INL/RPT-23-74217

Light Water Reactor Sustainability Program

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis: Tool Development and Method Evaluation

August 2023

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-23-74217

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis: Tool Development and Method Evaluation

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

August 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.lwrs.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Light Water Reactor Sustainability Program

This page intentionally left blank.

ABSTRACT

This report describes progress and findings for a program of research supporting the design and optimization of information automation systems for nuclear power plants (NPPs). Information automation is the customization and delivery of information for a work process, thereby providing users with intuitive, actionable information based on continuous measurements of plant performance. A prior report, Joe et al. (2023a), describes the initial efforts to develop tools and techniques based on a) systems-theoretic constructs underlying sociotechnical systems theory in general and the Systems-Theoretic Accident Modeling and Processes (STAMP) approach (Leveson, 2011) in particular, b) human systems integration principles, and c) artificial intelligence/machine learning/natural language processing-based technologies. This report is a continuation of that work and describes our efforts to evaluate the effectiveness of using STAMP to optimize information automation. This report also describes the development of an evaluation plan, our efforts to collaborate with industry partners, and presents the results obtained thus far from the evaluation.

Much of the domestic nuclear fleet is currently focused on modernizing technologies and processes, including transitioning toward digitalization in the control room and throughout the plant, along with a greater interest in the 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 early in the design process. This report describes modeling tools and techniques, based on sociotechnical systems theory, to support these design goals and their application in the current research effort. The report is primarily intended for senior nuclear energy stakeholders, including regulators, corporate management, and senior plant management.

Light Water Reactor Sustainability Program researchers have developed and employed a method to design an optimized information automation ecosystem (IAE) based on systems-theoretic constructs, sociotechnical systems theory, and STAMP. We argue that an IAE can be modeled as an interactive *information control system* whose behavior can be understood in terms of dynamic control, feedback, and communication relationships among the system's technical and organizational components. We have employed two STAMP-based tools in this effort. The first is Causal Analysis based on STAMP (CAST), an accident and incident analysis technique used to examine a performance- and safety-related incident at an industry partner's plant involving 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. The second tool is Systems-Theoretic Process Analysis (STPA), which is a proactive risk analysis tool used to examine existing and potential, planned sociotechnical systems. STPA was used to identify risk factors in the current design of a generic NPP preventive maintenance system. Our analyses focused on identifying near-term system improvements and longer-term design requirements for an optimized IAE system.

CAST analysis findings indicate an important underlying contributor to the incident under investigation, and a significant risk to information automation system performance, was perceived time and schedule pressures, 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 event. These findings are discussed in terms of their risk to overall system performance and their implications for information automation system resilience and brittleness. The STPA analysis produced a set of six system-level constraints and 27 system design requirements. These were identified through an analysis in which the control, feedback, and communication linkages between organizational components of a generic NPP preventive maintenance system were first identified and then analyzed for purposes of identifying ineffective control actions. These then served as the basis for an initial set of design requirements, a set that we expect to be modified as we refine and expand the STPA analysis in the next phases of the research effort. Finally, a simple inspection of the information control structure produced as part of the STPA revealed missing communication linkages between key system components that exist at the same levels of the preventive maintenance organizational hierarchy.

We also 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 and represents an end-state vision for our work. From our results, we have generated an initial set of preliminary system-level requirements and safety constraints for these models.

We have also focused on the early development of easy-to-learn, easy-to-use "transportable" tools for sociotechnical systems analyses. We intend these to be used by NPP personnel as a means of gaining reliable and relatively quick insight into (1) sociotechnical systems factors impacting incidents and accidents, (2) potential sociotechnical risk factors in existing or planned system designs, and (3) potential weaknesses in a system's safety and/or information control structure.

We conclude the report with a set of summary recommendations, a discussion of planned and potential follow-on research and development, and a draft list of system-level requirements and safety constraints for optimized information automation systems.

CONTENTS

FIGURES

TABLES

ACRONYMS

AI	artificial intelligence
CAP	corrective action program
CAST	Causal Analysis Based on STAMP
CE	contracting engineer
CWA	cognitive work analysis
DWEP	dynamic work execution platform
EDG	emergency diesel generator
EID	ecological interface design
HAT	human-autonomy teaming
HFE	human factors engineering
HSI	human-systems integration
IAE	information automation ecosystem
ICA	ineffective control action
ICS	information control structure
INL	Idaho National Laboratory
INPO	Institute of Nuclear Power Operations
LWR	light-water reactor
LWRS	Light Water Reactor Sustainability
MIRACLE	Machine Intelligence for Review and Analysis of Condition Logs and Entries
MISTIC	Method for Investigation of Socio Technical Incidents and Correction
MIT	Massachusetts Institute of Technology
ML	machine learning
NLP	Natural language processing
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operations and maintenance
OR	outage review
OSM	organizational systems modeling
PIR	proactive issue resolution
PROTECT	Proactive Resolution Of socioTechnical Ecosystem Cause Technique
PT	potential transformer
QC	quality control
R&D	research and development
SCS	safety control structure

SME	subject matter expert
SRO	senior reactor operator
STAMP	Systems-Theoretic Accident Modeling and Processes
STPA	Systems-Theoretic Process Analysis
U.S.	United States

Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis: Tool Development and Method Evaluation

Disclaimer: This August 2023 report is an update of Joe et al. (2023a), which was published in June 2023. The material retained from the prior report was deemed essential to understanding the approximately 45 pages of new content in this report. The background material provides important contextual information for the new content of this report.

1. INTRODUCTION

This report describes 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 digitalization in the control room and elsewhere, as well as a greater use of automation, artificial intelligence (AI), robotics, and other emerging technologies. There are significant opportunities to leverage these technologies for greater plant safety, efficiency, and overall performance. 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 (Leveson, 2011). 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 the system's technical and organizational components. 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. We have also employed the Systems-Theoretic Process Analysis (STPA) method to model the current ICS underlying preventive maintenance performance. This analysis was focused on identifying near-term process improvements and long-term design requirements for optimized ICSs. STPA is a useful modeling tool for analyzing actual or potential ICSs to proactively identify potential system weaknesses and thereby avoid unsafe events.

As stated previously in Joe et al. (2023a), the goals of this research project are:

- Develop an accurate cost-effective issue resolution process that utilizes information automation and 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 ICS 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 that, 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 safety control structures (SCSs) are generally caused by organizational and programmatic weaknesses, which manifest themselves through events and issues at all 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 remain relatively inconsequential due to constraints or barriers that mitigate 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.

Our previous research provided the industry with tools and techniques to support effective modernization from a human systems integration (HSI) point of view, specifically with regard to information automation. Information automation is the customization and delivery of information for a work process, thereby providing users with intuitive, actionable information based on continuous measurements of plant performance. This report is a continuation of that work and describes our efforts to evaluate the effectiveness of using STAMP to optimize information automation. This report also describes the development of an evaluation plan, our efforts to collaborate with industry partners, and presents the results obtained thus far from the evaluation (see Section 5.6).

The successful execution of this research 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 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 in 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 operations and refueling outages. This is a logistical challenge as well as a sociotechnical one.

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 (ANSI/HFES-400, 2021).

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, HFE, training and personnel selection, and management and others participate jointly in all aspects of the design process.

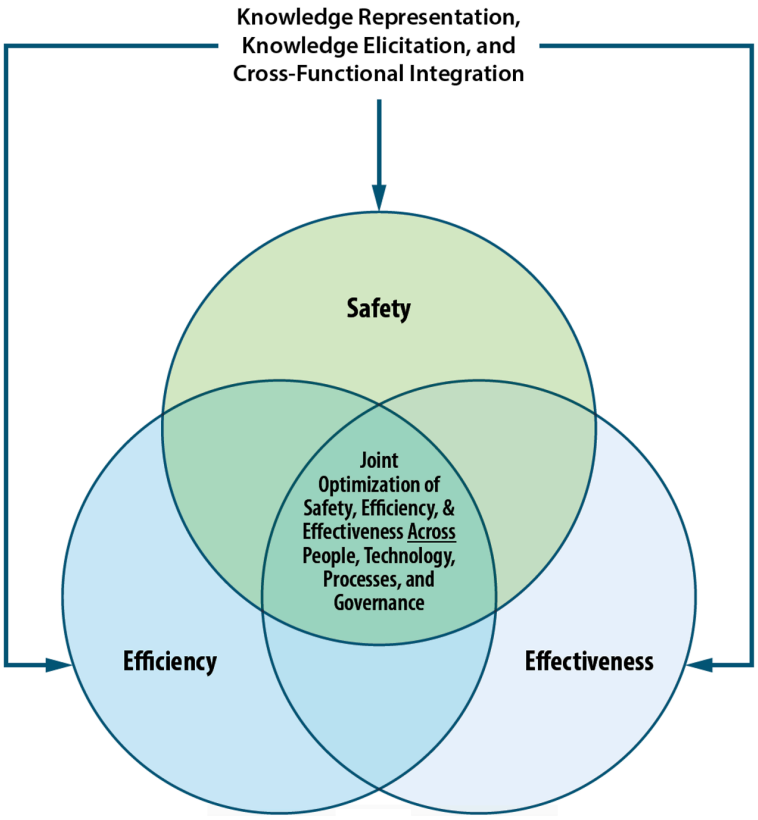

Figure 1. Joint optimization of safety, efficiency, and effectiveness.

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 done 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 the emergency safety system design and configuration not considering the loss of power scenarios initiated by a tsunami. The catastrophe could have been prevented if the utility had been 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.

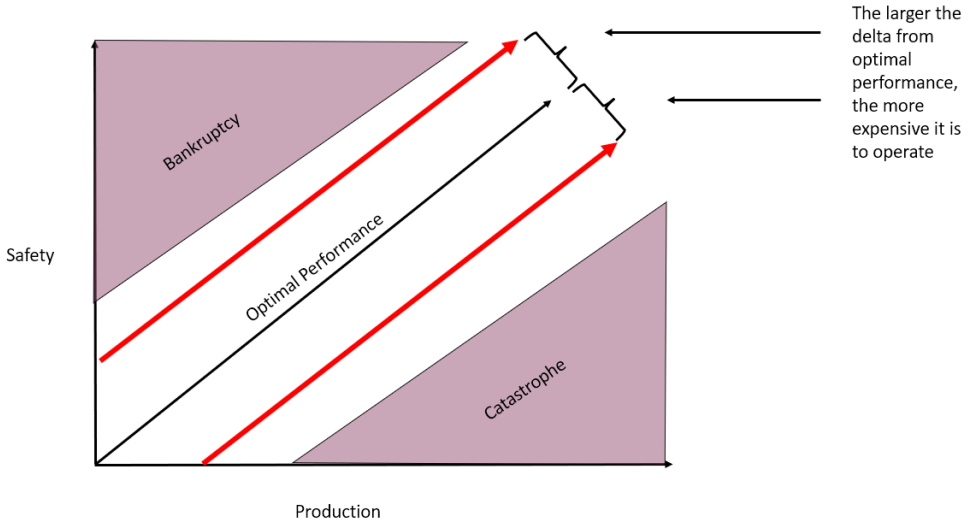

Figure 2. Optimal plant performance.

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 other NPPs. The solution to achieve optimal performance is to develop a more effective proactive issue resolution (PIR) 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 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.

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 organizational and programmatic weaknesses. 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 will be decreased.

Evaluating all 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 effectively performing this evaluation. We suggest that the solution is to develop a cost-effective issue resolution process that utilizes information automation and AI to identify trends in combination with a proactive analysis method, such as STPA, to continually analyze the data in search of technical, organizational, and programmatic precursors to significant events.

Figure 4 illustrates an initial PIR model and process structured around information automation, AI, and STPA. In support of the current research program's objectives, we are developing a PIR model, whose eventual instantiation and application is meant to address a significant near-term need in the nuclear industry (i.e., developing the ability to proactively identify potential issues and signs of weak or

weakening SCSs), while also serving as a prototype use case for developing a more general IAE model, instantiation, and application. We intend IAE to model a plant's entire IAE, within which the PIR and other "nested" models 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 advanced 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. Significant work remains to apply these tools to specific NPP use cases, but the system performance risk associated with their use has been diminished along with their technical maturation.

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. For instance, 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 information systems and analytic techniques. Tracking actions associated with issues and assessing their effectiveness is also desirable to ensure that an issue has been addressed and 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 IAE, and many extend beyond the realm of sociotechnical systems analysis, the focus of the current work. Our major research and design 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 and human-AI interaction, including issues such as user trust in the system (e.g., Hoff and Bashir, 2015), system transparency (e.g., Larsson and Heintz, 2020), information presentation, and interface design. Simply put, the focus of the current research effort is 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 an SCS, 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 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 hierarchically and characterized by occasionally complex control and feedback relationships among themselves.
- High-level system behaviors (e.g., safety, efficiency, productivity) are considered *emergent properties* of the activity within that system; however, emergent properties are not simply a linear function of the combined behavior of individual system components but are also heavily influenced by the combined, nonlinear 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 components, and associated processes. The analysis and design of sociotechnical systems, specifically from a systems perspective, is a relatively recent development in

engineering and the social sciences (e.g., Leveson, 2011; Noy et al., 2015), and its application in industry and defense applications is becoming more widespread. The current research applies two emerging techniques based heavily on sociotechnical systems theory to issues involved in NPP maintenance.

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.

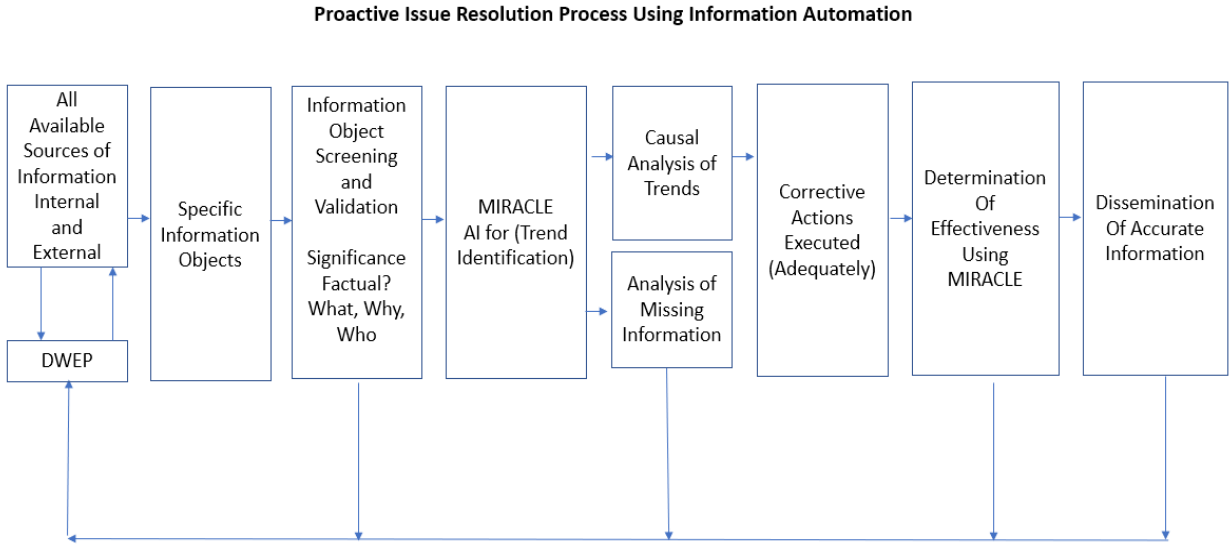

Figure 4. PIR process using information automation.

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 then performed as an in-depth evaluation of relevant 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 also all LWRs, 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 whose purpose is 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 also improve it incrementally while the actual work is being performed.

The DWEP improves itself and the user experience by 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 enables 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 should be 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 performance and reconfigure 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 (EID; Bennett and Flach, 2011; see Section 5.5), 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. In essence, this is why we believe there is potential analytic and design benefit in modeling IAEs as ICSs.

Figure 5 provides a high-level depiction of the IAE model as currently envisioned. It 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. It should be emphasized that the IAE model represents an end-state vision of what a functional IAE could look like. Whereas the PIR model has significant potential for near-term development and implementation, all of the initial requirements of the IAE model (e.g., near real-time extraction and processing of plant performance data) are not yet technically feasible.

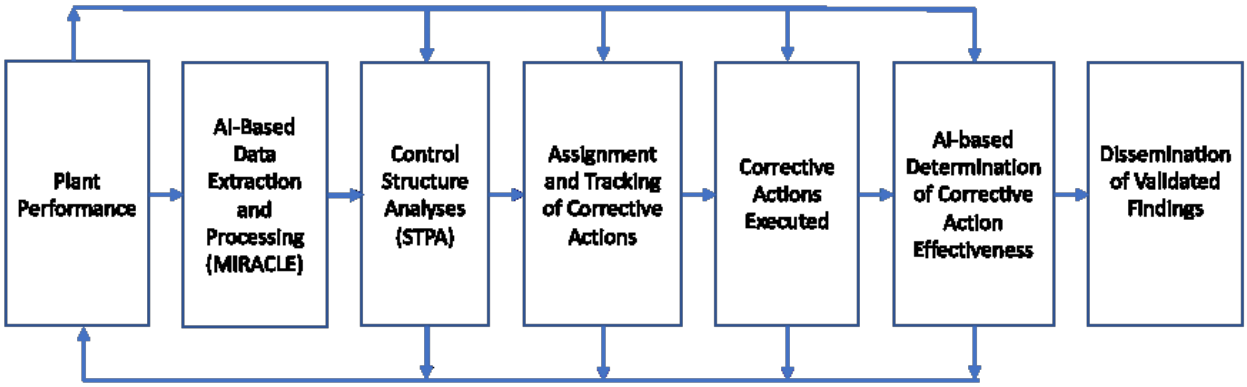

Figure 5. Preliminary IAE model.

Within the context of NPP operations, a plantwide IAE would:

- Continually extract plant system and component performance data.
- Perform data reduction and processing to identify potentially problematic trends.
- 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 in which automation and AI may be of value in providing users with suggested actions and approaches to addressing a particular problem. "Expert system" applications of this sort have been studied for some time (e.g., Waterman, 1985), but the recent surge in interest in AI and ML has rekindled interest in and the potential promise of the approach (e.g., Khan et al., 2021; Zhao et al., 2020).

1.5.1 Optimizing Information Automation

The principal goal of the current research effort is to support the development of an optimized IAE. When using "optimized," we refer to the following suggested set of characteristics. These 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, information needs 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's 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 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.

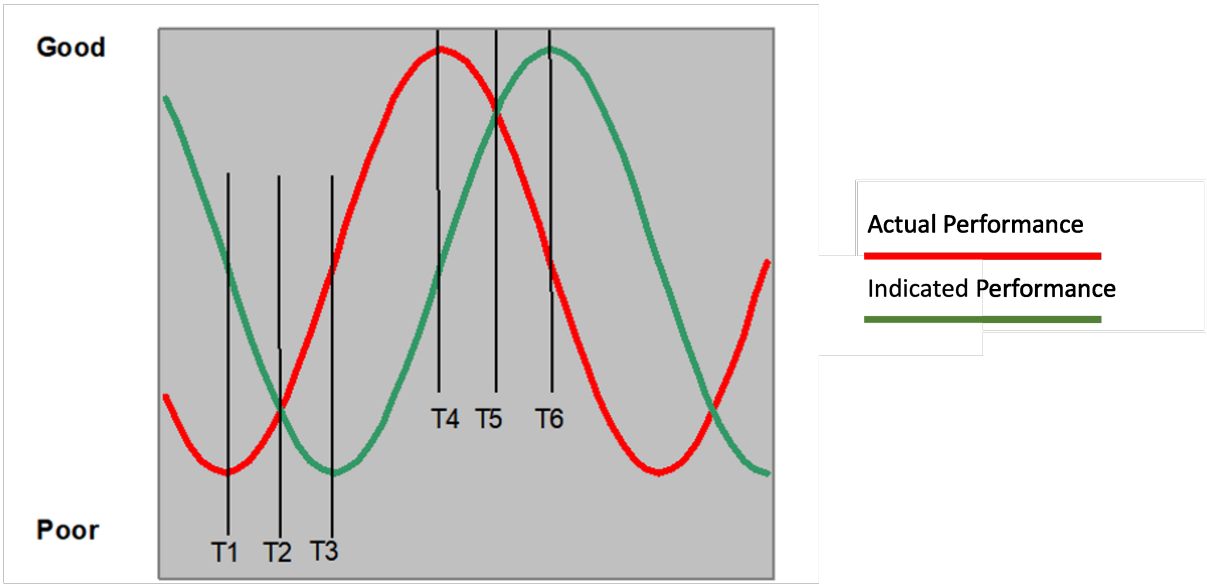

Figure 6. Time differences between indicated and actual plant performance.

Figure 6 illustrates the potential consequences of delayed information delivery. Specifically, if the 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

The principal goal of this research project is to support information automation design through the joint optimization of people, technology, processes, and governance, that is, to ensure the effective integration of humans with the technical and organizational systems that constitute the sociotechnical

system within which they perform their work. Within the context of the current effort, HSI has two general 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, testing, and deployment. This includes disciplines such as human factors and ergonomics, cognitive engineering, training, personnel selection, safety, organizational design, 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 effort. From a managerial perspective, it is viewed as a key risk and cost reduction approach during system design and development (e.g., Rouse, 2011). This is based in part on the military's experience with expensive and time-consuming system retrofits necessitated by a lack of attention, during system design and testing, to integrating the system with the humans on whom it relies for its operation. HSI is just as concerned with the design and implementation of organizational systems as it is with technical systems, as these also directly impact human-system performance quality. As the current effort evolves from the conceptual, research phase to the system development phase, this application of HSI will become increasingly important.

HSI can also be thought of as a research and design approach or discipline focused on optimizing the specifics of the relationships 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, and Hettinger, 2007; Tate, Estes, and 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, the term "sociotechnical" refers to those technical and organizational aspects of a given system 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 aspect of the system, defined as an interactive set of human and technical components, that has the potential to impact human-system 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 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 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 risks 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 when, for instance, senior management is separated by several layers of communication and technology from front-line 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 Transportable Tools for Sociotechnical System Analysis

The principal analytic methods used in the current work, STPA and CAST, are currently in wide use across multiple applications. This is due in large part to the unique insights on system performance that each affords and to the relative ease with which they can be learned and applied compared to traditional risk and accident analysis methods. However, there is an additional perceived need on the part of industry for simpler methods that can support more efficient analyses, identifying and assessing sociotechnical system issues at a relatively high level of abstraction, while flagging issues and areas of system performance that merit further analysis with STPA, CAST, or some other analytic method. We refer to this simpler class of methods as "transportable tools."

There are important tradeoffs to consider when adapting STPA and CAST to simpler methods such as checklists or flow charts. For instance, there is a risk that abridging the methods may result in the loss of important information and insights. Managing this risk will require that the tool, in addition to supporting a sufficiently broad survey of potential sociotechnical issues potentially impacting NPP system performance, must provide users with guidance on when more detailed analyses are warranted. At that point, personnel trained in the proper conduct of STPA and CAST analyses will be required.

The goal of transportable tool development, in the current effort, is to provide industry with valid and reliable methods for efficiently identifying sociotechnical risk factors, either related to an incident or accident (i.e., CAST) or to a potential future system or subsystem design (i.e., STPA). These methods and their outputs should be readily comprehensible and usable for the population for whom they are intended (i.e., nuclear plant workers). Therefore, to maximize efficiency and validity, the development of these methods and their means of implementation should follow a user-centered design approach.

Our initial efforts at transportable tool development are focused on two areas. The first involves providing NPP personnel with the knowledge and means to develop and analyze relatively uncomplicated control structures. Dainoff and Hettinger's past experience with this approach indicates that these abilities are easily learned and that, in many cases, examining control structures alone (i.e., without the other STPA or CAST components) can reveal significant issues in an existing or proposed system design. The second area focuses on the development of CAST and STPA checklists based on findings and themes from published literature and conference presentations. These checklists are intended to provide users with the means to efficiently assess sociotechnical system risks while also indicating when further analyses are called for.

1.8 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 the deployment of innovative approaches to improving the economic viability 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, event costs, although latent and more difficult to measure, can be monetized. The costs to react to and recover from an event become embedded in the costs of the actions taken to address the issue, to react to the violation of the regulations, and to prevent the recurrence of similar events through the mandated Causal Analysis. As previously stated, there is a direct correlation between the prevention of significant events and issues, and the operating and maintenance costs to run the plant safely and reliably. Therefore, the focus of this process is to make a step reduction in the number of significant events through the identification and subsequent correction of significant event precursors, before they can result in an impactful plant event.

As illustrated in Figure 7, we anticipate that the successful development and implementation of an effective PIR process will result in a significant reduction of O&M costs through a reduction in significant events that would be considerably more favorable to the industry than is currently the case.

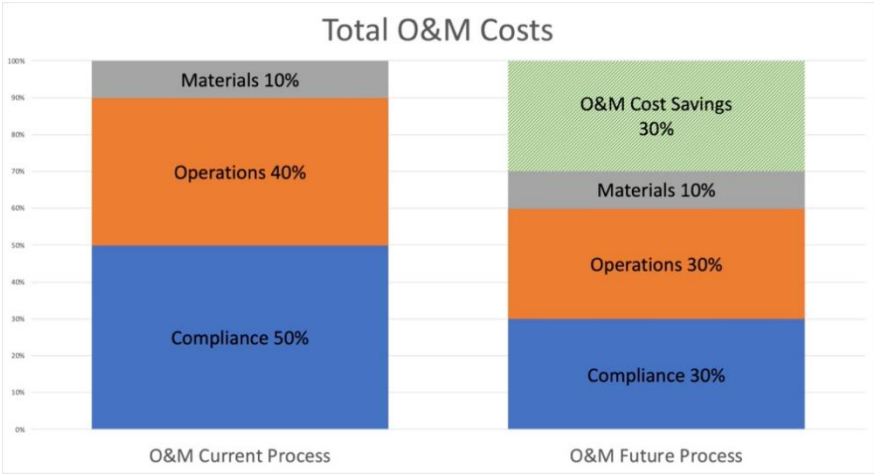

Figure 7. Projected impact of effective PIR on total O&M costs.

Sociotechnical system methods of the sort used in this program of research, notably those derived from STAMP and other HSI approaches, 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 of the NPP management and, when used early enough in the system lifecycle, will help prevent or reduce later excessive 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 the 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 ICS. The long-term objective of this work is supporting the development of this dynamic network, comprising multiple technical and organizational components, supported by AI (i.e., MIRACLE) and advanced automation (i.e., DWEP).

We are also developing easy-to-learn, easy-to-use analysis tools for sociotechnical systems analyses. Our objective is to provide the industry with the means to acquire reliable and rapid information about system incidents or to conduct proactive risk analyses on existing and proposed systems and subsystems.

We selected the near-term objectives (Sections 2.1–2.4) 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 incident analysis and in describing and modeling existing safety and ICSs, as described in previous related work by Dainoff et al. (2022). STPA focuses on proactive analyses of existing and potential systems, looking beyond the sociotechnical interactions that characterize specific events to examine broader system design and usage issues.

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 and control theory. To this end, we have focused on modeling a near-term application PIR model and a longer-term general IAE model, the latter serving as an end-goal vision of an optimized IAE.

The major focus of a sociotechnical-systems-based model of information automation is to identify areas of potential concern with regard to human-system 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 modeling, describing, and specifying 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 nested models (such as PIR) and other 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 assist in providing a basis for optimized information automation 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 the specification of

how system-level requirements will be met.

We will create a set of preliminary system-level requirements in conjunction with technical experts in MIRACLE and DWEP and subject matter expertise from our industry partner when possible. Additionally, we will create a set of preliminary system safety constraints, derived from the CAST and STPA analyses, that can be considered system-level requirements for what the system must *not* do and what it must be able to prevent from occurring.

2.4 Objective 4: Develop Transportable Tools for Sociotechnical Systems Analysis

The final objective of the current work is to develop sociotechnical systems analysis methods and tools for use by nonspecialists in NPP settings. While STAMP-based methods are relatively easy to learn, there is potential value in developing "quick-look" tools based on STPA and CAST for those without specific backgrounds in systems engineering or safety. These tools should rapidly identify sociotechnical systems issues present in existing and proposed systems or as part of incident investigations, while also clearly identifying situations in which more in-depth analyses are warranted.

3. APPROACH

Figure 8 provides an illustration of the current research effort's approach. The principal analyses we will perform include STPA and CAST. 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.

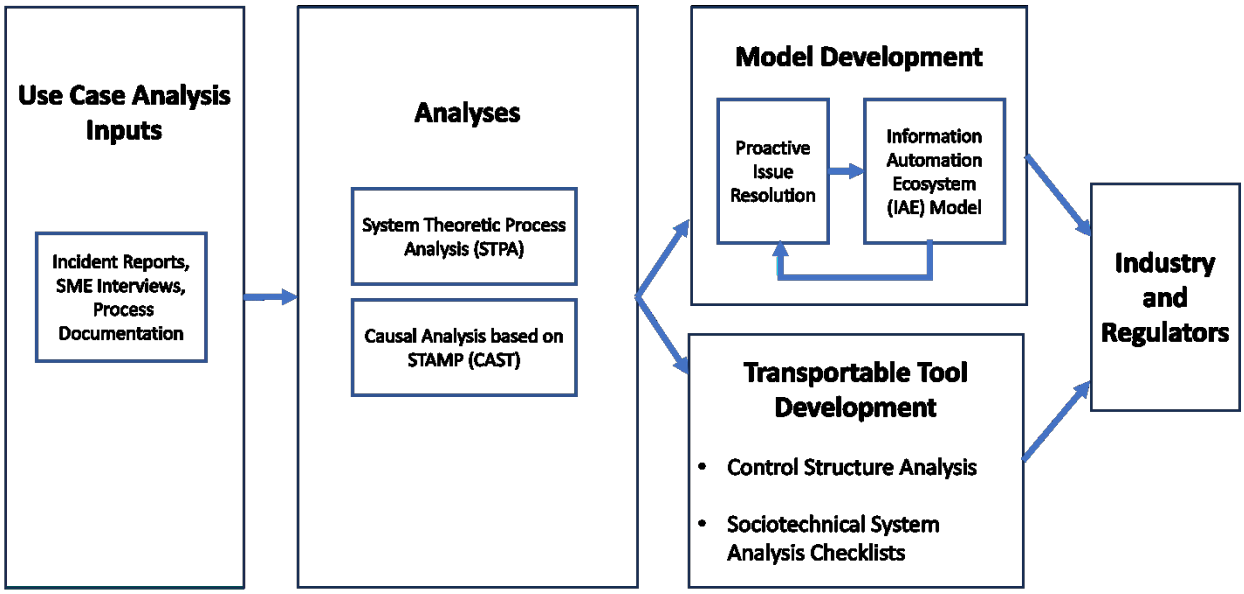

Figure 8. Research analysis and design approach.

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, models, and tools will be disseminated as broadly as possible within the industry and regulator communities.

3.1 Event and System Analyses

Two separate systems-based analyses were conducted as part of this work. The first (CAST) examined systemic causal factors in a recent NPP event involving the unplanned activation of an EDG. The second (STPA) examined current systemic factors impacting safe and efficient execution of preventive maintenance tasks. This section provides a discussion of the analytic methods that supported these analyses and the specific manner in which each was applied.

3.1.1 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; Leveson and Thomas, 2018). 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).

3.1.2 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, 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.

3.1.2.1 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.)

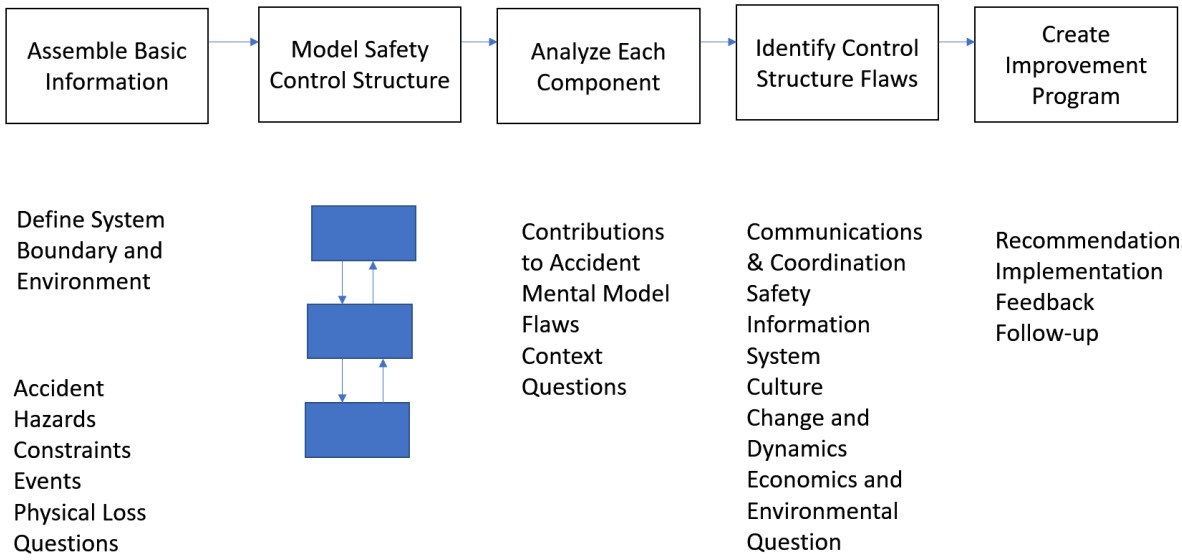

Figure 9. Major components of CAST analysis (Modified from Leveson, 2019, 34).

3.1.2.2 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, 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 system hazards and constraints.

3.1.2.3 Modification Based on Johnson's Coordination Model

Johnson (2017) has identified 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.

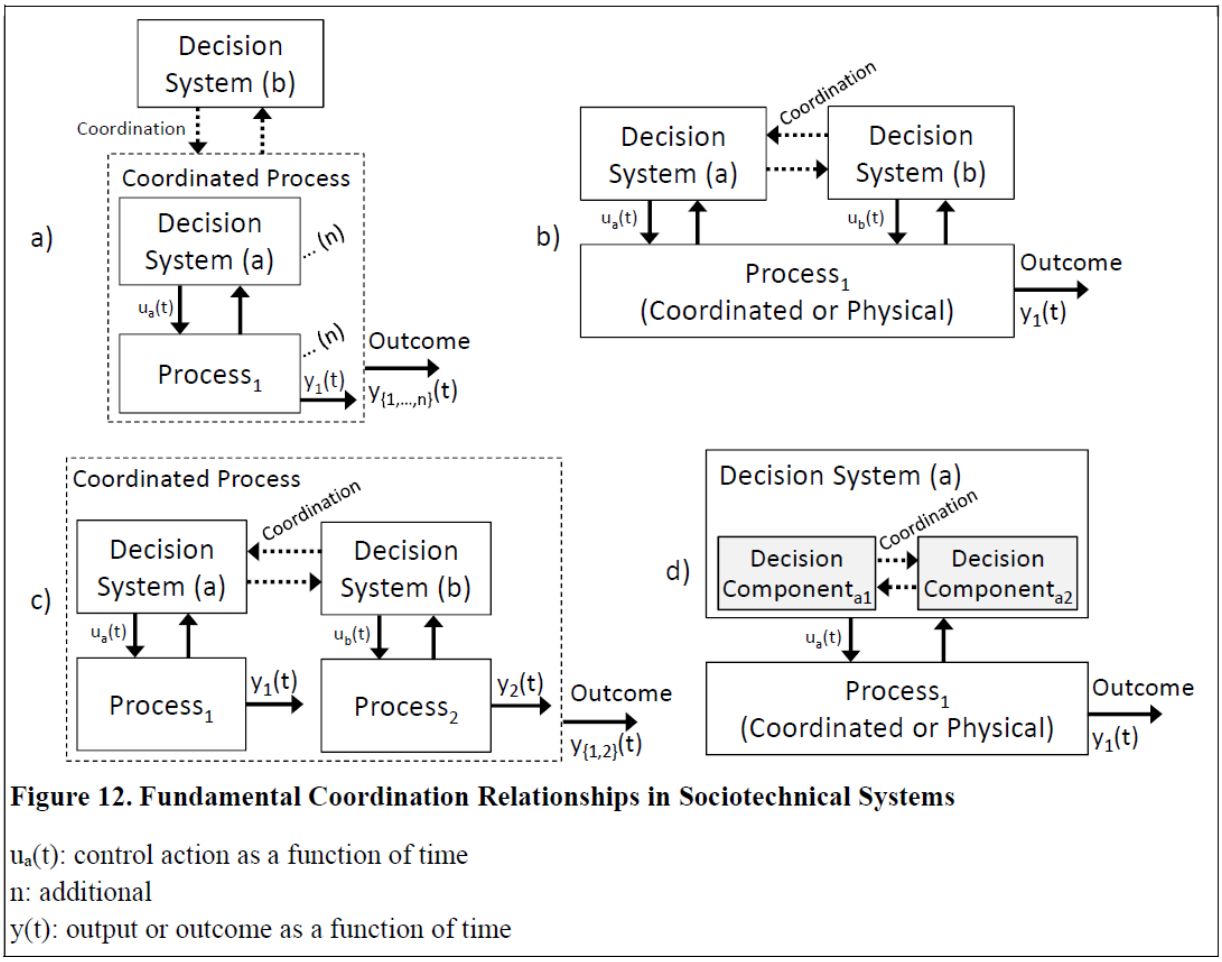

Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

$u_a(t)$: 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 with author permission).

Figure 11 (Johnson, 2017, Figure 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, particularly 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.

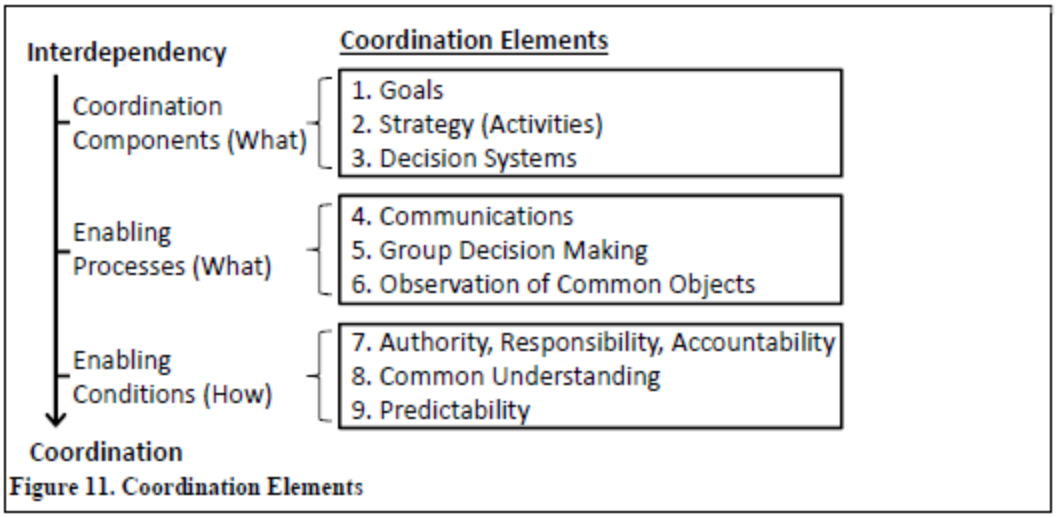

Figure 11. Element of coordination (redrawn from Johnson, 2017, Figure 11; Used with author permission).

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. Hierarchy, displayed on the y-axis, consists of two basic levels: the required layers of coordination on top and physical actions that emerge below. These physical actions also include the production of key documents. In the situation depicted in this diagram, which reflects holistic coordination, 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.

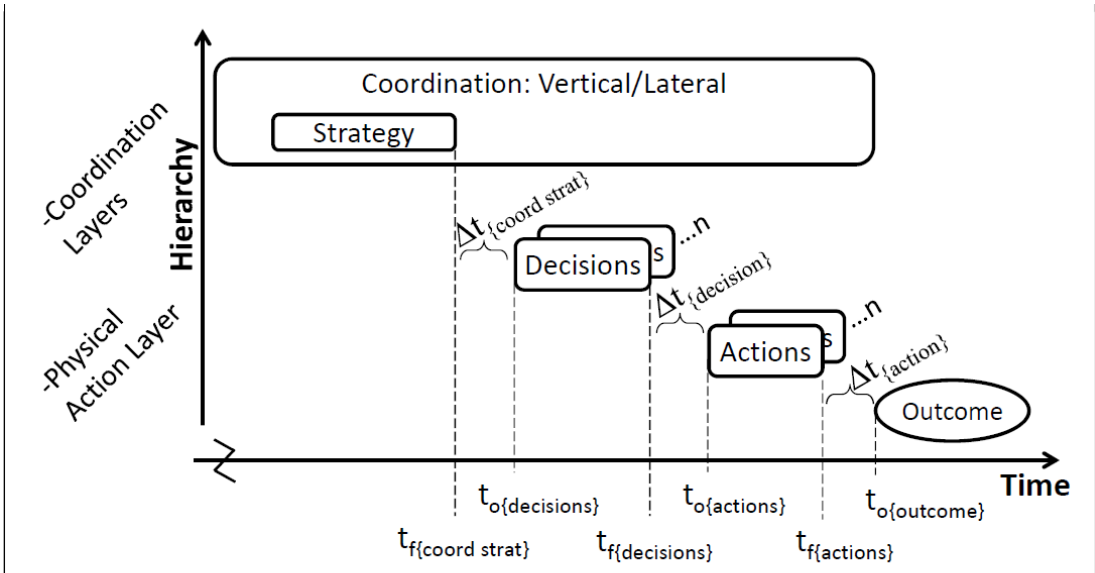

Figure 14. Coordination and Time

$t_{f\{behavior\}}$: finish time of a behavior
$t_{o\{behavior\}}$: initial time of a behavior
Δt: time difference between behaviors

Figure 12. Modified SCS (redrawn from Johnson, 2017, Figure 11; Used with author permission).

3.1.3 System Theoretic Process Analysis

STPA is a "proactive analysis method that analyzes the potential causes of accidents during development so that hazards can be eliminated or controlled" (Leveson and Thomas, 2018, 12). It has become a widely applied risk assessment technique in multiple applications, including defense (e.g., Johnson and Leveson, 2014), industry (e.g., Yousefi and Hernandez, 2019), nuclear energy (e.g., Bar-Or and Hartmann, 2023), and others. STPA provides a means of envisioning and analyzing complex sociotechnical systems by modeling them as control structures, comprising human and technical components interacting with one another by means of control, feedback, and communication linkages. The specific steps involved in STPA are described in Section 4.2, along with the analysis findings.

STPA serves two major roles in the research program. First, it is the principal tool in our analysis of generic NPP preventive maintenance information control systems. In this role it also supports the identification of near- and intermediate-term system improvements, including potential applications of automation, AI, etc. Second, the control structure element of STPA is a key component of the PIR and IAE models (see Figures 4 and 5). Specifically, the role of the control structure in the two models is to accept inputs from MIRACLE regarding identified trends of potential safety concern. These inputs expose the vulnerable parts of the control structure, whose changes reflect the nature of the impending safety concern and areas of the system under the most potential stress. The DWEP component of the models (see Section 1.4.2) then accepts input from the control structure, alerting personnel and organizations whose corresponding areas of the control structure are under potential stress or who otherwise have a need-to-know.

A prior report (Joe et al., 2023a) described an analytic process referred to as OSM. The purpose of OSM is to develop a control structure comprising all relevant organizational components involved in a particular system, along with their control, feedback, and communication linkages. The goal of OSM is to identify potential weaknesses in the organizational control structure of a sociotechnical system. However, the STPA that we performed on a generic NPP preventive maintenance system as part of the current work exclusively comprises organizational entities, thereby rendering the OSM analysis redundant for this

phase of the work. We anticipate that it may be used again when mapping the organizational relationships that underlie the full IAE.

Evaluation criteria related to the effectiveness of STPA may include:

- A number of insights regarding potential system risks that would not be expected to be uncovered with standard risk assessment techniques. Are there novel or surprising insights that may not be uncovered by other risk analysis methods.
- A number of opportunities identified for integration of automation, AI, and other advanced technologies. Are there appropriate locations and functions in the system where advanced technology could be used to address bottlenecks and/or inadequacies in control, feedback, and/or communication.
- Time and resources required for performing the assessment. Compared with other risk assessment techniques, how much time does it take to conduct an STPA and what resources and training are required.

3.1.4 Use Case Selection and Description

The analysis 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. 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 the utility partner's procedures, investigations, and CAP data, as well as interacting with internal SMEs, to help the team challenge conclusions and effectively develop this process.

3.1.4.1 CAST Analysis—Event Description

The event that was evaluated by the team was an unexpected start of an 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.

3.1.4.2 STPA—System Description

The use case selected for the STPA analysis focused on the assessment of the sociotechnical system supporting NPP preventive maintenance management, planning, scheduling, supervision, and work execution. Preventive maintenance was selected because system improvements in this area could afford

many benefits for the nuclear energy industry. More efficient maintenance of plant safety and greater predictability of future work and required resources are two of the benefits the industry might expect from improvements in preventive maintenance systems.

As part of Step 1 of the STPA process, we provide a more complete description of the generic maintenance system we selected for analysis (see Section 4.2.1).

3.2 Information Automation Model Development

One of the major objectives of this research effort is to develop IAE 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 PIR capability 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.

3.2.1 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 with 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 with all regulatory requirements can be as high as half of the utility's operating costs. Figure 13 shows the breakdown of the most significant contributors to this utility's operating costs.

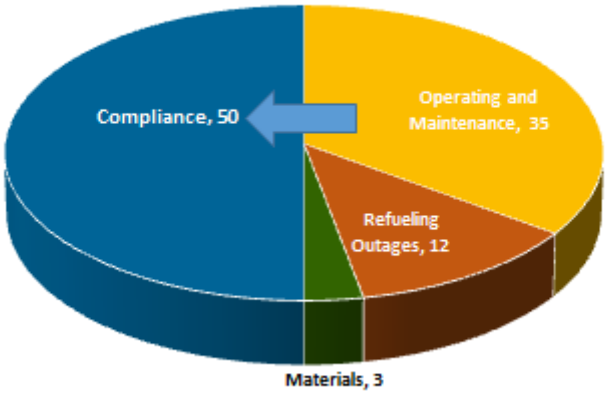

Figure 13. An estimate of one utility's operating costs.

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 becomes 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 had become too high to compete with other more economical sources of generation without financial intervention by their respective states.

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 United States 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. Since the beginning of human cognitive thought, it has been common knowledge 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 14 represents the widely accepted concept.

Figure 14. 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 is 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 previously unavailable. 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.

3.3 Transportable Tool Development

As part of the current effort, we have focused on three areas for transportable tool development. These include an approach for simplified control structure modeling and analysis and two checklists for quick-look incident and system design analysis. The latter is based on findings and themes from the STAMP, HSI, and HFE literature.

Control structures are extremely useful tools for identifying potential safety and system performance issues (e.g., Leveson and Thomas, 2018) in complex sociotechnical systems. The steps required to develop and analyze high-level control structures are quite straightforward and have been successfully trained and applied by Dainoff and Hettinger in a number of occupational settings, including trucking, rail operations, and manufacturing. In each of these cases, SCSs were largely developed and analyzed by workers themselves with assessment personnel serving primarily as facilitators. Our current efforts in this regard have focused on formalization and description of the steps involved in control structure modeling and analysis. Our intent is to produce an easy-to-learn, easy-to-use tool that provides a means of quickly and easily modeling the system being analyzed, including the presence (or absence) and adequacy of control, feedback, and communication linkages between its components.

The Method for Investigation of SocioTechnical Incidents and Correction (MISTIC) will consist of a checklist of items derived from common themes and findings from the CAST, HSI, and HFE literature related to sociotechnical system causal influences on incidents and accidents. Our approach was to review the published literature in these areas through Google Scholar searches, extracting and noting representative findings.

Similarly, the Proactive Resolution Of socioTechnical Ecosystem Cause Technique (PROTECT) will consist of a checklist of items derived from common themes and findings from the STPA, HSI, and HFE literature related to existing or proposed system analyses. As with MISTIC, our approach with PROTECT was to review the published literature in these areas through Google Scholar searches.

Figure 15 provides an illustration of the current and planned development process for the above tools. The current effort has resulted in the completion of Step 1, including developing a draft, stepwise procedure for control structure development and gathering themes and findings from the STPA, CAST, HSI, and HFE literature. Subsequent steps will focus on the development of draft tools and supporting training materials to support beta testing with NPP industry SMEs. Following the refinement of the tools based on these findings, we propose assessing their performance in the analysis of industry incidents and use cases by comparing their performance against full STPA and CAST analyses. Differences in performance related to such factors as the number of findings obtained and the time and resources needed for training on use of the tools and performance of the analyses are potential evaluation criteria for these

analyses.

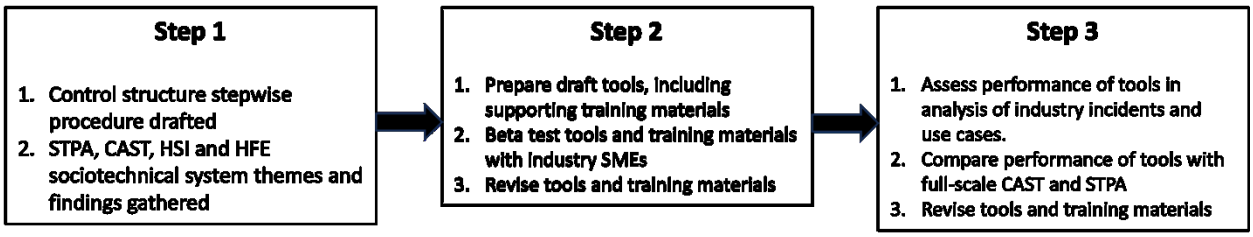

Figure 15. Transportable tool development process.

4. RESULTS

This section provides a description of the results of the analyses presented in Section 3.1above. Results are provided for the CAST analysis performed on the unintended EDG activation use case and for the STPA analysis performed on the NPP preventive maintenance system. Results of efforts to further mature the PIR model, specifically with regard to the contribution of MIRACLE, and to develop transportable tools for sociotechnical system analysis are provided.

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

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

This section describes the CAST analysis results, including the suggested modifications proposed by Leveson and Johnson, as discussed in Sections 3 and 3.1.2.3. 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 Constraints 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, 44).

Figure 16 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), see Figure 17. The specific levels identified with each of the three aspects of project work were governance, clearance, design, and work processes.

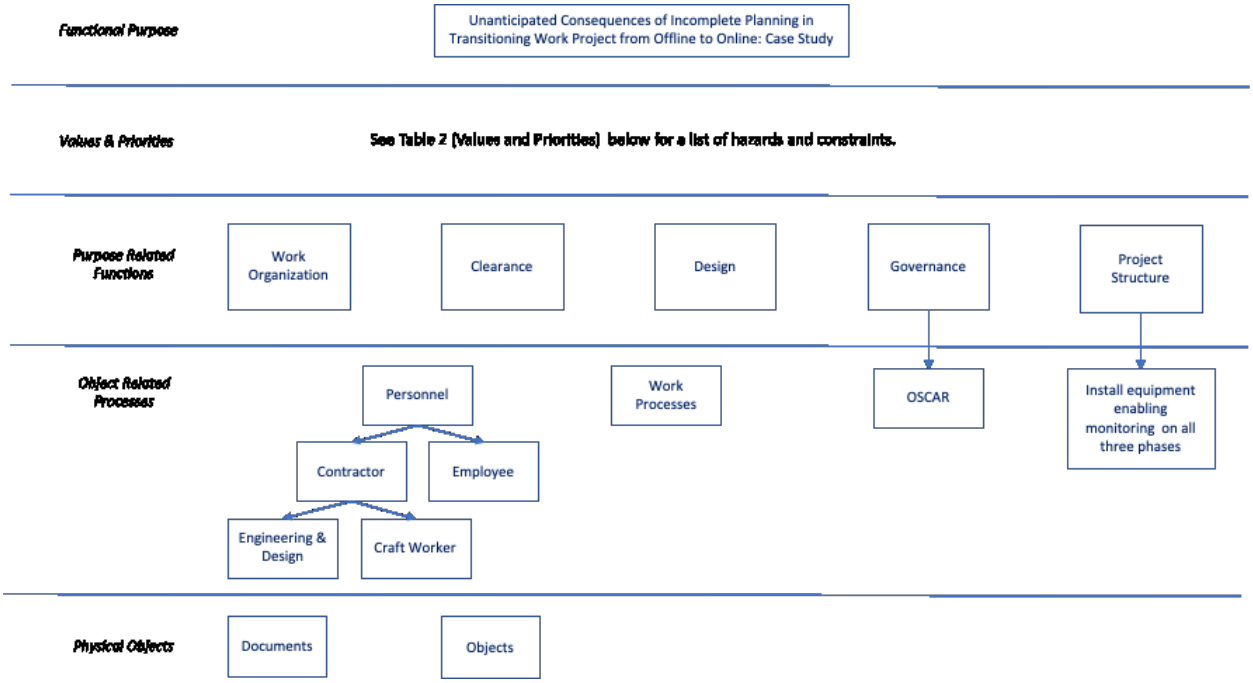

Figure 16. Skeleton means-end abstraction hierarchy.

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 Motor Control Center 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 the 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 the safety of plant workers
Walkdowns by planning and work execution workers should identify safety risks to workers
System Hazard #5: NRC Reportable Event
Safety Constraints:
The plant licensing process by the regulator is designed to ensure maximum nuclear safety is achieved
Reduced regulatory margin at one nuclear plant results in the 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 and 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	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

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
						performed again to evaluate the impacts of opening this bus drawer while the plant was 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 was there no feedback to the design review process to direct it to go back and redo several steps?	work, and even during the online work, the high voltage side of the PTs would be dead; however, other circuits (load 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).

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
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 cable interference or recognize Bus PT drawer in Cubicle 318	Previous efforts to address the Byron open phase vulnerability were performed when the NPP was offline (during outages). Why not by the maintenance or engineering manager?	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 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	—	—	Clearance request does not recognize that the workers could be exposed to dangerous voltage contained somewhere within the cubicle (in the drawer) and that actions in the cubicle could result in the start of the EDG.

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
				hazards specific to the evolution of this work activity.			
6	Work order walkdown	Work order 360 walkdown signed off as completed by construction contractor general foreman. Personnel actually involved in construction (construction subcontractor) were not involved in this walkdown.	—	—	—	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.
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	—	Although an independent review was performed, the original and independent reviews both	The independent reviewer should have recognized the risk to workers and the plant; however, it is unclear how “independent” this

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
				individuals would be working in the vicinity of Cubicle 318 drawer with 4 kV present.		failed to recognize that individuals would be in the vicinity of the Bus PT drawer—so far, all walkdowns failed to identify this risk.	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	Senior reactor operator (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 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 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	Why was the unique nature of Cubicle 318 not identified?	This meeting should have identified the unique issue with Cubicle 318 and added additional

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
					control (QC) engineering, construction contractor, operations, planning, and project management		barriers to prevent the worker safety issue and the possibility that load sequencer work in Cubicle 318 could result in an automatic start of the EDG.
13	Additional tabletop meeting held to address the stop work	Tabletop 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 changes to work plans made.	—	—	—	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 automatic start of the EDG.
14	Final review board for project	Restart work authorized	—	—	Final review board to address the project stop work held with plant manager,	Why was the unique nature of Cubicle 318 not identified?	This meeting should have identified the unique issue with Cubicle 318 and added additional

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
					QC, engineering, construction contractor, operations, planning, and project management		barriers to prevent the worker safety issue and the possibility that load sequencer work in Cubicle 318 could result in danger to installers and an automatic start of the EDG.
15	Work commenced on Cubicle 318	(2) Prejob 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 from their work package and saw the number 318 in the tagout list. They had previously successfully	—	(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
		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 17 depicts the control structures reflecting events through 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 the 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 1–660, 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 OR 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 17 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.

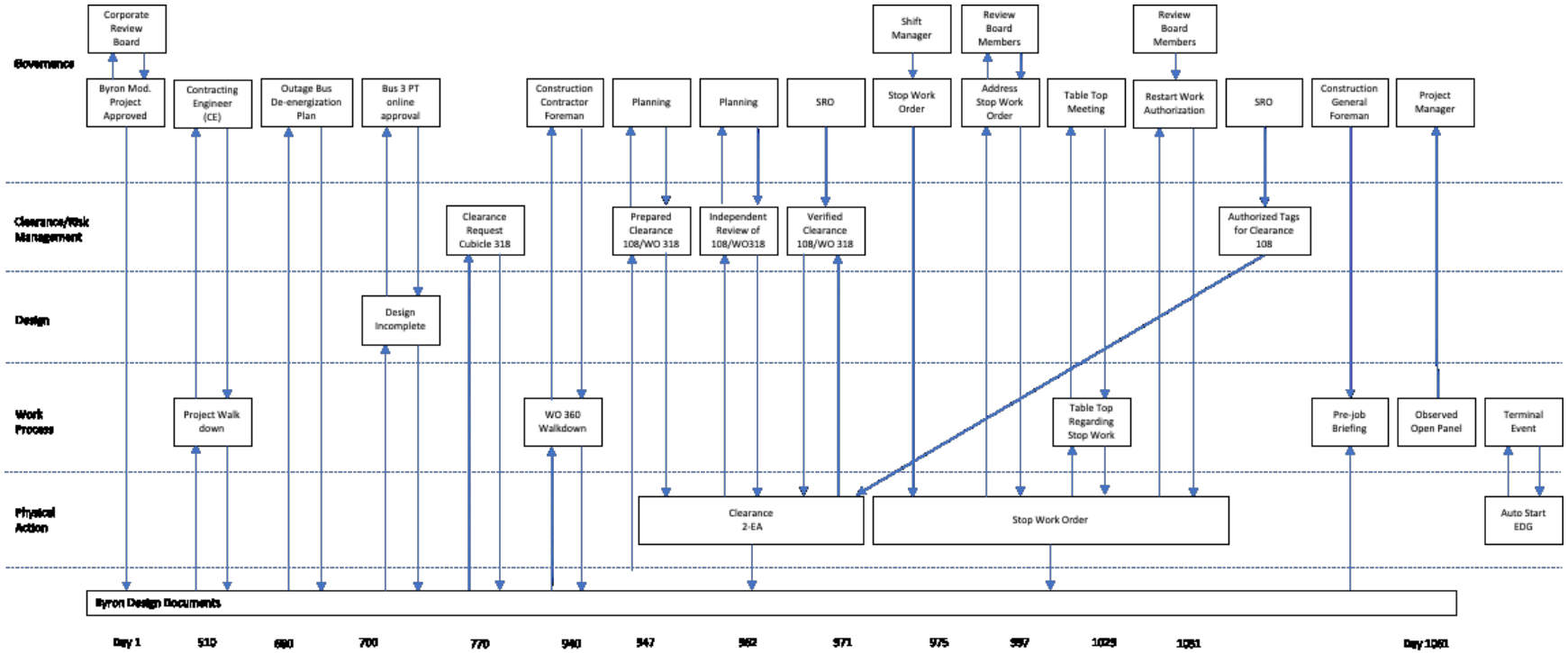

Figure 17. SCS using the format by Johnson (2017).

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 the 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 Probabilistic Risk Assessment (PRA) safety constraint described above, the EDG is the second most critical	Given that the work was scheduled for offline completion, the risk associated with the autoactivation of the EDG would have been lower.

Controller Or Controlled Process	Responsibility	Contribution	Process Flaws	Context
			element in plant protection.	
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 318 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 Day 700	Transition procedures for projects originally scheduled to be accomplished during the outage but now are to be done online.	No indication of the risk associated 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.	There is no indication in the available 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.	The final design, with applicable drawings 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

Controller Or Controlled Process	Responsibility	Contribution	Process Flaws	Context
				versions of work management systems running in parallel.
Construction Contractor Foreman Walkdown Day 940	According to the 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 other components within the bus, just as the implementing crew would not.	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.
Planning Prepared Clearance 108 Day 947	Prepare Clearance 108 for Work Order 360 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	Importance of Cubicle 318 to EDG safety system is still missing.

Controller Or Controlled Process	Responsibility	Contribution	Process Flaws	Context
			EDG, or recognize that workers would be in the vicinity of 4 KV.	
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	SRO 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 for work corrections and changes to work plans.	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.
Tabletop Meeting to Address Stop Work Day 1,029	Tabletop 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	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.

Controller Or Controlled Process	Responsibility	Contribution	Process Flaws	Context
	sequencer tie-in work. Discussed lessons learned and durations for work, corrections, and changes to work plans made.			
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 Prejob Briefing Day 1,061	Foreman gives a prejob 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 Day 1,061	Project manager observed the work crew opening Cubicle 318.	Project manager did not watch how the crew responded to the situation, which had safety-critical implications.	Unclear what the project manager's mental model of the crew's task was with respect to the drawer containing Fuse B318.	Time pressure.
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,	The crew had successfully performed the same operation before, including opening the fuse drawer, and had not been informed that Cubicle 318 was different.

Controller Or Controlled Process	Responsibility	Contribution	Process Flaws	Context
			that number referred to a fuse from a different cubicle. Thus, they thought they had been cleared.	

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, environment, organizational climate, economic and environmental factors, and safety information systems, changes, and dynamics over time in the system.

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 18, 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 the activity. The NRC's time requirements for completing this activity seem 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 2 of Section 4.1.1.1.
  - Decision Systems: Figure 18 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.

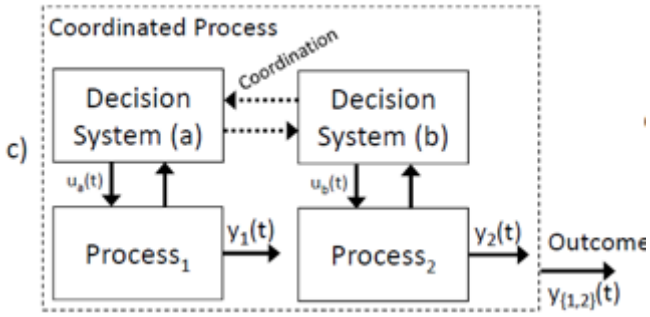

Figure 18. Generic fundamental coordination relationship applicable to the present case (Johnson 2017, Figure 12; used by permission of the author).

- 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 in Section 4.1.4. 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 17) 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 System-Theoretic Process Analysis

This section describes the steps taken and results observed during an STPA analysis of a generic NPP preventive maintenance system. Since NPPs, particularly those in the United States, have preventive maintenance systems in place that are broadly similar to one another, we felt that an analysis of generic systems, emphasizing qualities shared across NPPs, would be a logical starting point. In this analysis, we relied heavily on the methodology described by Leveson and Thomas in the *STPA Handbook* (2018). We also adopted work domain analysis (WDA) as a method for describing and modeling the means-end relations between high-level organizational values and intents and the means and methods of system performance (e.g., Dainoff et al., 2022; Leveson, 2020).

The present analysis relies heavily on one of the author's (Murray) extensive expertise in NPP operations across the United States and the world. Having studied and assessed preventive maintenance

systems in multiple plants, his subject matter expertise supported the analysis throughout. Having arrived at the findings described below in Sections 4.2.1–4.2.4, a logical next step will be to refine and validate the results, including the control structure, using additional SMEs from industry.

STPA is structured according to four steps, identified in Figure 19, and described in detail in the following sections. The unique analytic objective of each step is provided along with a summary of the findings from our application of each step to the modeling and analysis of a generic NPP preventive maintenance system.

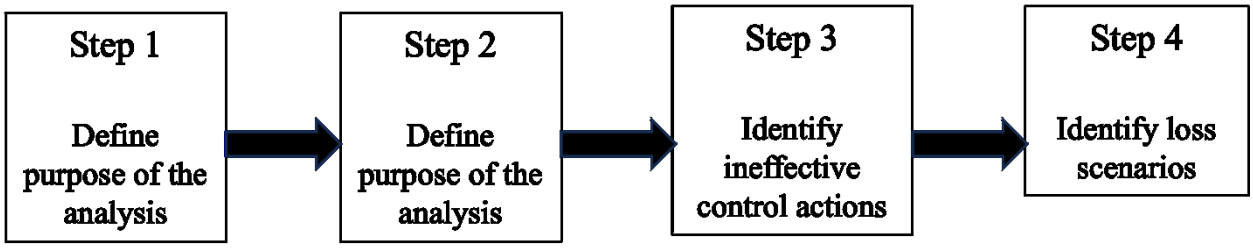

Figure 19. Four steps of STPA process.

4.2.1 Step 1: Define Purpose of Analysis

There are several analytic objectives addressed in STPA, with the most fundamental being to achieve a clear definition of the purpose of the analysis, including various specifications and descriptions of the system to be analyzed. This section describes the analytic issues addressed in the first of the four steps that comprise STPA, along with corresponding results. Similar treatments of the remaining three steps are provided in Sections 4.2.2, 4.2.3, and 4.2.4.

4.2.1.1 Define System Scope, System Boundaries, and System Stakeholders

To clarify the subject matter and scope of the analysis, it is important to clearly specify the system to be examined and to establish its boundaries. The subject matter of an STPA analysis is typically an existing or planned sociotechnical system, described with regard to the organizational and technical components that comprise it and the control, feedback, and communication linkages between them. Leveson and Thomas (2018) recommend setting system boundaries that exclude entities, processes, etc. that are outside the ability of the analyst and/or their organization to affect any changeover. We adhered to both of these areas of guidance in the current analysis.

The system we chose for analysis is a generic NPP preventive maintenance system and, specifically, the corporate, management, and front-line work entities involved in its management, supervision, and execution. System boundaries were established at the senior corporate level of management. Although there are other organizational entities with potential influence on preventive maintenance programs (e.g., NRC, Institute of Nuclear Power Operations [INPO]), the research team determined that they lay outside the bounds of direct influence.

Another component of Step 1 involves identifying key system stakeholders. This helps in clarifying the systems' organizational components and their role in its operation. This is an important step as it helps identify components of the control structure developed in Step 2 (see Section 4.2.2). Key system stakeholders in the current analysis are:

- Management, including senior and mid-level management and supervisors
- Full-time front-line workers
- Contracted front-line workers
- The public, who rely on affordable and accessible electricity
- Regulators

- Insurers
- Shareholders
- State and federal governments.

While not all stakeholders are represented in the ICS developed in Step 2, it is nonetheless important to identify them and, more importantly, to identify system losses from the perspective of each. Loss identification is another component of STPA Step 1.

Identifying stakeholder values in another component of Step 1. There are at least two ways of going about this: one involves developing a simple list, while another is performing WDA. WDA identifies stakeholder values but goes much further to identify the linkages, across several layers of organizational abstraction, between values and the structure of the work system. This accomplishes objectives in Step 1, greatly facilitates the development of a control structure in Step 2, and provides the analysis team with an early system model.

Figure 20 provides a schematic depiction of the WDA for a generic NPP preventive maintenance system. The three major system purposes identified were maintaining the plant in a sound operating condition, preventing consequential, unplanned equipment failures, and maintaining the design-basis of the plant. In general, stakeholder values were identified as:

- Protecting the health and safety of workers and the public
- Maintaining the functional and structural integrity of the plant
- Optimizing production capability
- Optimizing operational cost-effectiveness
- Optimizing power generation capability.

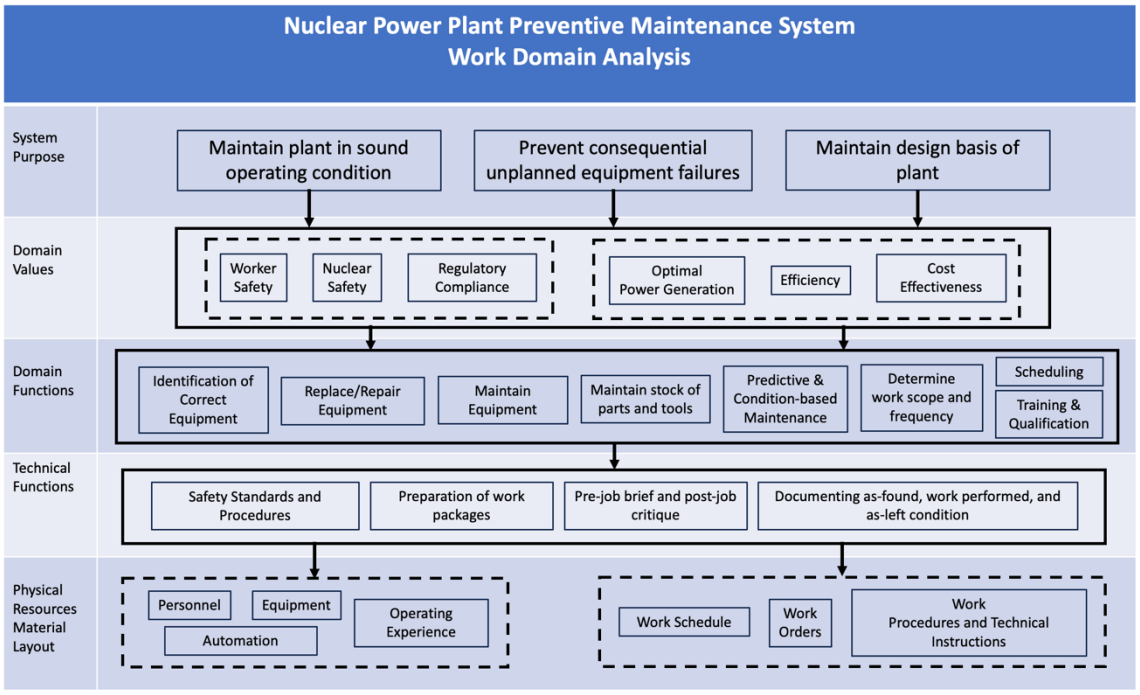

Figure 20. WDA of the preventive maintenance system.

The linkages indicated between these purposes and values across progressively finer levels of abstraction (i.e., down to the level of physical resources and material layout) indicate the highly

interactive relationship between safety, efficiency, and cost-effectiveness within the nuclear energy industry. The WDA also provides important information and insight regarding dependencies and interrelationships between components of the preventive maintenance information control system.

The next objective in STPA Step 1 is to identify system losses. These are directly tied to stakeholder values and describe unacceptable states or conditions for the system. Given the breadth of values listed above, the nature of specific losses can vary widely. For instance, there can be losses associated with injury or loss of life, environmental contamination, financial losses, and loss of reliable electric power. Losses are labeled (e.g., L-1, L-2, etc.) and tracked throughout the full STPA analysis. The system losses identified by the analysis team were:

- Loss of life for workers and/or the public (L-1)
- Loss of plant security (L-2)
- Injuries to workers and/or the public (L-3)
- Environmental contamination and damage (L-4)
- Loss of production capability (L-5)
- Decreased profitability of the operation (L-6)
- Increases in electricity bills (L-7)
- Loss of power to home, business, etc. (L-8)
- Loss of value in shares and dividends (L-9)
- Loss of or damage to equipment (L-10).

STPA analysis now identifies system-level hazards associated with the losses listed above. A system-level hazard is defined as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" (Leveson and Thomas, 2018, 2). The hazards identified by the analysis team, along with the corresponding loss, are:

- H-1: Integrity of core and nuclear fuel diminished (L-1, L-2, L-3, L-4, L-9)
- H-2: Plant releases radiation (L-1, L-2, L-3, L-4, L-9)
- H-3: Plant personnel exposed to unsafe conditions (L-1, L-2, L-3, L-10)
- H-4: Plant experiences unplanned loss of power generation capability (L-5, L-6, L-7, L-8, L-9, L-10)
- H-5: Plant experiences unplanned power outage (L-2, L-3, L-5, L-6, L-7, L-8, L-9, L-10)
- H-6: Plant operates at net loss economically for sustained period (L-5, L-6, L-7, L-9)
- H-7: Damage to equipment (L-4, L-5, L-10).

The final component of STPA Step 1involves the identification of system-level constraints. A system-level constraint specifies system conditions or behaviors that need to be satisfied to prevent hazards (and ultimately prevent losses). Once the system-level hazards are identified, it is straightforward to identify system-level constraints that must be enforced by simply inverting the statement of the hazard:

- SC1: Plant must satisfy conditions for preventing an accidental release of radiation within and outside of the plant's perimeter (H-1, H-2, H-3, H-5)
- SC2: Plant must satisfy conditions (e.g., PPE, training, proper equipment) for a safe and efficient work performance (H-1, H-2, H-3, H-5)
- SC3: Plant must satisfy conditions for preventing (minimizing?) the occurrence of unplanned loss of power generation capability (H-2, H-4, H-5)

- SC4: Plant must satisfy conditions for preventing (minimizing?) the occurrence of unplanned power outages (H-2, H-4, H-5)
- SC5: Plant must operate safely, efficiently, and profitably (H-2, H-5)
- SC6: Plant must implement procedures to minimize damage to equipment (H-3, H-7).

4.2.2 Step 2: Model the Control Structure

The second step in the STPA process involves modeling the control structure. Whereas the CAST analysis modeled an SCS focused on a particular incident as part of its process (see Section 4.1.2), the current STPA models an ICS ultimately focused on the management, planning, and execution of preventive maintenance tasks.

In general, a hierarchical control structure of the sort employed by STAMP contains at least five types of elements (Leveson and Thomas, 2018):

- *Controllers*—In the case of the current analysis, these are entities whose position in the organizational hierarchy requires providing instructions, resources, schedules, etc. to lower-level entities.
- *Control Actions*—Control actions can take several forms, including providing work instructions, schedules, performance expectations, and resources needed for executing the work.
- *Feedback*—While control actions and communication flow down the organizational hierarchy, feedback proceeds from lower-level to higher-level entities and can include information such as the status of specific preventive maintenance tasks, adequacy of instructions and resources to perform the work, and updates and revisions to schedules.
- *Communication Linkages*—Entities that share the same organizational level in the hierarchy, such as senior management, mid-level management and supervisors, and front-line workers, exchange communications that are neither control nor feedback but are nonetheless important in preventive maintenance.
- *Controlled processes*—Ultimately, there is a controlled process whose performance is a function of the activity present within the control structure, which in this study is a generic NPP preventive maintenance system.

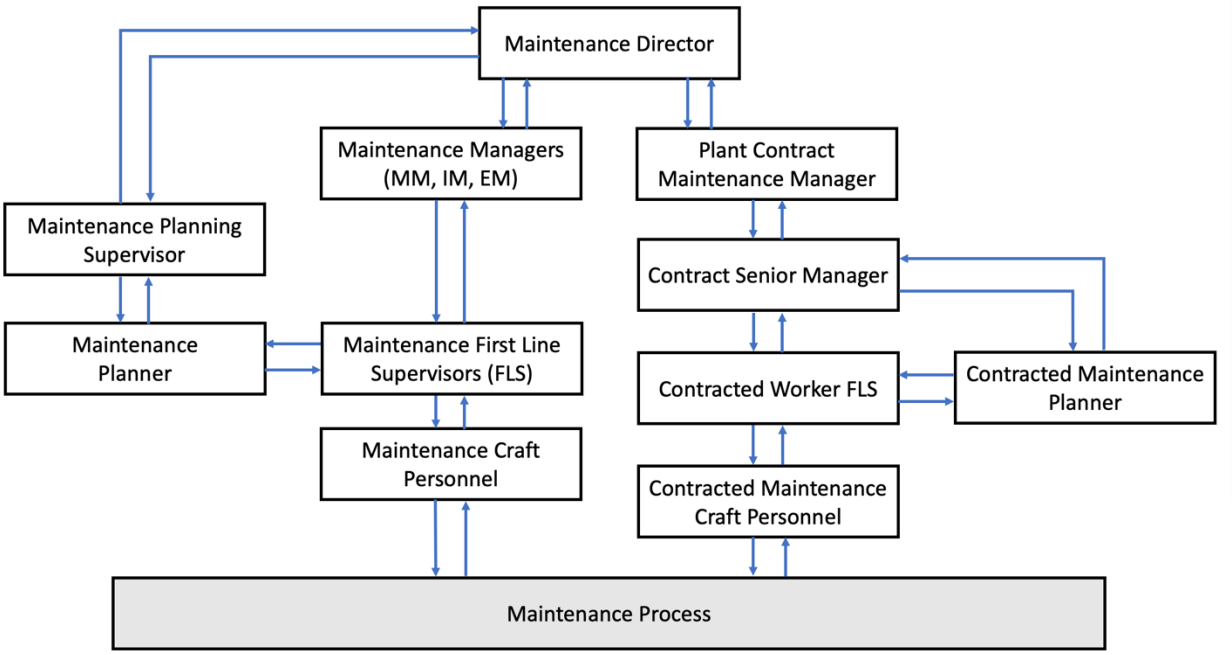

Figure 21. ICS for generic NPP preventive maintenance system.

While the intent of modeling the control structure is to support the identification of ineffective control actions (ICAs) in Step 3, an initial inspection can reveal potential issues very quickly. Figure 21 illustrates the ICS for a generic NPP preventive maintenance system. Downward control arrows indicate actions taken by entities to manage, supervise, and execute maintenance while upward arrows reflect feedback from lower-level entities to their higher-level counterparts concerning such issues as the effectiveness of the control actions, progress made on directed control actions, sufficiency of tools, procedures, etc. to execute the work, and others. Horizontal arrows indicate communication between entities at the same or approximately the same level in the hierarchy.

Specific characteristics of each control, feedback, and communication link will be identified in the next phase of work and will require inputs from industry SMEs to complete. However, Figure 20 reveals that there are no formal communication links in place between full-time maintenance craft personnel and contracted workers who are occasionally brought in to conduct maintenance nor are there communication links between the maintenance first-line supervisor and the contracted worker first-line supervisor. This seemingly creates unnecessary communication and potential performance issues, particularly in situations in which contracted workers may require access to the expertise possessed by the full-time maintenance craft personnel. The absence of communication linkages between these groups represents a potential risk to overall system performance.

4.2.3 Step 3: Identify Ineffective Control Actions

STPA Step 3 focuses on the identification of possible control actions that can potentially create system inefficiencies and, in some cases, contribute to safety risks. The vast majority of work in the STPA field focuses on SCSs and the identification of *unsafe* control actions, actions that can indirectly or directly lead to significant system risks. In the case of the ICS, we described above, we have chosen to initially identify control actions that can lead to *ineffectiveness* in communication and potential result in confusion in the information ecosystem. As we continue to refine the control structure as part of ongoing work, identifying potentially unsafe control actions will become a greater priority.

ICAs were formulated by initially identifying seven general classes of control actions that apply to each of the hierarchically organized pairings of higher-level controller and lower-level controlled processes. These are listed in the first column of Table 5 and are described as:

- *Authority to proceed with work*—A supervisor's approval of a supervisee's work objectives, plans, and processes. Note that supervisor-supervisee relationships exist up and down the control structure, with the defining factor being the supervisor's higher position of authority in the organization relative to the supervisee.
- *Allocation of resources*—Decision-making about the number and type of resources to be dedicated to work performed within the preventive maintenance system is another class of control actions, also largely determined by position within the organizational hierarchy. Resources may include the number and type of personnel assigned to the work, the budget allocated to support the work, tools, and equipment.
- *Scheduling*—Higher-level entities within the system typically have the ability to set and approve schedules related to the performance of lower-level entities' work, including preventive maintenance. Establishing schedules that are subject to time pressure or that conflict with other dependent work schedules are potentially unsafe control actions.
- *Specifying performance objectives and expectations*—This control action relates to formal and informal specification of work-related objectives and expectations. Note that this control action applies to the day-to-day (or thereabouts) performance of specific work activities, as well as the sort of objectives and expectations that are expressed as part of formal, annual employee reviews, etc.
- *Prioritization of work*—Higher-level entities within the system will also typically have the ability to establish work priorities for lower-level entities. This is an important form of control action as it largely establishes the importance attached to specific tasks and the order in which they must be completed, which places important constraints on the decision-making and work of the lower-level entity.
- *Enforcement of work performance standards*—A major responsibility of individuals in a supervisory role within the organization is the enforcement of performance standards on work performed by the personnel for whom they are responsible. This control action places constraints on the possible methods by which preventive maintenance work may be performed.
- *Critique of work performed*—Criticism of work performance is generally viewed as a feedback method, but it can also play an important role in the system as a control action. Specifically, supervisory criticism of work performed by a direct report can exert control over future work performance through the clear specification of what was done properly and improperly and/or what specific aspects of performance need to be improved.

Identifying ICAs was accomplished by examining four different areas of potential ineffective in information delivery. The first involves actions (or lack thereof) in which required information from a controller to a controlled process is not provided. The second involves actions in which information provided by a controller to a controlled process creates inefficiencies. The third identifies control actions in which information is provided by a controller to a controlled process too early, too late, or out of order with other information. Finally, the fourth identifies actions in which the control action is stopped too soon or applied for too long. This fourth class may not apply as much as the other three in the case of an ICS as communications tend to be discrete and not a form of continuous control.

Table 5. STPA ICAs.

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Too Early, Too Late, Out of Order**	**Stopped Too Soon, Applied Too Long**
Authority to proceed with	ICA-1: Supervisor does not authorize	ICA-2: Supervisor authorizes	ICA-4: Supervisor authorizes preventive	N/A

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped Too Soon, Applied Too Long
work	work when preventive maintenance of equipment is required. [H-3, H-4, H-5]	preventive maintenance work that creates schedule and/or resource conflict with other work in plant. [H-3, H-4, H-5] ICA-3: Supervisor authorizes incorrect or out-of-date preventive maintenance work procedure(s). [H-3, H-4, H-5]	maintenance work to be performed out of sequence with other work. [H-3, H-4, H-5] ICA-5: Supervisor does not authorize preventive maintenance before component or system failure. [H-3, H-4, H-5]	
Allocation of resources	ICA-5: Supervisor does not authorize or provide sufficient time, personnel and/or financial resources needed to conduct preventive maintenance work. [H-3, H-4, H-5]	ICA-6: Supervisor allocates insufficient resources needed to conduct preventive maintenance work. [H-3, H-4, H-5]	ICA-7: Supervisor is excessively delayed in authorizing allocation of resources needed to conduct preventive maintenance work. [H-3, H-4, H-5, H-6]	N/A
Scheduling	ICA-8: Supervisor does not provide workers with schedule needed for conduct of preventive maintenance work. [H-3, H-4. H-5, H-6] ICA-9: Supervisor does not distribute schedule to other supervisors within organization with related or overlapping work. [H-3, H-4, H-5, H-6]	ICA-10: Supervisor provides incorrect or unrealistic schedule for preventive maintenance work. [H-3, H-4, H-5, H-6] ICA-11: Supervisor provides schedule for preventive maintenance work with incomplete and/or erroneous information. [H-3, H-4, H-5, H-6]	ICA-12: Supervisor is excessively delayed in providing schedule needed for preventive maintenance work. [H-3, H-4, H-5, H-6] ICA-13: Supervisor provides a preventive maintenance work schedule that overlaps and/or conflicts with one or more other work schedules. [H-3, H-4, H-5, H-6]	N/A
Specifying performance objectives and expectations	ICA-14: Supervisor does not communicate preventive maintenance work performance objectives and	ICA-15: Supervisor imposes excessive and/or unrealistic preventive maintenance work performance objectives and	ICA-16: Supervisor communicates preventive maintenance work performance objectives and expectations to	N/A

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped Too Soon, Applied Too Long
	expectations to lower-level entities. [H-3, H-4, H-5, H-6]	expectations on lower-level entities. [H-3, H-4, H-5, H-6]	lower-level entities after work is completed. [H-3, H-4, H-5, H-6]	
Prioritization of work	ICA-17: Supervisor does not provide lower-level entities with priorities for scheduled preventive maintenance work. [H-3, H-4, H-5, H-6]	ICA-18: Supervisor provides lower-level entities with erroneous priorities for scheduled preventive maintenance work. [H-3, H-4, H-5, H-6]	ICA-19: Supervisor provides lower-level entities with priorities for scheduled work after preventive maintenance work is completed. [H-3, H-4, H-5, H-6]	N/A
Enforcement of work performance standards	ICA-20: Supervisor does not enforce preventive maintenance work performance standards. [H-1, H-2, H-3, H-4, H-5, H-6]	ICA-21: Supervisor enforces preventive maintenance work performance standards that are not relevant to the work being performed. [H-1, H-2, H-3, H-4, H-5, H-6]	ICA-22: Enforcement of preventive maintenance work performance standards is lax and/or inconsistent. [H-3, H-4, H-5, H-6]	N/A
Critique of work performed	ICA-23: Supervisor does not provide feedback or critique of preventive maintenance work performance. [H-1, H-2, H-3, H-4, H-5, H-6]	ICA-24: Supervisor provides critique that is unrelated to the preventive maintenance work performed. [H-1, H-2, H-3, H-4, H-5, H-6]	ICA-25: Supervisor provides critiques of preventive maintenance work performance on inconsistent, irregular basis. [H-1, H-2, H-3, H-4, H-5, H-6]	N/A

Following identifying ICAs, the final component of Step 1 involves identifying controller constraints. These are constraints, translatable into system requirements, on the action of the controller in each ICA to mitigate the chances of its occurrence. Controller constraints are developed in STPA by essentially inverting the ICA description. In each case in Figure 6, the constraint is placed on the design and behavior of the information automation system as opposed to individual personnel.

Table 6. Controller constraints.

ICAs	Controller Constraints
ICA-1: Supervisor does not authorize work when preventive maintenance of equipment is required. [H-3, H-4, H-5, H-6]	C-1: The information automation system must verify that authorization of preventive maintenance work has been granted by the relevant supervisor before work begins. [ICA-1]
ICA-2: Supervisor authorizes preventive maintenance work that creates schedule and/or resource conflict with other work in the plant. [H-3, H-4, H-5]	C-2: The information automation system must verify that newly scheduled preventive maintenance work does not create schedule and/or resource conflicts with other work in the plant. [ICA-2]
ICA-3: Supervisor authorizes incorrect or out-of-date preventive maintenance work procedure(s). [H-3, H-4, H-5]	C-3: The information automation system must provide supervisors and workers with correct and up-to-date work procedures. [ICA-3]: C-4: The information automation system must be automatically updated whenever new procedures are introduced, or existing procedures are modified. [ICA-3]
ICA-4: Supervisor does not authorize or provide sufficient time, personnel, and/or financial resources needed to conduct preventive maintenance work. [H-3, H-4, H-5]	C-5: The information automation system must provide supervisors with guidance on resource requirements for preventive maintenance evolutions. [ICA-4] C-6: The information automation system must verify that sufficient resources have been allocated before preventive maintenance work is performed. [ICA-4]
ICA-5: Supervisor does not authorize preventive maintenance before component or system failure. [H-3, H-4, H-5]	C-7: The information automation system must notify supervisors of the need to authorize preventive maintenance work once deterioration in component and system performance is observed. [ICA-5]
ICA-6: Supervisor allocates insufficient resources needed to conduct preventive maintenance work. [H-3, H-4, H-5]	C-8: The information automation system must provide supervisors with guidance on resource requirements for preventive maintenance evolutions. [ICA-6] C-9: The information automation system must verify that sufficient resources have been allotted to performance of preventive maintenance evolutions. [ICA-6]
ICA-7: Supervisor is excessively delayed in authorizing allocation of resources needed to conduct preventive maintenance work. [H-3, H-4, H-5, H-6]	C-10: The information automation system must provide supervisors with reminders to authorize preventive maintenance work before it is allowed to begin. [ICA-7]

ICAs	Controller Constraints
ICA-8: Supervisor does not provide workers with schedule needed for conduct of preventive maintenance work. [H-3, H-4. H-5, H-6]	C-11: The information automation system must provide supervisors with reminders to provide schedule information to workers before preventive maintenance work can begin. [ICA-8]
ICA-9: Supervisor does not distribute schedule to other supervisors within the organization with related or overlapping work. [H-3, H-4, H-5, H-6]	C-12: The information automation system must identify supervisors with conflicting schedules and notify them. [ICA-9]
ICA-10: Supervisor provides incorrect or unrealistic schedule for preventive maintenance work. [H-3, H-4, H-5, H-6]	C-13: The information automation system must be able to verify that schedules provided by supervisors are correct for each preventive maintenance evolution. [ICA-10] C-14: The information automation system must verify that schedules provided by supervisors are feasible given constraints such as budget and number and type of available personnel. [ICA-10]
ICA-11: Supervisor provides schedule for preventive maintenance work with incomplete and/or erroneous information. [H-3, H-4, H-5, H-6]	C-15: The information automation system must verify that schedules developed by supervisors are complete and do not contain erroneous information. [ICA-11]
ICA-12: Supervisor is excessively delayed in providing schedule needed for preventive maintenance work. [H-3, H-4, H-5, H-6]	C-16: The information automation system must provide supervisors with reminders to provide schedule information in advance of preventive maintenance work. [ICA-12]
ICA-13: Supervisor provides a preventive maintenance work schedule that overlaps and/or conflicts with one or more other work schedules. [H-3, H-4, H-5, H-6]	C-17: The information automation system must verify that schedules provided by supervisors are not in conflict with other projects. [ICA-13]
ICA-14: Supervisor does not communicate preventive maintenance work performance objectives and expectations to appropriate lower-level entities. [H-3, H-4, H-5, H-6]	C-18: The information automation system must verify that preventive maintenance work performance objectives and expectations have been received and acknowledged by appropriate lower-level entities before work proceeds. [ICA-14; ICA-16]
ICA-15: Supervisor imposes excessive and/or unrealistic preventive maintenance work performance objectives and expectations on appropriate lower-level entities. [H-3, H-4, H-5, H-6]	C-19: The information automation must verify that preventive maintenance work objectives and expectations align appropriated with schedule and resources. [ICA-15]
ICA-16: Supervisor communicates preventive maintenance work performance objectives and expectations to lower-level entities after work is	C-18: The information automation system must verify that preventive maintenance work performance objectives and expectations have been received and

ICAs	Controller Constraints
completed. [H-3, H-4, H-5, H-6]	acknowledged by appropriate lower-level entities before work proceeds. [ICA-14; ICA-16]
ICA-17: Supervisor does not provide lower-level entities with priorities for scheduled preventive maintenance work. [H-3, H-4, H-5, H-6]	C-19: The information automation system must verify that adequate information regarding the prioritization of preventive maintenance work has been received and acknowledged by appropriate lower-level entities. [ICA-17]
ICA-18: Supervisor provides lower-level entities with conflicting priorities for scheduled preventive maintenance work. [H-3, H-4, H-5, H-6]	C-20: The information automation system must verify that preventive maintenance work performance priorities do not conflict with other relevant schedules and priorities. [ICA-18]
ICA-19: Supervisor provides lower-level entities with priorities for scheduled work after preventive maintenance work is completed. [H-3, H-4, H-5, H-6]	C-21: The information automation system must verify that preventive maintenance work priorities are received and acknowledged by appropriate lower-level personnel. [ICA-19]
ICA-20: Supervisor does not enforce preventive maintenance work performance standards. [H-1, H-2, H-3, H-4, H-5, H-6]	C-22: The information automation system must notify supervisors when preventive work performance standards are not met and assign an action to address and verify completion of action. [ICA-20]
ICA-21: Supervisor enforces preventive maintenance work performance standards that are not relevant to the work being performed. [H-1, H-2, H-3, H-4, H-5, H-6]	C-23: The information automation system must verify that preventive maintenance work performance standards as specified by supervisors are appropriate for specific tasks and evolutions. [ICA-21]
ICA-22: Enforcement of preventive maintenance work performance standards is lax and/or inconsistent. [H-1, H-2, H-3, H-4, H-5, H-6]	C-24: The information automation system must verify that preventive maintenance work performance standards are received and acknowledged by appropriate lower-level personnel prior to initiating specific tasks and evolutions. [ICA-22]
ICA-23: Supervisor does not provide feedback or critique of preventive maintenance work performance. [H-1, H-2, H-3, H-4, H-5, H-6]	C-25: The information automation system must verify that feedback and critique information has been received and acknowledged by appropriate lower-level personnel following specific tasks and evolutions. [ICA-23]
ICA-24: Supervisor provides critique that is unrelated to the preventive maintenance work performed. [H-1, H-2, H-3, H-4, H-5, H-6]	C-26: The information automation system must verify that supervisor critiques accurately correspond to the actual preventive maintenance tasks and evolutions completed. [ICA-24]

ICAs	Controller Constraints
ICA-25: Supervisor provides critiques of preventive maintenance work performance on inconsistent, irregular basis. [H-1, H-2, H-3, H-4, H-5, H-6]	C-27: The information automation system must verify that supervisor critiques of preventive maintenance work performance are received and acknowledged by appropriate lower-level personnel following the performance of tasks and evolutions. [ICA-25]

4.2.4 Step 4: Identify Loss Scenarios

The final step in the STPA process involves identifying potential loss scenarios or situations in which conditions might cause ICAs to arise. Loss scenarios describe "the causal factors that can lead to the unsafe control actions and to hazards" (Leveson and Thomas, 2018, 42). The value of these scenarios lies in their ability to illuminate aspects of a design that can lead to risk during system operation. These include design features such as missing or problematic control and/or feedback linkages, missing or problematic communication linkages between components that exist at the same organizational level, inadequate or missing design requirements, and other factors. Other classes of loss scenarios are also generated. These include situations in which proper control actions might be provided but are not executed properly, misunderstood, delivered too late, etc., resulting in problems with the execution of subsequent control actions.

The value of generating loss scenarios lies in their usefulness in supporting the identification of system requirements and safety constraints. This is principally due to the exercise of identifying the types of situations in which ICAs might arise and the various sociotechnical influences that gave rise to them.

There are two major questions involved in the development of loss scenarios:

- Why would ICAs occur?
- Why would control actions be improperly executed, or not executed at all, potentially leading to hazards or other issues in the performance of preventive maintenance?

There are several classes of issues examined in this phase of STPA to assist in answering these questions. The first examines ineffective controller behavior, which, in the case of the current analysis, refers to human controllers since we have focused on modeling a control structure comprising organizational components. Issues that arise in loss scenarios may frequently be related to controllers' incomplete or erroneous process models (i.e., mental models) resulting from poor training or, from more of a systems perspective, inadequate, dysfunctional control inputs and/or feedback received from other system components. Inadequate operator process models frequently result in faulty decision-making with subsequent negative impacts across the rest of the system.

The second class of issues examines the influence of inadequate feedback or lateral communication within the system. Feedback may not be generated or received, or it may be provided too late or in a form that cannot be easily comprehended. In any case, the result is likely to be a faulty controller process model. When generating potential loss scenarios that involve inadequate feedback as a potential causal factor, it is important to specify why the feedback might be inappropriate or not useful.

The following examples of loss scenarios were generated using the above guidance, with particular attention paid to factors that might negatively influence workers' process models of the systems they are working with and within. As noted by Leveson and Thomas (2018) and others, problems with the feedback received by controllers and decision makers can become manifest in the form of subsequent faulty decision-making and control actions. The following examples illustrate the potential nature of such problems.

- ICA-2: Supervisor authorizes preventive maintenance work that creates schedule and/or resource conflict with other work in the plant. [H-3, H-4, H-5]

- Scenario 1 for ICA-2: Information regarding potential schedule and resource conflicts is not provided by the information automation system, resulting in an inadvertent authorization of conflicting work.
- Scenario 2 for ICA-2: Correct information regarding potential schedule and resource conflicts is provided by the information automation system, but is misunderstood by supervisor, resulting in inadvertent authorization of conflicting work.

- ICA-23: Supervisor does not provide feedback or critique of preventive maintenance work performance. [H-1, H-2, H-3, H-4, H-5, H-6]
  - Scenario 1 for ICA-23: Supervisor is not aware of the status of preventive maintenance work and its performance.
  - Scenario 2 for ICA-23: Supervisor is provided with inadequate or incomplete information regarding preventive maintenance work performance.

4.3 Proactive Issue Resolution Model Development

As part of PIR model development, and also as part of determining the requirements for an optimized IAE, we have been exploring MIRACLE's ability to identify adverse trends and weak signals from industry condition reports. We have approached this by comparing the results of a MIRACLE-based, custom topic evaluation ("preventive maintenance") with traditional and labor-intensive manual trending of the condition reports provided by a utility. This process is continuing, primarily through manipulating the underlying seed words for the custom topic, and will help shape MIRACLE's capabilities and accuracy as a critical component of the PIR and IAE models and systems. Based on these interactions, we are providing feedback to INL to further enhance MIRACLE as the AI program of choice to evaluate numerous large nuclear data sources.

4.4 Transportable Tool Findings

As discussed above (Section 3.3), our efforts in transportable tool development have focused on the initial development of three potential applications: one focused on modeling and analyzing control structures and two checklists based on themes and findings from the STPA, CAST, HSI, and HFE technical literature.

While our objective is to develop tools that are easy to learn and easy to apply, there is a risk that excessive simplification may lead to an overall loss of effectiveness in identifying existing or potential sociotechnical system risks. To address this risk, future development of these tools will involve working with industry SMEs to refine content and procedures and to produce prototype tools. These tools will then be assessed by comparing the results of their application with those of full-scale control structure, STPA, and CAST analyses of identical systems by experienced analysts. Evaluation criteria will include the scope and nature of the differences observed in the results between the two classes of tools, as well as the time and effort required to use them.

The following sections provide a description of the methods used to model and analyze a control structure and are based on experience working across several industries and applications and lists and descriptions of key themes and findings from the literature that have been selected as potential candidates for inclusion in an incident analysis checklist and a system design analysis checklist.

4.4.1 Control Structure Modeling and Analysis

Modeling and analysis of control structures, whether SCSs, ICSs, or some other form, in the absence of a full STPA or CAST analysis, can nonetheless yield important insights about areas of risk and concern. Often it is relatively (or painfully) clear, once a control structure has been developed, where high-level risks may be present. Missing but important components (organizational or technical) and missing and/or dysfunctional control, feedback, and communication linkages are examples of the types of findings that a relatively simple control structure affords.

Figure 22 provides a highly simplified model of the sort of organizational control structure that can serve as a starting point for adding more detail. The additional detail may take the form of several or multiple entities that exist at the same hierarchical level, whether corporate leadership, middle management and supervisors, or workers, and whose effective communication is important to the purposes of the control structure. Examples of the types of control and feedback information that are commonly observed in hierarchical organizational control structures are also provided in Figure 22. The control structure previously illustrated in Figure 20 is only somewhat more detailed than that in Figure 22, but it illustrates the somewhat more detailed hierarchical and lateral characteristics of an actual control structure. Interestingly, it also clearly illustrates the absence of communication linkages between organizational entities that occupy more or less the same hierarchical level in the system. The absence of such communications should be flagged as a potential risk and addressed as necessary.

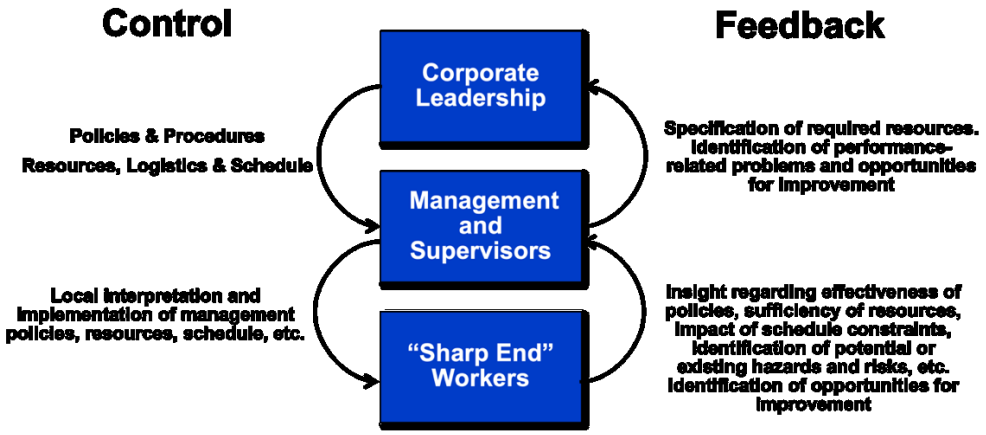

Figure 22. Simplified organizational control structure.

Table 7 identifies the steps involved in a simplified control structure modeling and analysis process. It is important to note that, while Leveson and Thomas (2018) acknowledge that much can be learned from simple modeling, analysis, and discussion of a control structure, the process described below in Table 7 represents a distinct abridgment of the full STPA and CAST approach.

Table 7. Steps in control structure modeling and analysis.

Steps Involved in Simplified Organizational Control Structure Development and Analysis	
Step	**Description**
Assemble analysis team	The makeup of the analysis team is an important influence on the utility and quality of the process. To the greatest extent possible, representatives of stakeholder groups or entities within the system or problem area of concern should be included. One member of the team should serve as facilitator while another serves as recorder.
Define system to be analyzed and system boundaries	The next two steps are components of STPA Step 1 (see Section 4.2.1). The first involves determining the system to be modeled and analyzed, along with identification of the key organizational and technical components to be included. Establishing the system boundary keeps the focus of the analysis on the system of concern and not on external entities over which the team's recommendations will have little or no impact.
Identify losses and hazards of concern	Identical to the processes involved in STPA Step 1. The team must determine the losses (losses in safety, losses in productivity, losses in communication effectiveness, etc.) and hazards of concern to the analysis.

Steps Involved in Simplified Organizational Control Structure Development and Analysis	
Step	**Description**
Identify the system's organizational components	Note that this does *not* mean identifying individuals' names, rather it means identifying relevant organizations.
Arrange components hierarchically, beginning with senior corporate management (see Figure 22)	Ultimately, we are interested in determining how system behavior impacts the performance of work and the management of controlled processes. However, arranging the components hierarchically is done to reflect the fact that in most organizations high-level controls on system behavior begin at the corporate and management levels, and their effects become manifest at subsequent levels (e.g., mid-management and supervisors, "sharp-end" workers).
Depict control, feedback, and communication linkages between system components *as they exist* in the current or planned system	Control actions are depicted with downward arrows from the controller to the entity being controlled. Feedback arrows flow in the opposite direction. Communication arrows between components at the same organization level are depicted as horizontal arrows (see Figure 20). It may become clear at this stage that there are missing components or control, feedback, and communication linkages between components in the current system. However, the goal for most analyses will be to analyze systems *as they are* or *as they are currently planned* and not as they "should be." Developing a control structure of an improved sociotechnical system can be an additional and highly useful exercise, but the initial objective is to analyze the system as it currently exists or as it is currently planned.
Examine control structure	The critical examination of the control structure by the multidisciplinary, multistakeholder analysis team is the next step. Topics for examination include: Are there missing components, for example are there other organizational components that should play a role in the system but currently do not? Are there missing control, feedback, or communication linkages between system components? Are any of the existing control, feedback, or communication linkages unsatisfactory or dysfunctional in some way?
Identify areas for improvement	Having identified any of the issues mentioned above, the final task for the analysis team is to identify areas for improvement. Developing a control structure of the system "as redesigned" is a useful way to accomplish this.
Additional, optional analysis	It can also be useful to develop a control structure of the system "as designed" or "as it supposed to work" and compare it to the control structure of the system as it actually performs. This can be very helpful in identifying areas of needed improvement.

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 the form of performance data, information about the effectiveness of policies and procedures, etc. Problems with dysfunctional or nonexistent feedback links from lower to higher organizational levels, for example, are commonly observed in many organizations and can result in very poor senior-level decision-making due to missing, insufficient, or erroneous

information about the system and its performance.

4.4.2 Method for Investigation of Socio Technical Incidents and Correction

Our initial efforts at developing the MISTIC checklist to support initial sociotechnical system analyses of NPP incidents focused on identifying and organizing common themes and findings from the CAST, HSI, and HFE literature. These themes and findings, listed in Table 8, describe potential sociotechnical and human-system performance issues that CAST and other system analyses have identified as actual or potential causal factors in specific incidents or which present risks to sociotechnical system performance in general.

The sources used to populate Table 8 were identified by searching Google Scholar and the Massachusetts Institute of Technology's (MIT) STAMP Workshop website (http://psas.scripts.mit.edu/home/stamp-workshops/). The latter contains STAMP, CAST, and STPA presentations from MIT's annual STAMP Workshop, from 2012 to the present. These presentations provide a rich source of information across a wide variety of applications, including nuclear energy (e.g., Stephane, 2013).

Table 8. Potential MISTIC items.

Finding or Theme	Description	Setting(s)	Source
Access to updated policies and procedures	Changes in policies and/or procedures that are not adequately communicated or otherwise made available.	Management of electronic medical records	Al-Barnarwi et al. (2019)
Trust in information provided before, during, and after work performance (automation, AI, etc.)	Insufficient confidence in the information provided via automation or AI can result in ineffective decision-making and subsequent actions.	Space flight, multiple	Lordos et al. (2019) Hoff and Bashir (2015) Lee and See (2004) Dekker and Woods (2002) Flach and Voorhorst (2017)
Clarity of boundary between human and machine functions	Confusion with respect to the functions supported by automation, AI, or other system tool versus those supported by humans can result in system errors.	Space flight, air traffic control and navigation, multiple	Lordos et al. (2019) Fitts (1951) Scallen and Hancock (2001) Flach and Voorhorst (2017)
Time pressure	Performance of any kind of work under time pressure is at risk of succumbing to the speed-accuracy tradeoff. Time pressure is a frequent contributor to ineffective and/or unsafe behavior.	Nuclear plant maintenance, air traffic control	Heitz (2015) Joe et al. (2023a) Trapsilawati et al. (2015)
Organizational or supervisory pressure	Excessive or inappropriate pressure to conduct work quickly, inexpensively, etc. from upper levels of an organizational hierarchy has much the same effect as time pressure.	Multiple	Kamran et al. (2022)
Schedule and/or process	Confusion and lack of coordination	Nuclear plant	Joe et al. (2023a)

Finding or Theme	Description	Setting(s)	Source
miscoordination	of contemporaneous work processes can lead to work being performed out of sequence, presenting potential risks.	maintenance, multiple	Johnson (2017)
Inadequate training and experience of personnel	Personnel lack adequate training and/or experience to perform specific tasks and procedures.	Gas line explosion	Li et al. (2020)
Inadequate process model of system	Personnel involved in work process (management, supervisors, and/or workers) do not have an accurate mental model or awareness of the operation and condition of the system being worked upon.	Nuclear plant maintenance, gas line explosion, multiple	Joe et al. (2023a) Li et al. (2020) Rook and Donnell (1993) Flach and Voorhorst (2017)
Inadequate communication	Issues of this type include problems with formal communications, such as work orders and prejob briefings. Also included are the nature of formal and informal communications between system entities during work planning and execution.	Nuclear plant maintenance	Joe et al. (2023a)
Inadequate organizational safety climate	Safety climate can be defined as employees' perception of the relative importance of safety within their organization. Poor safety climates, those in which safety is not perceived as a priority, are associated with an increased likelihood of accidents.	Multiple	Christian et al. (2009) Huang et al. (2017) Read et al. (2019) Dekker (2018)
Differences between formal procedures and informal actions	Tendencies to take "short-cuts" with procedures can, in some instances, contribute to the likelihood of an incident occurring. Note, however, that they can sometimes also reflect greater efficiencies without an associated loss of safety. In these cases, changes to formal procedures may be considered.	Nuclear waste management	Berg et al., 2017
Comprehensibility and usability of human-system interfaces	Problems with the interpretability and usability of human-system interfaces are a frequent precursor of accidents. Confusion and/or excessive frustration in the use of an interface could result in poor decision-making due to an ability to access or comprehend the information presented. This may then result in ineffective or unsafe	Electronic medical records, nuclear, multiple	Zahabi et al. (2015) Jou et al. (2009) Bennett and Flach (1992) Flach and Voorhorst (2017)

Finding or Theme	Description	Setting(s)	Source
	behaviors.		
Presence of ambiguous or overlapping decision-making authority	Confusion regarding conflicting guidance from higher levels of the organizational hierarchy can negatively influence worker decision-making and behavior.	Friendly fire, fratricide	Leveson (2011)
Critical information unavailable or provided too early or late	If task-critical information (e.g., work orders, data displayed on a human-system interface) is not made available in a timely fashion, or at all, then worker decision-making and behavior could be negatively affected.	Multiple	Leveson and Thomas (2018)
Diffusion of responsibility	Lack of clarity regarding responsibility for the conduct of all aspects of the work process (approving, scheduling, managing, executing, etc.) can result in situations in which responsibility "slips through the cracks," resulting in potential system risks.	Social networking, emergency intervention, multiple	Whyte (1991) Martin and North (2015) Darley and Latane (1968)
Asynchronous evolution of people, technology, process, and/or governance	Situations in which, for example, a system's technology is upgraded or changed in some way, but workers' knowledge, skills, and abilities are not, can result in situations in which the value of the technology is not realized and/or human error is a result.	Multiple	Leveson (2011)
Actions or decisions by individuals or groups omitted or performed out of sequence, too soon, or too late	Not performing key tasks at any level of the organizational hierarchy presents system risks. Similarly, work performed out of sequence can lead to confusion, poor decision-making, and ineffective behaviors at lower levels of the hierarchy.	Multiple	Leveson and & Thomas (2018) Johnson (2017)
Actions taken or decisions made on the basis of incomplete, erroneous or misleading information	Decision-making and associated behavior in the partial or complete absence of relevant information can results in system errors and incidents.	Multiple	Reason (1990)
Inaccurate operator/team process model	If organizational entities or personnel at any level of the hierarchy lack an accurate, up-to-date mental model of the operation	Team mental model, tactical decision-	Langan-Fox et al. (2000) Adelman et al. (1986)

Finding or Theme	Description	Setting(s)	Source
	and condition of a particular system under consideration, decision-making and/or subsequent behaviors will be negatively impacted.	making, shared situation awareness	
Organizational failure to enforce proper constraints	System errors make occur if entities at upper levels of the organizational hierarchy do not consistently and appropriately enforce safety constraints on personnel and processes at lower levels.	Gas line explosion, multiple	Li et al. (2020) Leveson (2011)

As described above (Section 3.3, Figure 15), the next step in the process of developing MISTIC will involve translating the findings and themes into checklist form. In essence, the checklist will address whether any of the sociotechnical system influences observed in incidents involving complex systems were present in the incident under analysis. Any issues that are determined to be actually or potentially present can then lead to more detailed examination and incorporation into findings and recommendations stemming from the incident.

4.4.3 Proactive Resolution Of socioTechnical Ecosystem Cause Technique

Our approach to developing PROTECT, a checklist (or similar easy-to-learn, easy-to-use tool) to support initial sociotechnical system analyses of existing or proposed NPP system or subsystem designs was similar to that for MISTIC, the incident analysis checklist. That is, we focused on identifying and organizing common themes and findings from the STPA (as opposed to CAST), HSI, and HFE literature on sociotechnical influences and risk factors in system design. These themes and findings, listed in Table 9, describe potential sociotechnical and human-system performance issues that STPA and other system analyses have identified as risk areas in specific applications or that present risks to sociotechnical system performance in general.

The sources used to populate Table 9 were identified by searching Google Scholar and MIT's STAMP Workshop website (http://psas.scripts.mit.edu/home/stamp-workshops/).

Table 9. Potential PROTECT items.

Finding or Theme	Description	Setting(s)	Source
Trust in information provided before, during, and after work performance (automation, AI, etc.)	Issues involving lack of trust in information provided by automation, AI, etc. can negatively impact decision-making.	Human-robot interaction, space flight, multiple	Hancock et al. (2011) Hoff and Bashir (2015) Lordos et al. (2019) Schaefer et al. (2016)
Joint optimization of people, process, technology, and governance established in design	Joint optimization refers to the relationship between factors such as new technology and corresponding worker knowledge and skill sets. If these are not developed jointly, a mismatch between technical capability and worker knowledge and skill may result.	Space flight, nuclear energy	Lordos et al. (2019) Joe et al. (2023a)
Appropriate	Introducing technologies such as	Space flight,	Lordos et al. (2019)

Finding or Theme	Description	Setting(s)	Source
allocation of function between humans and machine(s)	automation and AI into new or existing sociotechnical systems requires a clear definition of roles and responsibilities for technical systems and for workers. For example, should a human always serve as the decision maker in the system, or will automation or AI serve that function in all or some situations.	flight deck automation, medical AI, multiple	Fitts (1951) Letsu-Dake et al. (2012) Scallen and Hancock (2001) Formosa et al. (2022)
Formal controls on safety within organizational hierarchy	System errors may occur if entities at upper levels of the organizational hierarchy do not consistently and appropriately enforce safety constraints on personnel and processes at lower levels. System design must promote the enforcement on controls on safety.	Rail, medical, multiple	Read et al. (2019) Dekker (2004) Leveson (2011)
End users included in all phases of system design	User-centered design is a vital mitigation technique against the risk of developing or modifying a system such that it does not meet the user's needs, resulting in poorer-than-necessary human-system performance. End users and other system SMEs also have unique insights into the potential risks associated with system design.	Rail, nuclear	Read et al. (2019) Hettinger et al. (2020)
Comprehensibility and usability of human-system interfaces	As described in Table 8, problems with the interpretability and usability of human-system interfaces are a frequent precursor of poorer-than-necessary human-system performance and accidents. Confusion and/or excessive frustration in the use of an interface could result in poor decision-making due to an inability to access or comprehend critical information. The inclusion of human-system interfaces in a system design requires consistent user testing to ensure performance effectiveness.	Multiple	Zahabi et al. (2015) Jou et al. (2009) Bennett and & Flach (1992) Flach and Voorhorst (2017)
Access to updated policies and procedures	Will system entities be able to easily access or be notified of updated work policies and procedures? Determining means for keeping system entities up-to-date on changes that impact them is an important design goal.	Electronic medical records management	Al-Barnarwi et al. (2019)
Clear lines of communications supported	Muddled and/or misdirected communications are often an important causal influence on system ineffectiveness, incidents, etc. Are lines	Multiple	Leveson (2011)

Finding or Theme	Description	Setting(s)	Source
	of communication clear and available, particularly for emergency or unusual conditions?		
Clear responsibilities for decision-making	As noted in Table 8, confusion regarding responsibilities for decision-making can lead to lack of coordination in work activities, wasted efforts, and other issues that impact human-system performance.	Multiple	Leveson (2011)
Employee knowledge, skills, and abilities	In designing a revised or new sociotechnical system, it is important to be clear about the sorts of new knowledge, skills, and abilities employees will need to meet their own and the system's performance objectives.	Information science, multiple	Blackiston (2011)
Sufficient training for employees	The presence of mechanisms and methods to promote effective training is a key attribute of any system under design.	Nuclear, multiple	Hettinger (2003) Muma et al. (1994) Gaddy and Wachtel (1992)

As described above (Section 3.3, Figure 15), the next step in the process of developing PROTECT will involve translating the findings and themes into checklist form. In essence, the checklist will address whether any of the sociotechnical system influences described above might have potential influence on the proposed system under consideration. If so, part of a sociotechnical systems approach to complex systems design is to make sure issues of this sort are addressed as early in the design process as possible. Any issues that are determined to be actually or potentially present can then lead to a more detailed examination and incorporation into findings and recommendations stemming from the incident.

4.5 Preliminary Human-System Design Requirements and Safety Constraints

As a result of the current work, and although there is further R&D to be conducted (see Section 5.7), we feel that we can propose preliminary system-level requirements and safety constraints for a prototype information automation system. Fundamentally, it is essential to specify what information needs to be delivered to whom, when, and in what form. Similarly, it is just as essential to specify what information can be accessed and/or queried by whom, when, and in what form (e.g., graphic user interface and/or conversational interface). Table 10 provides a set of preliminary system-level requirements for an optimized information automation system.

It is also important to specify system safety constraints (i.e., what an optimized information automated system must *not* do and what it must prevent from happening). Table 11 presents a set of preliminary system-level safety constraints for the same system.

In addition to the initial system-level requirements and constraints provided in Table 10 and Table 11, the controller constraints listed and described in Table 6 provides an additional set of 27 system requirements. Finally, STPA Step 1 identified six additional system-level constraints.

Table 10. 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.
3	The system shall provide appropriate plant personnel with suggested actions for addressing the anomalous conditions.
4	The system shall assist in assigning and tracking the status of 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 changes in plant operational, maintenance, design and outage schedules, and processes related to the anomalous conditions.
9	The system shall determine the impact of plant operational, maintenance, design, and outage schedules on other related schedules and processes, determine the nature and likelihood of resulting safety or performance risks, and inform appropriate plant personnel.

Table 11. 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.

Further development of system-level requirements and safety constraints will take place over the next phases of this research effort. Progress on this aspect of the work will continue to be heavily reliant on access to technical expertise related to MIRACLE and DWEP, as well as NPP subject matter expertise from industry partners. A multidisciplinary approach is the most 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 and STPA methods used in prior analyses to include models of process coordination based on STAMP and sociotechnical systems theory in general. We have also proposed two prototype information automation systems whose development will continue in collaboration with the INL MIRACLE research team. Finally, we have initiated the development of easy-to-learn, easy-to-use sociotechnical system analysis methods to facilitate efficient incident analysis and the proactive analysis of existing and proposed system designs.

5.1 Summary of Findings

This section summarizes our findings with regard to each of the major objectives described in Section 2 and examines the findings in light of resilience theory (e.g., Woods, 2015), EID (Vicente, 2002), and their implications for designing information automation systems. We also summarize research conducted to date on the development of transportable tools for sociotechnical incident and systems analyses. The

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

relevance of CAST and STPA findings for developing the PIR and IAE models is also provided, along with a discussion of the research planned for the next phase of this research 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 and STPA of a generic NPP preventive maintenance system. 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 were 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 in 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.

The STPA analysis produced a set of six system-level constraints and 27 system design requirements for an information automation system. These were identified through a process of systems analysis in which the control, feedback, and communication linkages between organizational components of a preventive maintenance system were first identified and then analyzed to identify ineffective ICAs. These ICAs then served as the basis for the initial set of requirements, a set that we expect to be modified as we refine and expand the STPA analysis in the next phases of the research effort. Finally, a simple inspection of the ICS produced as part of the STPA reveals missing communication linkages between key system components that exist at the same levels of the preventive maintenance organizational hierarchy.

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 PIR, while the IAE model supports the development of the broader IAE. 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.

5.1.4 Objective 4: Develop Transportable Tools for Sociotechnical System Analysis

As part of the current effort, we began developing three transportable tools, defined as easily learned and easily deployed sociotechnical system assessment methods for use in NPPs. These include one based on the modeling and analysis of control structures and two based on findings and common themes from the STAMP, STPA, and CAST literature.

Each of the above tools is in an early stage of development, and subsequent work will focus on refinement and, if possible, an onsite assessment of the methods at a partner utility's plant.

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 mechanisms 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. The same may be said of time pressure, another relevant factor in the CAST use case analysis. The well-known "speed-accuracy tradeoff," one of the most universal human performance phenomena, can negatively impact human and organizational performance in numerous ways (e.g., Heitz, 2015).

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 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, 4), where boundaries refer to the limits of safe, effective, and economically viable operations. Resilient systems, therefore, by definition, can effectively handle unanticipated disturbances in the environment that are outside of its design envelope (Woods, 2006). 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, 1).

Resilient systems have specific properties such as *buffering capacity, flexibility, margin,* and *tolerance* (Woods, 2006). Buffering capacity refers to a system's ability to absorb and adapt to disturbances in the environment without compromising the system's basic capabilities. Flexibility means the extent to which a system is capable of restructuring itself in response to external challenges, changes, and perturbances. Margin denotes the proximity between the state of a system's current operation and its performance boundary. Tolerance signifies how a system performs near its performance boundary—does it abruptly or gradually break down as stress to the system increases? Changes external (e.g., economic pressure, geopolitical disturbances) or internal (e.g., poor, or missing feedback loops within the sociotechnical system, mismanagement of goals, poor automation design) to the system are unavoidable, and a system possessing these properties is likely to perform and respond to such changes robustly.

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 23). 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.

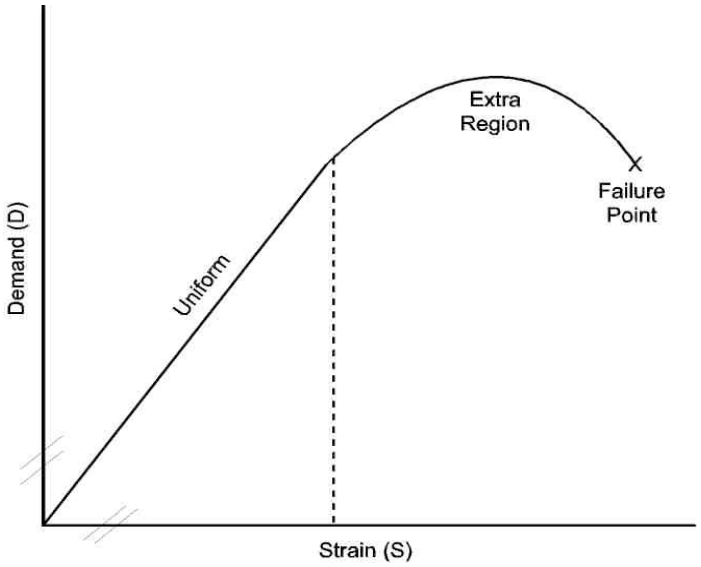

Figure 23. Stress-strain model of resilience (taken from Woods and Wreathall, 2016).

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.

Why would a sociotechnical system become susceptible to disturbances and lose its resilience? One possible reason is the inadequacy or excessive weakening of the SCS underlying the system of concern. If a control action or feedback between a controller and a controlled process is missing, dysfunctional, or otherwise compromised, unsafe control actions may produce a system-level accident. Recently, Johnson (2022) proposed the coordination of multiple decision systems as a critical element that helps control and integrate multiple, interdependent entities in a sociotechnical system. In the discussion of system resilience, the coordination process allows coordination goals, coordination strategy and group decision-

making, increasing the bandwidth of the link between a controller and a controlled process to increase the four features of a resilient system—buffering capacity, flexibility, margin, and tolerance. Note that the coordination process does not simply mean redundant links but functional, bidirectional, and accountable communications between two entities in an organization. In other words, coordination elements involve multiple employees at different skill and authority levels for maintenance work at an NPP, potentially greatly impacting the resilience of the overall system.

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 Ecological Interface Design

One of the current objectives is to support interface design using a user-centered, multidisciplinary team approach while applying relevant sociotechnical system analysis results. The proposed IAE system will require an orchestration of automated systems empowered by cutting-edge technologies such as AI/ML, or so-called *hyperautomation* (Wilson, 2022), to support HSI. The resulting information system will be not only complex but also self-evolving and adaptable to the continuing flow of input from the environment. Human operators will access the computational results via interfaces where they may request certain output from the system such as trend analysis for early detection of equipment failure. However, the interface should follow the human-centered design principle because display designers must represent the complex and evolving data structure and computational results onto displays efficiently.

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. With the rapidly growing complexity of data that represent concrete or abstract quantities via AI/ML capabilities, the development of an interface that supports operators’ mental models appears urgent.

EID (Bennett and 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 useful for developing prototype HSI concepts. One of the key outcomes of CWA is a description of constraints on 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 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 supports later HSI designs. However, EID’s focus is primarily on the workspace, 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 and 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.

One consideration when employing EID to develop an interface for hyperautomation, like the AIE system, is the complexity and dimensionality of generated data to be represented. For example, the

current version of MIRACLE can employ an ML algorithm to generate a one-dimensional representation of the number of documents that reports specific equipment failure by generating a language model of informative topics via Correlational Explanation (Gallagher et al., 2018). Essentially, Correlational Explanation technique allows modeling domain knowledge via a hierarchical cluster of domain-specific words with stronger correlations between each other. Naturally, the modeled knowledge is represented with multiple dimensions that will need to be represented to human users efficiently. Two- or three-dimensional displays, for example, may not be suitable for representing this high-dimensional data. Instead, an ideal EID would allow users to fractalize the display and deep dive into lower-level structures of hierarchically organized data. In short, the EID should allow the ecological representation of multidimensional data in a way that is congruent to the user's mental models.

Conversational AI is a new candidate for a component of EID that has the potential to be incorporated in the IAE system and support the HSI to be more integrated and effective. Conversational AI combines natural language processing (NLP) and ML to streamline interaction between a human and a machine using human language. Conversational AI has the potential to revolutionize the way the human user interfaces with machines and navigates the complex data. For example, a user may request a history of equipment failure data for a certain period of time along with actions taken in a particular NPP via entering the request in a chat box. The user then converses with the AI to visualize the data using a two-dimensional bar graph chart along with NPP performance data, updating the visual display following the EID. Conversational AI thus may support human-AI interaction, or even teaming, within the proposed IAE system. However, there are several caveats to consider when using the currently available conversational AI in EID. First, currently available conversational AI technologies are limited in their ability to fully interpret human queries and retain information beyond a certain number of dialogue. Recent developments such as MemoryGPT might allow GPT to possess "long-term memory" to provide more continuity in human-bot conversations. Second, though conversational AI offers a novel means to interact with AI, it will probably not replace icon-based visual interface because some cognitive tasks that humans perform require mentally integrating pieces of information from different sources. For example, an NPP operator may have to make a decision on effectively allocating limited human resources to address a certain equipment failure in an NPP by coordinating employees at different levels based on acquired data. A decision-making process that requires the assessment of multiple sources of information is complex enough that a simultaneous visual presentation of necessary data organized following the EID would be more effective than a sequential presentation triggered via each verbal query using a bot. Nonetheless, conversational AI is a promising tool to further accelerate the development and use of emerging information ecosystems, such as IAE.

5.5 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, notably MIRACLE, 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.

Our efforts at establishing an ICS for the management, planning, and execution of preventive maintenance, using STPA, have provided us with an initial means to screen inputs from MIRACLE and assess the potential impact of emerging trends on system performance. While MIRACLE, in its current form, does not yet support everything that the PIR and IAE models ask of it, notably closer to real-time trending of plant data, it does provide a means for developing initial models. The development of these models and their transition to functioning systems will continue to be a priority for this research program.

5.6 Evaluation of STPA to Optimize Information Automation

As mentioned previously, one new aspect of this report relative to the research presented previously in Joe et al. (2023a) is that the LWRS Program researchers would develop an evaluation plan and evaluate the effectiveness of using STPA to optimize Information Automation in collaboration with an industry partner. Previous sections of this report, including parts of Section 1, the objectives described in Section 2, and the approach described in Section 3 describe the evaluation plan we developed. This section evaluates the results of our research efforts, which were described in greater detail in Section 4, providing commentary on what work was completed successfully, and what work is still in progress.

As seen in the results described in Section 4, the potential for STAMP and STPA to optimize information automation is high. A key benefit of STPA is that it is a systems-theoretic analytic approach that is a paradigm shift (Kuhn, 1962) from traditional engineering analytic approaches. This paradigm shift in thinking is not, in and of itself, the means to optimize information automation but is a prerequisite because it reveals within the dynamics of the system being analyzed where there are communication breakdowns, bottlenecks, and where situation awareness is poor. The communication issues and instances of poor situation awareness are the opportunities to optimize information automation, and so once they are identified with STPA, digitalization technologies can be applied to optimize information automation and reduce O&M costs.

Additionally, Sections 4.3 and 5.5 described this research's exploration of the use of MIRACLE with STPA to automate aspects of PIR modeling to identify weak, weakening, or nonexistent control structures. Broadly, the potential for AI/ML/NLP to be used in conjunction with human SMEs to reduce the workload of tedious and/or computationally intensive activities is high. This potential was beginning to be seen in the summer of 2023 when LWRS Program researchers for this project met with researchers developing MIRACLE to evaluate the feasibility of using AI/ML/NLP to help the human SME with processing and analyzing CAP condition reports. Exploration of this research topic is on-going, but initial results indicate that using MIRACLE will increase the speed by which STPA analyses can be performed. AI/ML/NLP technologies need further development, however, to be specifically used for this application.

While this research successfully demonstrated the how STAMP and STPA can optimize information automation within the organization of an NPP, and showed how MIRACLE can potentially enhance that effect, STPA still requires human SMEs and is currently somewhat labor intensive. As a result, we also developed transportable tools, such (1) as the step-by-step guidance provided in Table 7 on how to develop a control structure model and perform that analysis, and (2) the MISTIC and PROTECT checklists, which assist in the analysis of organizational error precursors and performance influencing factors for incidents (e.g., MISTIC), and analyses of existing or proposed NPP systems (e.g., PROTECT). These tools enable non-SMEs to perform these analyses more expertly. However, more work is needed to assist with the requisite domain-specific knowledge transfer between SMEs and non-SMEs.

One other activity should also be mentioned in this evaluation. LWRS Program researchers for this project worked with a utility industry partner and a software vendor in the summer of 2023 to create a use-case demonstration of optimizing information automation at an NPP. The use-case successfully demonstrated how information automation could be optimized in two different ways. First, software for a handheld device (i.e., a mobile app) was developed to digitize and digitalize[b] information for a partially

[b] To digitize something is to convert information from an analog format into a digital format, but to digitalize is to use digital technologies to synthesize work processes as a means to integrate operations. See Dainoff et al. (2022).

paper-based reporting process at the utility partner's NPP. This digitalization of the utility's work process was one form of information automation optimization. Second, when the mobile app was developed, industry SMEs helped create the workflow and checklists in the app that enable non-SME users of the app to create reports that were informed by SME domain-specific knowledge, thereby improving the overall quality of the content of the reports. This technology-assisted knowledge transfer between SMEs and non-SMEs is a second kind of information automation. Overall, while further development and refinement of the mobile app is needed, this additional activity proved to be helpful in demonstrating how information automation as a theoretical construct can become realized in a practical tool that digitizes and digitalizes information to jointly optimize workload and situation awareness as a means to improve overall human-system performance and reduce O&M costs. Additional details about this effort can be found in Hall et al. (in press).

5.7 Next Steps

This report has provided a description of our work to support developing an optimized information automation system. The CAST and STPA 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 potentially optimized design.

5.7.1 System-Theoretic Process Analysis Model Refinement

We will continue to refine the STPA modeling and analysis effort described in the current report, specifically with regard to several key objectives. First, we plan to work with NPP industry personnel with expertise in the management, supervision, and execution of preventive maintenance tasks to extend several components of the analysis. These include descriptions of the specific nature of control, feedback, and communication linkages, their purpose, and the types of problems that are observed with them, refinement of existing ICAs and addition of others, refinement and addition of controller constraint, and addition of loss scenarios incorporating control, feedback, communication, and other system performance issues.

In cooperation with MIRACLE and DWEP personnel, we will continue to examine the role that a dynamic ICS will play at the heart of the PIR and IAE models. Of particular concern is determining the type of information that MIRACLE must provide to STPA, how that information would dynamically alter the corresponding control structure, the type of information STPA must provide to DWEP to dynamically alter work platforms and interfaces, and how that information would dynamically alter work platforms and interfaces.

5.7.2 Maturation of Proactive Issue Resolution and Information Automation Ecosystem Models

The intent of this research is to work with the MIRACLE and DWEP system developers to further understand the capabilities of the two models, to best utilize information from MIRACLE, and to push those insights gained from MIRACLE, analyzed using STPA back through the DWEP to help proactively and continuously improve the performance of the utility. Our objectives will be to provide as complete a set of system-level requirements and safety constraints as possible, including those for human-system interfaces, and to develop a prototype PIR model.

MIRACLE's role in these models and eventual systems is to identify adverse trends and weak signals indicative of control structure weaknesses from plant performance data sources, such as internal and external operating experience, CAPs, and work management information, not previously identified using conventional data evaluation methods. Then we will analyze these control structure weaknesses to identify the causes so that corrective actions can be recommended, taken, completed, and verified as effective, and the information ultimately disseminated for use by LWRs, to help improve the overall performance of the rest of the nuclear industry.

In order to further develop this model, we propose conducting knowledge elicitation sessions with a member of the analysis team who is an internationally recognized expert on nuclear safety. The elicitation sessions will focus on uncovering expert sources of knowledge and analytic strategies as they relate to the identification of potential negative trends in system, subsystem, or component performance. This will help to inform MIRACLE's development by providing an expert system model of trend analysis and will also help to refine custom topics and associated seed words.

It is particularly important to involve MIRACLE and DWEP technical expertise, along with industry subject matter expertise, to a greater extent. This type of multidisciplinary input is required to refine the design of the PIR and IAE models, to develop an initial prototype PIR system, 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.

5.7.3 Human and Artificial Intelligence Collaboration

As part of PIR and IAE model development and analysis, as well as prototype system development, we will need to consider factors impacting human-AI teaming. AI serves an important function in both models, serving as a means of accessing and assessing multiple streams of data to produce useful information regarding emerging negative performance trends. However, we do not assume that AI should necessarily "replace the human" in the system. Indeed, it may be much more effective from a systems performance perspective to optimize the collaborative relationship between humans and AI. This will be an important area of emphasis in our forthcoming work.

Emerging technologies, such as AI and ML, are likely to serve as key drivers for NPP modernization and the development of the IAE and will revolutionize the way humans work in technological and professional environments. These technologies will enable autonomy, which is conceptualized as a multifaceted construct that is viable in a defined environment, independent to perform without assistance from other agents such as humans, and self-governing to define goals and strategize to accomplish the goals (Kaber, 2018).

Recent HFE researchers define and emphasize the importance of human-autonomy teaming (HAT; O'Neill et al., 2022; Lyons et al., 2021). For example, O'Neill and colleagues (2022) define HAT as "interdependence in activity and outcomes involving one or more humans and one or more autonomous agents" where autonomous agents are powered by advanced digital technologies, such as AI. HAT has been increasingly considered in various areas including space exploration (e.g., NASA Ames Roverscape; Kaber, 2018), military (e.g., royal wingman; Layton, 2021; Chen et al., 2018), healthcare (Suhan et al., 2019), driving (Kridalukmana et al., 2020), logistics (Zhang et al., 2020), and finance (Wilson, 2022). As AI quickly evolves to be an autonomous agent and teammate for humans, human trust toward the autonomous agent powered by AI is a critical construct to enable the social integration of AI and streamline and facilitate interactions between humans and AIs (Abbass, 2019; McNeese et al., 2021; Demir et al., 2021). Another characteristic that is likely to affect the relationship between humans and AIs is communication and coordination (Johnson et al., 2021). In the context of NPP modernization and the IAE, trust and communication between humans and AIs should be a future research focus to optimize the collaborative relationship between humans and AIs.

5.7.4 Human-System Interface Development

The development of prototype human-system interface concepts for use in conjunction with the PIR and IAE models and subsequent systems will also be addressed in the next phase of work. The outcome of the CAST and STPA analyses, such as the Controller Constraints described in Section 4.2.3, have provided initial guidance on requirements for interfaces with users. As described in Section 5.4, our intent is to pursue EID as a method for human-system interface development.

Having been previously applied in the nuclear domain (e.g., Vicente and Rasmussen, 1992), we will revisit the method in light of new insights from the nuclear energy field as well as other process control and safety-critical applications. Of particular interest are conversational interfaces, as these may permit the most natural and effective means of querying complex data within the IAE.

5.7.5 Refinement of Transportable Tools

The next stage of development for the transportable tool concepts described in this report will involve several components. We will begin by presenting the three tools in their current state to a group of three to six industry SMEs with expertise in incident and systems analysis. Our goals in these sessions will first be to validate the need for and potential utility of tools of this nature. We will then ask the group to critique the materials presented in Sections 4.4.1–4.4.3, such as the instructions provided for modeling and analyzing control structures. We will also ask participants to critique the relevance of themes and findings from Sections 4.4.2–4.4.3 to NPP settings, suggest additional themes, and then rank the remaining themes in terms of their relevance to NPP concerns.

Following this step, we will revise the materials into a "Version 1" form of the tools, including training materials on their use. We will request that our industry SMEs, already familiar with the objectives of the project, again critique the materials, this time for comprehensibility and ease of use.

Once updates have been made to the tools and training materials based on feedback received, we propose conducting a more formal evaluation. Specifically, we propose testing the performance of MISTIC versus a full CAST analysis of the same representative NPP incident. Similarly, we proposed testing the performance of PROTECT versus a full STPA analysis of an existing or proposed NPP system or subsystem design. Evaluation criteria will include measures such as the number of useful findings obtained by the transportable tools versus those found by full analyses, the time and resources required to obtain the findings, and the time and resources needed to train personnel on the use of the tools.

5.7.6 Approach

We propose accomplishing much of the above 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 24 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 stove-piped 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 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.

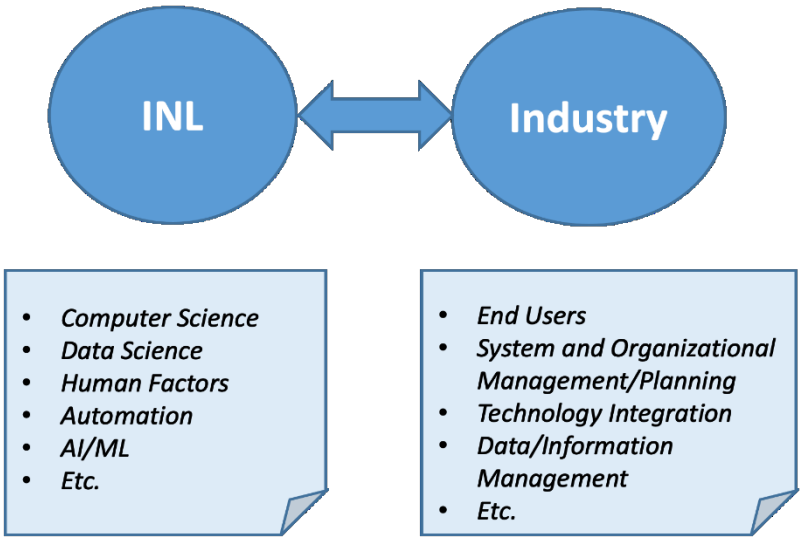

Figure 24. Elements of a multidisciplinary, user-centered design.

6. CONCLUSIONS AND RECOMMENDATIONS

The following sections describe conclusions and recommendations from the current effort, including a discussion of the implications of our 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 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.
- The requirements and constraints generated to date by the STPA analysis provide initial guidance on the design of an optimized information automation system. Similarly, the analysis of the ICS suggests areas of concern related to “lateral” communications between entities at the same level of the system hierarchy. This suggests an area of concern to be addressed by information automation design.

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

INPO provides a database that allows member organizations such as nuclear utilities to share events and issues as operating experience, in order to improve NPPs through continuous learning. This database is called the Industry Reporting and Information System. As all U.S. NPPs are bound by the regulations set forth by the NRC and guidelines enforced by INPO, there are factors that affect all U.S. NPPs. Based on our research so far, we have seen some common themes that appear to have the same impact on the performance of unrelated plants from different utilities. After reviewing events from one plant and comparing them to plants from other utilities, as well as reviewing all events reported to the NRC through licensee reporting, we are beginning to see common sociotechnical design issue flaws that appear to affect all plants. This raises a couple of questions: Are current regulatory enforcement methods inadvertently causing utilities to design sociotechnical flaws into their plants' highest-level control structures? Did utilities respond to these regulations and guidelines 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 regulators and nuclear plants can utilize this process to both improve the resilience of their control structures 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 an 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.
- The STPA analysis resulted in the identification of 27 unique system design requirements and constraints. In many cases, these represent opportunities for advanced automation and AI support, and some may have strong dependencies on the availability and functionality of such technologies. Additionally, an inspection of the control structure developed as part of the analysis revealed a concerning absence of formal communication linkages between organizational components at the same hierarchical levels of the system. Continued refinement of this analysis in the next phases of this research will result in the identification of additional system requirements and constraints, as well as additional opportunities for the incorporation of automation and AI.
- The development of valid and reliable transportable assessment tools will support nuclear modernization by making it possible to analyze the influence of sociotechnical system factors on incidents and potential influence on existing and future designs in a manner that can be efficiently learned and used by NPP employees.

These findings 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 model, 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

Abbass, H. A. (2019). "Social integration of artificial intelligence: functions, automation allocation logic and human-autonomy trust." *Cogn Comput* 11(2), 159-171. https://doi.org/10.1007/s12559-018-9619-0.

Adelman, L., Zirk, D. A., Lehner, P. E., Moffett, R. J., and Hall, R. (1986). "Distributed tactical decisionmaking: Conceptual framework and empirical results." *IEEE Transactions on Systems, Man, and Cybernetics* 16(6), 794-805. https://doi.org/10.1109/TSMC.1986.4308998.

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, *Sage Journals* 11(2), 175–201. https://doi.org/10.1177/2041386621992105.

ANSI/HFES (2021). "Human Readiness Level Scale in the System Development Process." American National Standards Institute and Human Factors and Ergonomics Society, ANSI/HFES-400-2021. https://www.hfes.org/Portals/0/Documents/DRAFT%20HFES%20ANSI%20HRL%20Standard%201_2_2021.pdf?ver=2021-01-06-142004-860&timestamp=1609964482681.

Bar-Or, L. and Hartmann, D. (2023). "Unifying Defense in Depth (Did) in the Nuclear Industry and Stamp System Safety Model." *SSRN Electronic Journal*. https://dx.doi.org/10.2139/ssrn.4330171.

Bennett, K. and Flach, J. M. (2011). *Display and Interface Design*. 1st edition, Boca Raton, FL: CRC Press. https://doi.org/10.1201/b10774.

Bennett, K. B. and Flach, J. M. (1992). "Graphical displays: Implications for divided attention, focused attention, and problem solving." *Human Factors*, 34(5), 513-533. https://doi.org/10.1177/001872089203400502.

Blakiston, R., (2011). "Building knowledge, skills, and abilities: Continual learning in the new information landscape." *Journal of Library Administration*, 51(7-8), 728-743. http://dx.doi.org/10.1080/01930826.2011.601272.

Booher, H. R. (2003). *Handbook of Human Systems Integration*. New York City, NY: Wiley & Sons, [Online]. 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." *Journal of Mathematical Sociology* 31(2), 121–147. https://doi.org/10.1080/00222500601188056.

Checkland, P. (1981). *Systems Thinking, Systems Practice*. Chichester, UK: John Wiley and Sons.

Chen, J. Y. C., Lakhmani, S. G., Stowers, K., Selkowitz, A. R., Wright, J. L., and Barnes, M. (2018). "Situation awareness-based agent transparency and human-autonomy teaming effectiveness." *Theoretical issues in Ergonomics Science*, 19(3), 259-282. https://doi.org/10.1080/1463922X.2017.1315750.

Dainoff, M., Hettinger, L., Hanes, L., and Joe. J. C. (2020). "Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology." INL/EXT-20-57908-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://doi.org/10.2172/1615671.

Dainoff, M., Hettinger, L., Hanes, L., and Joe, J. C. (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)*, (virtual) Providence, RI: 162-170. https://doi.org/10.1080/00295450.2022.2138065.

Dainoff, M. J., Hettinger, L. J., and Joe, J. C. (2022). "Using Information Automation and Human Technology Integration to Implement Integrated Operations for Nuclear." INL/RPT-22-68076-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://doi.org/10.2172/1879683.

Dainoff, M. J., Murray, P. J., Joe, J. C., Hall, A., Oxstrand, J., Hettinger., L. J., Yamani, Y., and Primer, C. A. (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-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://doi.org/10.2172/1894897.

Darley, J. M. and Latané, B. (1968). "Bystander intervention in emergencies: diffusion of responsibility." *Journal of Personality and Social Psychology*, 8(4, Pt 1), 377-383. https://psycnet.apa.org/doi/10.1037/h0025589.

Dekker, H. C. (2004). "Control of inter-organizational relationships: evidence on appropriation concerns and coordination requirements." *Accounting, Organizations and Society*, 29(1), 27-49. https://doi.org/10.1016/S0361-3682(02)00056-9.

Dekker, S. (2018). *Just culture: restoring trust and accountability in your organization, 3rd Edition*. New York: CRC Press. http://dx.doi.org/10.1201/9781315590813.

Dekker, S. W. A. and Woods, D. D. (2002). "MABA-MABA or abracadabra? Progress on human–automation co-ordination." *Cognition Tech Work*, 4, 240-244. https://doi.org/10.1007/s101110200022.

Demir, M., McNeese, N. J., Gorman, J. C., Cooke, N. J., Myers, C. W., and Grimm, D. A. (2021). "Exploration of teammate trust and interaction dynamics in human-autonomy teaming." *IEEE Transactions on Human-Machine Systems*, 51(6), 696-705. https://doi.org/10.1109/THMS.2021.3115058.

Fitts, P. M. (1951). "Human engineering for an effective air-navigation and traffic-control system." Washington, DC: National Research Council, 1-109. https://apps.dtic.mil/sti/citations/ADB815893.

Flach, J. and Voorhorst, F., (2016). *What matters? Putting common sense to work*. Dayton, OH: *Wright State University Libraries*. https://corescholar.libraries.wright.edu/books/127/.

Formosa, P., Rogers, W., Griep, Y., Bankins, S., and Richards, D. (2022). "Medical AI and human dignity: Contrasting perceptions of human and artificially intelligent (AI) decision making in diagnostic and medical resource allocation contexts." *Computers in Human Behavior*, 133, 107296. https://doi.org/10.1016/j.chb.2022.107296.

Gaddy, C. D. and Wachtel, J. A. (1992). "Team skills training in nuclear power plant operations." In R. W. Swezey and E. Salas (Eds.), *Teams: Their training and performance* (pp. 379–396). Norwood, NJ: Ablex Pub. Corp.

Gallagher, R. J., Reing, K., Kale, D., and Ver Steeg, G. (2017). "Anchored correlation explanation: Topic modeling with minimal domain knowledge." *Transactions of the Association for Computational Linguistics*, 5, 529-542. https://doi.org/10.1162/tacl_a_00078.

Hall, A., Miyake, T., Joe, J., Spielman, Z., and Oxstrand, J. (in press). "Digitalization guiding principles and method for nuclear industry work processes." INL/RPT-23-74429-Rev000, Idaho National Laboratory, Idaho Falls, ID.

Hancock, P. A., Billings, D. R., Schaefer, K. E., Chen, J. Y. C., de Visser, E., and Parasuraman, R. (2011). "A meta-analysis of factors affecting trust in human–robot interaction." *Human Factors*, 53(5), 517–527. https://doi.org/10.1177/0018720811417254.

Heitz, R. P. (2014). "The speed-accuracy tradeoff: history, physiology, methodology, and behavior." Front Neurosci, 8, p.150. https://doi.org/10.3389/fnins.2014.00150.

Hettinger, L. (2003). "Integrating training into the design and operation of complex systems." In H. R. Booher (Ed.) *Handbook of human-systems integration*. New York, NY: Wiley-Interscience. https://www.wiley.com/en-us/Handbook+of+Human+Systems+Integration+-p-9780471020530.

Hettinger, L. J., Kirlik, A., Goh, Y. M., 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. C. (2020). "Guidance on Including Social, Organizational, and Technical Influences in Nuclear Utility and Plant Modernization Plans." INL/EXT-20-60264-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://doi.org/10.2172/1696804.

Hoff, K. A. and 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.

Huang, Y. H., Jeffries, S., Tolbert, G. D., and Dainoff, M. J. (2017). "Safety climate: How can you measure it and why does it matter?" *Prof. Safety*, 62(1), 28-35. https://onepetro.org/PS/issue/62/01 or https://onepetro.org/PS/article-abstract/62/01/28/33529/Safety-Climate-How-Can-You-Measure-It-and-Why-Does?redirectedFrom=fulltext.

Hunton, P. J., England, R. T., 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, Idaho Falls, ID. https://doi.org/10.2172/1660976.

Joe, J. C., Hettinger, L., Dainoff, M., Murray, P., and Yamani, Y. (2023a). "Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis." INL/RPT-23-73099-Rev000, Idaho Falls: Idaho National Laboratory. https://doi.org/10.2172/1988134.

Johnson, C. J., Demir, M., McNeese, N. J., Gorman, J. C., Wolff, A. T., and Cooke, N. J. (2021). "The impact of training on human–autonomy team communications and trust calibration." *Human factors*, 0(0), 187208211047323, PMID: 34595958. https://doi.org/10.1177/00187208211047323.

Johnson, K. (2017). "Extending Systems-Theoretic Safety Analyses for Coordination." MIT PhD Dissertation. http://psas.scripts.mit.edu/home/wp-content/uploads/2017/05/Johnson_STPA-Coord_STAMP-17-Release-No.-17139.pdf

Johnson, K. and Leveson, N. G. (2014). "Investigating Safety and Cybersecurity Design Tradespace for Manned-Unmanned Aerial Systems Integration Using Systems Theoretic Process Analysis." *GI-Jahrestagung,* 643-647. https://api.semanticscholar.org/CorpusID:17848173.

Jou, Y.-T., Yenn, T.-C., Lin, C. J., Yang, C. W., and Chiang, C.-C. (2009). "Evaluation of operators' mental workload of human–system interface automation in the advanced nuclear power plants." *Nuclear Engineering and Design*, 239(11), 2537-2542. https://doi.org/10.1016/j.nucengdes.2009.06.023

Kamran, K., Azam, A., and Atif, M. M. (2022). "Supervisor bottom-line mentality, performance pressure, and workplace cheating: moderating role of negative reciprocity." Front. Psychol., 13, 801283. https://doi.org/10.3389/fpsyg.2022.801283.

Khan, M., Mehran, M. T., Haq, Z.U., Ullah, Z., Naqvi, S.R., Ihsan, M., and Abbass, H. (2021). "Applications of artificial intelligence in COVID-19 pandemic: A comprehensive review." *Expert Syst Appl.*, 185, 115695. https://doi.org/10.1016/j.eswa.2021.115695.

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-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://lwrs.inl.gov/Advanced%20IIC%20System%20Technologies/InnovationToolSet.pdf

Kridalukmana, R., Lu, H. Y., and Naderpour, M. (2020). "A supportive situation awareness model for human-autonomy teaming in collaborative driving." Theoretical Issues in Ergonomics Science, 21(6), 658-683. https://doi.org/10.1080/1463922X.2020.1729443.

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.

Kuhn, T. (1962). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Langan-Fox, J., Code, S., and Langfield-Smith, K. (2000). "Team mental models: Techniques, methods, and analytic approaches." *Human factors*, 42(2), 242-271. https://doi.org/10.1518/001872000779656534.

Larsson, S., and Heintz, F. (2020). "Transparency in artificial intelligence." *Internet Policy Review*, 9(2). http://dx.doi.org/10.14763/2020.2.1469.

Layton, P. (2021). "Fighting artificial intelligence battles: Operational concepts for future AI-enabled wars." Australian Government, Department of Defence, 4(20), 1-100. https://tasdcrc.com.au/wp-content/uploads/2021/02/JSPS_4.pdf.

Lee, J. D. and See, K. A. (2004). "Trust in automation: Designing for appropriate reliance." *Human factors*, 46(1), 50-80. https://doi.org/10.1518/hfes.46.1.50_30392.

Letsu-Dake, E., Rogers, W., Dorneich, M.C. and De Mers, R., (2012). "Innovative flight deck function allocation concepts for NextGen." In: S. J. Landry (Ed.), *Advances in Human Aspects of Aviation*, 301-310, CRC Press. https://doi.org/10.1201/b12321.

Leveson, L., Malmquist, S., and Wong, L. (2021). "CAST Tutorial: How to Learn More from Accidents." https://www.youtube.com/watch?v=bFRX32YFKGU

Leveson, N. (2011). *Engineering a Safer World*. Cambridge, MA: MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001.

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, N. and Thomas, J. (2018). "STPA Handbook." https://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.

Lordos, G. C., Summers, S. E., Hoffman, J. A., and De Weck, O. L., (2019). "Human-Machine Interactions in Apollo and Lessons Learned for Living off the Land on Mars." In proceedings of the *2019 IEEE Aerospace Conference,* Big Sky, MT: pp. 1-17. https://doi.org/10.1109/AERO.2019.8741618.

Lyons, J. B., Sycara, K., Lewis, M., and Capiola, A. (2021). "Human–autonomy teaming: Definitions, debates, and directions." *Front. Psychol*., 12, 589585. https://doi.org/10.3389/fpsyg.2021.589585.

Martin, K. K., and North, A. C. (2015). "Diffusion of responsibility on social networking sites." *Computers in Human Behavior*, 44, 124-131. https://doi.org/10.1016/j.chb.2014.11.049.

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

McNeese, N. J., Demir, M., Chiou, E. K., and Cooke, N. J. (2021). "Trust and team performance in human–autonomy teaming." *International Journal of Electronic Commerce*, 25(1), 51-72.

https://doi.org/10.1080/10864415.2021.1846854.

Mumaw, R. J., Swatzler, D., Roth, E. M., and Thomas, W. A. (1994). "Cognitive skill training for nuclear power plant operational decision making." (No. NUREG/CR-6126). Nuclear Regulatory Commission, Washington, DC, USA: Div. of Systems Research; Westinghouse Electric Corp., Pittsburgh, PA, USA. https://doi.org/10.2172/10161883.

O'Neill, T., McNeese, N., Barron, A., and Schelble, B. (2022). "Human–autonomy teaming: A review and analysis of the empirical literature." *Human factors*, 64(5), 904-938. https://doi.org/10.1177/0018720820960865.

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*, 119(1), 25-33. https://doi.org/10.1111/j.0028-1425.2007.00001.x.

Rasmussen, J., Pejtersen, A. M., and Goodstein, L. P. (1994). "Cognitive Systems Engineering." New York City, NY: Wiley. in *J. Multi-Crit. Decis. Ana*., 5(1) (1996):75-75. https://doi.org/10.1002/(SICI)1099-1360(199603)5:1%3C75::AID-MCDA92%3E3.0.CO;2-4.

Reason, J. (1990). *Human Error*. Cambridge University Press. https://doi.org/10.1017/CBO9781139062367.

Rook, F. W., and Donnell, M. L. (1993). "Human cognition and the expert system interface: Mental models and inference explanations." In *IEEE Transactions on Systems, Man, and Cybernetics*, 23(6), 1649-1661. https://doi.org/10.1109/21.257760.

Rouse, W. B. (2010). *The Economics of Human System Integration*. Hoboken, NJ: Wiley. https://doi.org/10.1002/9780470642627.

Scallen, S. F., and Hancock, P. A. (2001). "Implementing adaptive function allocation." *The International Journal of Aviation Psychology*, 11(2), 197-221. https://doi.org/10.1207/S15327108IJAP1102_05.

Schaefer, K. E., Chen, J. Y. C., Szalma, J. L., and Hancock, P. A. (2016). "A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems." *Human factors*, 58(3), 377-400. https://doi.org/10.1177/0018720816634228.

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

Stephane, L. (2013). "Analysis of the Fukushima disaster: Reinforcement for using STAMP as a vector of safety governance." *MIT STAMP Workshop*. Accessed at: https://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/02_Stephane_STAMP_2013.pdf.

Sujan, M., et al. (2019). "Human factors challenges for the safe use of artificial intelligence in patient care." *BMJ Health & Care Informatics*, 26(1), 100081. http://dx.doi.org/10.1136/bmjhci-2019-100081.

Tate, C. C., Estes, T., Hagan, J., 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(23), 2041-2044. https://doi.org/10.1177/154193120504902309.

Thomas, K. and Hunton, P. (2019). "Nuclear Power Plant Modernization Strategy and Action Plan." INL/EXT-19-55852-Rev000, Idaho National Laboratory, Idaho Falls, ID. https://lwrs.inl.gov/Advanced%20IIC%20System%20Technologies/NPP_Modernization_Strategy_Action_Plan.pdf.

Trapsilawati, F., Qu, X., Wickens, C. D., and Chen, C. H. (2015). "Human factors assessment of conflict resolution aid reliability and time pressure in future air traffic control." *Ergonomics*, 58(6), 897-908.

https://doi.org/10.1080/00140139.2014.997301.

Vicente, K. J. (2002). "Ecological interface design: Progress and challenges." *Human Factors*, 44(1), 62-78. https://doi.org/10.1518/0018720024494829.

Vicente K. J. and Rasmussen, J. (1992). "Ecological interface design: Theoretical foundations." *IEEE Transactions on Systems, Man, and Cybernetics*, 22(4), 589-606. https://doi.org/10.1109/21.156574.

von Bertalanffy, L. (1968). "General Systems Theory: Foundations, Development and Applications." New York, NY: *George. Braziler, Inc*. https://monoskop.org/images/7/77/Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf.

Wahlstrom, B. (2004). "Challenges in the Nuclear Industry: Perspectives from Senior Managers and Safety Experts." in N. Itoigawa, B. Wilpert, and B. Fahlbruch, (Eds.), *Emerging demands for the safety of nuclear power operations,* Boca Raton, FL: CRC Press, 17-29. https://www.researchgate.net/publication/313470238_Challenges_in_the_nuclear_industry_perspectives_from_senior_managers_and_safety_experts.

Waterman, D. A., (1985). *A guide to expert systems*. Addison-Wesley Longman Publishing Co., Inc. https://dl.acm.org/doi/abs/10.5555/4131.

Whitworth, B. (2009). "A brief introduction to sociotechnical systems." *In Encyclopedia of Information Science and Technology, Second Edition,* edited by Mehdi Khosrow-Pour, D.B.A., 394-400. Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-60566-026-4.ch066.

Whyte, G. (1991). "Diffusion of responsibility: Effects on the escalation tendency." *Journal of Applied Psychology*, 76(3), 408-415. https://psycnet.apa.org/doi/10.1037/0021-9010.76.3.408.

Wilson, J. R. (2014). "Fundamentals of system ergonomics/human factors." *Applied Ergonomics,* 45(1), 5–13. https://doi.org/10.1016/j.apergo.2013.03.021.

Wilson, R. (2022). *The Age of Invisible Machines*. New York: Wiley, ISBN: 978-1-119-89992-1. https://www.wiley.com/en-us/Age+of+Invisible+Machines:+A+Practical+Guide+to+Creating+a+Hyperautomated+Ecosystem+of+Intelligent+Digital+Workers-p-9781119899921.

Woods, D. D. (2015). "Four Concepts for Resilience and their Implications for the Future of Resilience Engineering." *Reliability Engineering and System Safety,* 141, 5–9, ISSN 0951-8320. https://doi.org/10.1016/j.ress.2015.03.018.

Woods, D. 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-1.pdf.

Woods, D. D. (2006). *Resilience Engineering: Concepts and Precepts*. E. Hollnagel, Ed. (1st Edition), CRC Press. https://doi.org/10.1201/9781315605685.

Woods, D. D., and Wreathall, J & Company. (2003). "Managing Risk Proactively: The Emergence of Resilience." https://www.researchgate.net/publication/228711828_Managing_Risk_Proactively_The_Emergence_of_Resilience_Engineering.

Yousefi, A. and Hernandez, M. R. (2019). "Using a system theory based method (STAMP) for hazard analysis in process industry." *Journal of Loss Prevention in the Process Industries*, 61, 305-324. https://doi.org/10.1016/j.jlp.2019.06.014.

Zahabi, M., Kaber, D. B., and Swangnetr, M. S. (2015). "Usability and safety in electronic medical records interface design: a review of recent literature and guideline formulation." *Human factors*, 57(5), 805-834. http://dx.doi.org/10.1177/0018720815576827.

Zhang, M., Zhang, D., Yao, H., and Zhang, K., (2020). “A probabilistic model of human error assessment for autonomous cargo ships focusing on human–autonomy collaboration.” *Safety Science*, 130(3), 104838. http://dx.doi.org/10.1016/j.ssci.2020.104838.

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.

Zhao, S., Blaabjerg, F., and Wang, H. (2020). “An overview of artificial intelligence applications for power electronics.” in *IEEE Transactions on Power Electronics*, 36(4), 4633-4658. https://doi.org/10.1109/TPEL.2020.3024914.

Appendix A
Draft Research Summary Article

Briefing Paper

Author: Jeffrey C. Joe

August 30, 2023

LWRS LIGHT WATER REACTOR SUSTAINABILITY

System-Theoretic Process Analysis Based Tools to Optimize Information Automation

Problem Statement

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.

Solution

Light Water Reactor Sustainability (LWRS) Program researchers have developed tools and techniques to support effective modernization from a system-theoretic and human-systems integration point of view, specifically with regard to information automation.

Background

LWRS Program researchers have developed and employed a method to design an optimized information automation ecosystem (IAE) based on 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, feedback, and communication relationships among the system's technical and organizational components. We have employed two STAMP-based tools in this effort. The first is Causal Analysis based on STAMP (CAST), an accident and incident analysis technique used to examine a performance- and safety-related incident at an industry partner's plant involving 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. The second tool is Systems-Theoretic Process Analysis (STPA), which is a proactive risk analysis tool used to examine existing and potential, planned sociotechnical systems. STPA was used to identify risk factors in the current design of a generic NPP preventive maintenance system. Our analyses focused on identifying near-term system improvements and longer-term design requirements for an optimized IAE system.

Results

Two preliminary information automation models were developed. 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 and represents an end-state vision for our work. From our results, we have generated an initial set of preliminary system-level requirements and safety constraints for these models.

Tools

A number of easy-to-learn, easy-to-use "transportable" tools for sociotechnical systems analyses have been developed based on the results. The first tool is the Method for Investigation of Socio Technical Incidents and

Correction (MISTIC), which consist of a checklist of items derived from common themes and findings from the CAST, HSI, and HFE literature related to sociotechnical system causal influences on incidents and accidents. The second tool is the Proactive Resolution Of socioTechnical Ecosystem Cause Technique (PROTECT), which consists of a checklist of items derived from common themes and findings from the STPA, HSI, and HFE literature related to existing or proposed system analyses

Both MISTIC and PROTECT can be used by NPP personnel as a means of gaining reliable and relatively quick insight into (1) sociotechnical systems factors impacting incidents and accidents, (2) potential sociotechnical risk factors in existing or planned system designs, and (3) potential weaknesses in a system's safety and/or information control structure.

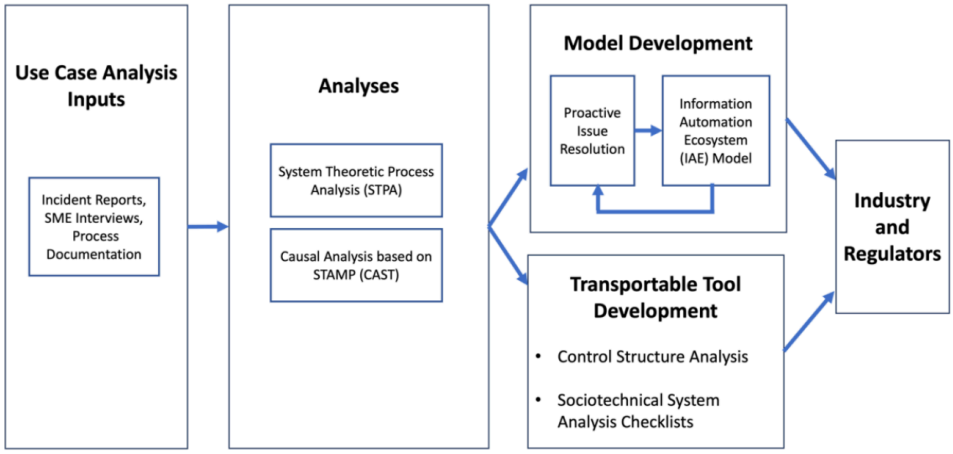

Figure 1. Research approach to develop transportable tools to optimize information automation that has been informed by System-Theoretic Process Analysis.

Contact

Jeffrey C. Joe | 208-526-4297 | Jeffrey.Joe@inl.gov

More on the LWRS Program: https://lwrs.inl.gov/

References

Joe, J.C., Hettinger, L., Yamani, Y., Murray, P., and Dainoff, M. (2023). Optimizing Information Automation Using a New Method Based on System-Theoretic Process Analysis: Tool Development and Method Evaluation, *INL/RPT-23-74217,* Idaho Falls: Idaho National Laboratory.