Nuclear Industry: Perspectives from Senior Managers and Safety Experts." In N. Itoigawa, B. Wilpert & B. Fahlbruch. (Eds.), *Emerging demands for the safety of nuclear power operations* (pp.1729). Boca Raton, FL: CRC Press.

Whitworth, B. 2009. "A brief introduction to sociotechnical systems." In *Encyclopedia of Information Science and Technology*, 394–400, IGI Global. https://doi.org/10.4018/978-1-60566-026-4.

Wilson, J.R. 2014. "Principles of system ergonomics/human factors." *Applied Ergonomics* 45: 5–13. https://doi.org/10.1016/j.apergo.2013.03.021.

Woods, D.D. 2015. "Four Concepts for Resilience and their Implications for Systems Safety in the Face of Complexity." Reliability Engineering and System Safety 141: 5–9. https://doi.org/10.1016/j.ress.2015.03.018.

Woods, D. 2016. "Resilience as graceful extensibility to overcome brittleness, IRGC Resource Guide on Resilience, EPFL International Risk Governance Center." https://irgc.org/wp-content/uploads/2018/09/Woods-Resilience-as-Graceful-Extensibility-to-Overcome-Brittleness.

Woods, D., and Hollnagel, E. 2006. *Resilience Engineering: Concepts and Precepts*, Boca Raton, FL: CRC Press. https://doi.org/10.1201/9781315605685.

Woods, D.D., & Wreathall, J. 2003. *Managing Risk Proactively: The Emergence of Resilience Engineering*. Columbus, OH: Ohio State University.

Zhang, W. and Lin, Y. 2010. "On the principle of design of resilient systems: Application to enterprise information systems." Enterprise Information Systems 4(2): 99–110. https://doi.org/10.1080/17517571003763380.

APPENDIX A
Draft Research Summary Article

Title: Optimizing Information Automation: A Human-Systems Integration Perspective

Subtitle: A summary of INL Report INL/RPT 23-73099

Report Content Overview

Much of the nuclear industry is currently focused on modernizing plant systems, including the potential introduction of advanced automation, artificial intelligence (AI), and other emerging technologies. The introduction of novel technologies will change the nature of much of the work currently conducted at nuclear plants. Effectively integrating new technical systems with the user community is key to ensuring their effectiveness once deployed. In this report, we describe progress on a program of research focused on providing the industry with tools and techniques to support effective modernization from an human-systems integration point of view, specifically with regard to information automation.

- *In a few impactful words (for technical audience), summarize the current problem and context.*
  - **Designing Information Automation Systems**
    - Information automation provides users with intuitive, actionable information based on continuous measurements of plant performance.
    - How can we most effectively implement automation and AI-based tools to support human performance and, by extension, system performance?
- *In a few impactful words summarize the solution developed by this research.*
  - **Proactive Issue Resolution Model**
    - Incorporates automation and AI to provide users with information regarding precursors of incidents, impending equipment failures, etc.
    - Incorporates a dynamic sociotechnical systems model to identify emerging safety control structure weaknesses.
    - Is projected for near-term application.
  - **Information Automation Ecosystem Model**
    - Models plantwide sociotechnical system components and their interactions to provide enterprise wide information automation.
    - Uses PIR model development as a test case for broader information automation ecosystem development.
    - Projected for intermediate-term application.
- *In a few impactful words summarize the impact on the sector, stakeholders, etc. You can also describe demonstration projects or collaborations with external stakeholders.*
  - **Implementing an effective proactive issue resolution model will enhance plant safety and result in improved distribution of operating and maintenance (O&M) costs.**
    - This project will reduce the magnitude and number of significant events to improve plant safety and performance. Even a modest reduction in significant events will result in a large return on investment, because gains in regulatory margin will reduce the plant O&M costs associated with regulatory compliance and improvements in plant performance will reduce the O&M costs associated with recovery from events and, in some cases, replacement generation. Figure 23 demonstrates O&M costs before and after the proactive issue resolution model implementation.

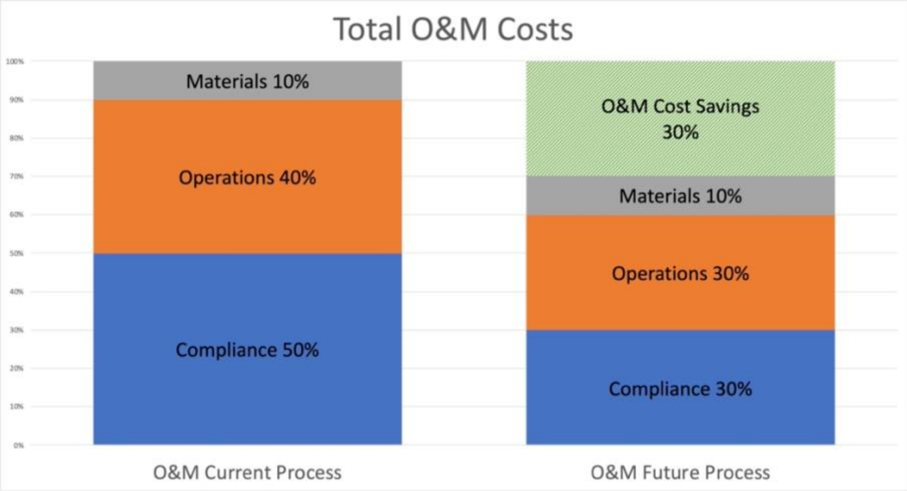

Figure 23. Projected impact of effective proactive issue identification and resolution on total O&M costs.

- The reduction in significant events will be accomplished using control structure mapping and information automation that screens and subsequently feeds numerous sources of plant information into Idaho National Laboratory’s Machine Intelligence for Review and Analysis of Condition Logs and Entries to recognize indications of degrading performance and negative variances from accepted control structures at a much lower level of consequence. Once these emerging issues are validated through some additional analysis, the adverse condition is documented and reported to the organization so that they can take corrective measures to strengthen the control structures without having to realize a significant event. Corrective actions are seamlessly integrated into daily work activities at all levels of the organization and continuously assessed for effectiveness until no more signs of the performance deficiency are intercepted.