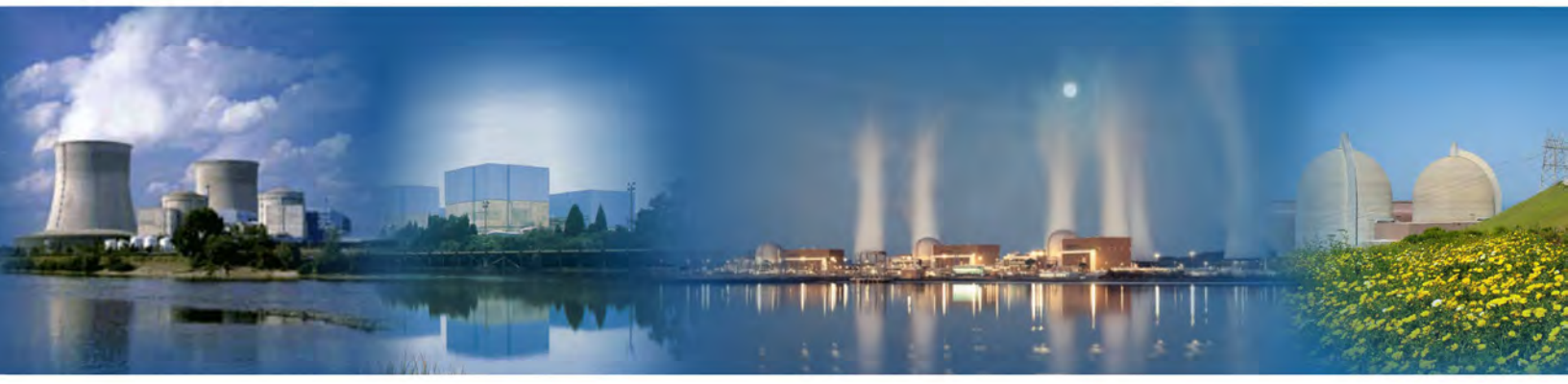
INL/RPT-24-80094

Light Water Reactor Sustainability Program

Mapping Data to Support Optimum Work Automation: The Socio-Technical-Organizational Modeling Process



August 2024

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-24-80094

Mapping Data to Support Optimum Work Automation: The Socio-Technical-Organizational Modeling Process

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

August 2024

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.

EXECUTIVE SUMMARY

This report describes recent progress on a research program focused on developing analytic methods and tools to support the assessment and management of sociotechnical risks in nuclear power plants (NPPs). This research is being conducted as part of the Department of Energy's Light Water Reactor Sustainability Program and its efforts, in partnership with industry, to support NPP modernization through effective work automation.

Extending the Systems-Theoretic Accident Modeling and Processes (STAMP) Framework, a multilayered model was developed to make the socio-technical and organizational constraints on managing and operating a NPP explicit. The Socio-Technical Organizational Modeling Process (STOMP) shows these constraints in terms of nested feedback loops where outer loops set the context for activities within inner loops and where inner loops provide feedback to support supervision, planning, and decision-making in the outer loops. A scheme (i.e., ontology or semantic structure) for analyzing and coding incidents (e.g., condition reports) was developed with the goal of localizing problems within the multilayered organization, identifying contributing factors, and recommending potential interventions.

The research team performed a detailed analysis of a significant event at a commercial NPP and plotted the outcome of our analysis on the layered loop model to highlight the areas of weakness. The team compared its results to that of the original root cause analysis and presented the differences in findings to a root cause expert from that utility to get critical feedback on the conclusions. Although different from the outcome of the analysis performed by the utility, the expert was intrigued with the outcome and expressed interest in helping to evaluate more test cases to further develop STOMP.

While the current research has focused on deriving a semantic structure from incident and condition reports, STOMP has broad implications for using advanced computational methods (e.g., artificial intelligence, machine learning, natural language processing, large language models) to process and filter information to enhance communications within and across levels of the organization. The semantic structure also has important implications for the design of graphical user interfaces tuned to the specific questions and decisions made within different levels of the organization. Finally, the semantic structure provides a framework for learning from incidents and designing appropriate training interventions to improve the quality of control within the organization.

The next step in the development process will be to formalize the logical or computational formulae utilizing the STOMP coding scheme that will be the basis for an automated inference engine or algorithm using big data analytics (i.e., artificial intelligence and machine learning). These algorithms could then be used to identify socio-technical-organizational weakness that go beyond specific incidents to reflect control weakness in a plant, a fleet plants, or across the entire commercial nuclear industry.

ACKNOWLEDGEMENT

The success of this project would not have been possible without the leadership, knowledge, and insight of Larry Hettinger, who, unfortunately, has had to leave the team due to health issues. Larry has had a highly influential career in Human Factors: first as a leading expert in simulator sickness, next as the Human Systems Integration coordinator for the construction of the *USS Zumwalt*, then as principal researcher in the Center for Behavior Science at the Liberty Mutual Research Institute for Safety, and finally as leader of our team of contractors to Idaho National Laboratory. Larry's work at Liberty Mutual involved applying sociotechnical systems theory to safety issues. His passion for applying sociotechnical theory greatly influenced the efforts of our team, which he was responsible for recruiting and building. All of our work effort at Idaho National Laboratory reflects his influence.

CONTENTS

FIGURES

TABLES

ACRONYMS

AI	artificial intelligence
CAPR	corrective actions to prevent recurrence
CAST	Causal Analysis Based on STAMP
DEHC	digital electro-hydraulic controller
EDG	emergency diesel generator
EPRI	Electric Power Research Institute
GUI	graphical user interface
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
KPI	key performance indicator
LLM	large language models
LWRS	Light Water Reactor Sustainability
MIRACLE	Machine Intelligence for Review and Analysis of Condition Logs and Entries
ML	machine learning
MRM	management review meeting
NLP	natural language processing
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
RCA	root cause analysis
SCS	safety control structure
STAMP	Systems-Theoretic Accident Modeling and Processes
STOMP	Socio-Technical-Organizational Modeling Process
STPA	Systems-Theoretic Process Analysis

Mapping Data to Support Optimum Work Automation: The Socio-Technical-Organizational Modeling Process

1. INTRODUCTION

This report describes recent progress on a research program focused on the development of analytic methods and tools to support the assessment and management of socio-technical risks in nuclear power plants (NPPs). 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 nuclear power plant modernization through effective work automation. It builds on prior work focused on the design and integration of new technologies into existing NPP processes (Kovesdi et al., 2021; Joe et al., 2023) and the use of systems-theoretic methods to assess sociotechnical risks in NPPs (Dainoff et al., 2020).

In support of this effort, LWRS Program researchers have developed a conceptual model of the multilayered processes that comprise the social, organizational, and technical features of how NPPs operate. Examples of multilayered processes include NPP operations, maintenance, procurement, surveillances, and outage management. In operations, there are teams of people (e.g., main control room crews, auxiliary operators), systems (e.g., primary, secondary, safety, non-safety), and technologies (e.g., analog indications and controls, digital control systems, business systems) that work together in a multilayered fashion in order for the NPP to operate.

The purpose of the multilayered conceptual model is to enable the identification of gaps and weaknesses in these processes and to provide recommendations for addressing them. LWRS Program researchers tested the potential utility of the model by using it to assess the presence of sociotechnical influences on multiple separate incidents in a representative NPP. These researchers then extended the model to develop a prototype system analysis tool, the Socio-Technical-Organizational Modeling Process (STOMP), as an initial step in developing risk assessment tools for the nuclear industry, including incident analysis and proactive risk assessment. The initial STOMP prototype, described in this report, is intended to support incident analysis by proactively focusing on potential sociotechnical and organizational influences on human-system performance.

Sociotechnical and organizational risk factors comprise a range of influences, including adequacy of communications, intra- and interorganizational coordination, planning, supervision, and other processes. Previous work by Joe et al. (2023) identified sociotechnical factors that were influential in an incident involving the unintentional activation of an emergency diesel generator. The research team has since extended this work by analyzing additional use cases to illuminate the role played by these influences and to supplement findings from root cause analyses and other incident analysis methods, particularly with respect to the role of sociotechnical and organizational factors in system performance.

The goal in developing STOMP and other sociotechnical risk analysis tools for the nuclear industry is to support a substantial (>30%) reduction in unplanned significant NPP events. In addition, proactively assessing the presence and extent of sociotechnical risk will afford industry the opportunity to take the necessary steps to address the relevant areas of concern to enhanced plant safety. Similarly, identifying sociotechnical risk factors involved in the occurrence of specific incidents will also shed light on broader systemic influences on performance than are typically discussed in root cause analyses. The ability to reliably identify and address systemic risk factors will also have important implications for the design of automated decision tools, including artificial intelligence (AI) and graphical user interfaces (GUIs) to enhance system performance with the potential for significant cost savings for the industry. The intent is to guide future analyses away from the "whack-a-mole" approach of solely focusing on the most proximal influences on an event and instead focus on the broader, systemic issues involved in such events.

2. OBJECTIVES

The major goals of this research effort are to improve nuclear safety and reduce operating and maintenance costs through real-time and proactive correction of social, organizational, and technical factors that are precursors to adverse events. In support of these goals, this LWRS research project is developing easy-to-learn and easy-to-use tools for sociotechnical systems analysis by NPP personnel. The objective is to provide the industry with the means to acquire reliable and rapid information about sociotechnical influences on adverse incidents and to discover patterns across multiple incidents that reflect deeper, systemic problems associated with communication and coordination within a complex, multilayered organization. Thus, rather than merely addressing symptoms (specific incidents), the goal is to improve the overall health and resilience of the whole organization.

For the research described in this report, LWRS Program researchers selected near-term objectives (Sections 2.1–2.4) as logical follow-ons to work conducted in Fiscal Year 2023 (Joe et al., 2023), which demonstrated the utility of sociotechnical systems analysis in support of incident and event investigation, and as necessary steps in the early development of analysis tools.

2.1 Objective 1: Demonstrate Effectiveness of Information Automation in Support of Work Automation Deployment

The scope and tasking for the current research focused on developing approaches (e.g., tools, techniques) to promote the greater use of effective automation in support of NPP operations and maintenance. One specific focus was to demonstrate the effectiveness of information automation to enable broad deployment of work automation. Toward this end, this research project focused on identifying patterns across multiple incidents that reflect systemic weaknesses associated with *observability* and *controllability* within a multiloop, nested control organization.

The scope of this research also focused on identifying and evaluating how a work process at a commercial NPP is currently performed (e.g., preventive maintenance, corrective action program), how it fits in with the existing compliance work function in order to support the digitalization analyses to optimize the process. Toward this end, this research evaluated how condition reports are currently generated in commercial NPPs and how these results could be coded within a large database to allow advanced computational tools to detect patterns in the data that could be helpful for identifying systemic weaknesses within the organization.

To accomplish the scope and tasking described above, this research focused on determining key performance indicators, identifying the best ways to digitalize the work processes, and developing a process to map data to support optimum work automation. These intermediary activities are the focus of the work described in Section 4.

2.2 Objective 2: Model the Socio-Technical-Organizational System

As a first step tool to assess sociotechnical risks and gaps in NPPs, this research developed a conceptual model of plant operations and maintenance. Previous work by Dainoff et al. (2022) and Joe et al. (2023) had demonstrated the utility of STAMP-based techniques to support system analysis. However, to get full benefit of the STAMP approach, it is essential to start with a systemic model of the organization that reflects how multiple layers within the organization interact to address fundamental issues of *observability* and *controllability*. *Observability* focuses primarily on communications to ensure that essential states of the system are communicated to key decision makers. *Controllability* focuses on the decision processes associated with planning and supervising activities as well as on the performance of those activities. To this end, this research modeled the organization as a multilayered, nested control system in which outer layers set the context for and monitor the activities of inner layers. This model will be described in more detail in Section 4.

2.3 Objective 3: Review Incidents to Identify Socio-Technical and Organizational Contributing Factors

Multiple incidents have been reviewed using STOMP. As a result of this process, a table of proximal causes was developed to specify socio-technical and organizational factors associated with incidents. The rows in the table reflect decisions, activities, and process steps leading up to a critical event. The columns in the table reflect variables that help to identify which layers in the organization are involved in the incident, the criticality of the activity relative to the incident, and the types of interventions that would help to prevent future incidents.

2.4 Objective 4: Align the Dimensions of the Table of Proximal Causes with the Attributes of Information Objects in an Extensive Database of Incidents

The analysis of multiple incidents has contributed to the development of an ontology (semantic structure) for creating information objects. An information object is an observation (e.g., a step in an incident) coded in terms of a collection of attributes. These attributes then allow associations to be made across objects. For example, steps in different incidents can be judged in terms of their similarity and thus, patterns can be identified to make inferences about organizational weaknesses or common causes of incidents.

2.5 Objective 5: Provide a General Framework for Improving Observability and Controllability in Nuclear Organizations

The semantic structure provides an important framework for integrating information from many different incidents or condition reports to identify patterns associated with weaknesses associated with the quality of control (e.g., in terms of safety, efficiency, or resilience) and communication (i.e., observability). Additionally, this semantic structure can suggest more effective ways to integrate and filter information to help ensure the right people get the right information in the right form and at the right time relative to the sphere of their authority and decision responsibilities. This has important implications for the design of dashboard representations to be effective decision aids.

3. ALIGNMENT WITH STATEMENT OF WORK

This research has important implications for improving the effectiveness of information automation and has broad implications for how various computational capabilities can be integrated into a multilevel organization to enhance the quality of control. Most importantly, the semantic structure that this research has identified provides an important foundation for utilizing AI and machine learning (ML) and GUIs (e.g., ecological interfaces) to enhance communications and coordination within the complex organization of an NPP.

In short, the semantic structure is a strong hypothesis about meaningful dimensions for key performance indicators, and the STOMP framework provides an important guide for using computational interventions to enhance the quality of control within the organization.

4. LAYERED SYSTEMS MODEL

This section describes the evolution of the current approach this research is taking by providing a brief overview of STAMP, and summarizing the STAMP-based research that has been performed.

4.1 Evolution of Current Approach

4.1.1 Overview of STAMP

The current STOMP approach originates in the Systems-Theoretic Accident Modeling and Processes (STAMP) framework developed by Leveson (2011) at the Massachusetts Institute of Technology. STAMP is a systems-theoretically based accident causation model. In STAMP, the emphasis shifts from preventing failures to enforcing safety constraints. Safety is viewed as an emergent property of a complex system of interactive controllers with multiple degrees of freedom.

In STAMP, safety is determined by sets of constraints that maintain control over the system. Therefore, control rather than reliability is the primary focus. The system's safety control structures (SCS) map out the interaction between controllers and controlled processes. The level of safety of a system depends on the extent to which safety constraints allow the system to avoid hazardous processes. In this sense, the system can be considered under control.

Within the overall conceptual framework of STAMP are two specific methods, called Systems-Theoretic Process Analysis (STPA) and Causal Analysis based on STAMP (CAST). STPA is a hazard analysis method with four fundamental steps:

1. Identifying possible undesirable losses and hazards
2. Modeling the SCS
3. Identifying unsafe control actions
4. Identifying loss scenarios (causal explanations for unsafe control actions).

Therefore, the STPA method, in general, can identify the safety constraints that must be in place to avoid and mitigate potential hazards. Constraints can be at the level of physical components, but accidents can result from dysfunctional component interaction, flawed algorithms and mental models, or organizational and social factors.

CAST is a STAMP-based method specifically aimed at accident analysis. It does not look for single causes but rather examines the entire sociotechnical system related to the incident being analyzed. Its goal is to: "… get away from assigning blame and instead to shift the focus to *why* the accident occurred and how to prevent similar losses in the future" (Leveson 2011, p. 349). 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, 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 it might have seemed reasonable.

Central to both methods is the SCS. To avoid hazards, safety constraints must be in place within the system. SCSs are the means of maintaining these constraints. Figure *1*, from Leveson and Thomas (2018), depicts a simplified generic control structure for an operating process. Note that both human and mechanical systems are analyzed within the same framework. In later versions of this diagram, human controllers are depicted with a similar internal structure.

The controller contains both a control algorithm and a process model. Control actions are emitted from the controller to the controller process, and feedback is received from the controlled process. In later versions of this diagram, human controllers are depicted with a similar internal structure. In the human controllers, the process model is called a mental model of the system.

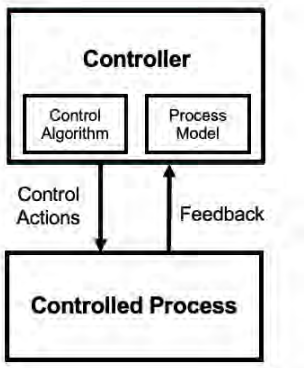


Figure 1. Generic safety control structure (Leveson and Thomas, 2018, with permission).

4.1.2 STAMP-Based Research

The STAMP framework has been the basis for a series of studies conducted by LWRS Program researchers, which has evolved into STOMP. This section will review those studies to provide a context for STOMP development.

4.1.2.1 Sociotechnical Approach to Human and Organizational Problems

Dainoff et al. (2020) and Hettinger et al. (2020) developed an overall framework for a sociotechnical approach to human and organizational issues in the digital modernization of an NPP. A review of relevant documents from the United States (U.S.) Nuclear Regulatory Commission (NRC), Electric Power Research Institute (EPRI), Institute of Electrical and Electronics Engineers (IEEE), and international requirements revealed that these documents frequently called for cross-disciplinary coordination and communication but gave no guidance on how these goals were to be met. The sociotechnical approach was an attempt to fill that gap. STAMP-based methods were an important component of that approach along with cognitive systems engineering, ecological interface design, human-systems integration, resilience engineering, and macroergonomics.

4.1.2.2 Dashboard for Management Review Meetings

A partnership between the LWRS Program and a utility company sought to employ this sociotechnical approach to develop solutions to specific modernization issues of concern (Kovesdi et al., 2021). One of these issues was the inefficiency of current management review meeting (MRM) processes for issue resolution with a particular focus on addressing gap analysis. Gaps are operational events that fall below performance standards. They are processed locally as condition reports but also may be detected by a large array of performance indicators used by the Institute of Nuclear Power Operations. This information goes directly to the Institute and is then fed back to the utility. The NRC may also be made aware. A management decision process selects a small sample of critical gaps for extended discussion at MRMs.

The proposed solution involved developing technical and procedural innovations to support NPP management decision-making. A “management-by-exception” approach to issue resolution, such as those related to performance gaps typically addressed during MRMs, was proposed as a means of increasing the efficiency of the issue resolution process without sacrificing the thoroughness of review. To provide technical support for this novel approach, a prototype information support dashboard was developed. The dashboard was built upon the concept of the information object, a software architecture entity specialized for the automated gathering analysis, dissemination, and tracking of data and information related to a specific gap. Drawing on the proposed functionality of information objects, the dashboard supports automated data gathering and analysis, high-level issue summaries, and resolution statuses with

corresponding drilldowns into more detailed information. The dashboard is always available to management personnel on the organizational intranet.

A key component of the design of the prototype dashboard was an STPA conducted on the gap analysis process. The resulting SCS was used to inform specific design features of the prototype demonstration.

4.1.2.3 NRC Problem Identification and Resolution Inspection

Dainoff, Hettinger, and Joe (2022) utilized a combination of cognitive work analysis and STAMP to explore the structure and operations of aspects of the NRC inspection process. This work was in support of LWRS Program efforts to develop information automation tools to make the inspection process more efficient.

This research concentrated on the routine inspection portion of the NRC's Problem Identification and Resolution Program. One component of that inspection is the requirement to verify that corrective actions commensurate with the significance of the issue have been identified and implemented. The use of cognitive work analysis and STAMP tools was to focus on the actions and resources available to the human inspector, realizing that this kind of work analysis is typically a necessary step prior to any automation.

The resulting control structure and information mapping revealed two separate processes for verifying corrective actions: those in which the actions were rectified and those for which no supporting condition reports could be found. The analysis found the sources of information support and procedures for these two processes were quite different, which has implications for future information automation efforts.

4.1.2.4 Reactor Trip Linked to Newly Designed Digital Controller

Dainoff et al. (2022) conducted a CAST analysis of a utility that experienced a reactor trip following the conversion from analog to digital turbine control system. This analysis utilized previously published root cause investigation materials. The NPP, which had two units, had recently implemented a digital electrohydraulic controller (DEHC) for reactor Unit A only. Based on operating experience from Unit A, a modified DEHC was designed for Unit B. When control room operators attempted to start up the reactor using the new device, a reactor trip occurred.

A CAST analysis, following the procedures specified in the CAST Manual (Leveson, 2019), was carried out. The analysis determined that several push buttons on the controller were repurposed from their original function. Specifically, the control sequence that had been used for normal startup was now allocated to emergency operations. Therefore, when the operator followed what they thought was a normal sequence, they inadvertently tripped the reactor.

The CAST results determined that, although the hand-off process between the project manager and plant technical leadership was not discussed in the formal incident report, several deficiencies in communication and coordination were clearly present:

- Despite a common procedure document, Units A and B used two different versions of the DEHC in which the same soft controls had different functional characteristics. Given that the operators were licensed to operate both units, this is a major human factors flaw.
- Procedural requirements related to documentation and testing were not followed.
- Procedural requirements for specific technical representation at key meetings were ignored. Knowledgeable individuals who might have picked up the discrepancies and omissions discussed earlier and who were supposed to be present were absent.
- It was unclear who was responsible for ensuring that the project team followed existing procedures for modifications.

- Just-in-time training of operators prior to startup did not cover the revised functionality. Moreover, the training materials used in this training did not reflect an accurate representation of DEHC. Updated drawings were not provided to the training personnel.

The CAST analysis conclusions provided additional insights into causal mechanisms not found in the root cause investigative report.

4.1.2.5 Unexpected Startup of an Emergency Diesel Generator

Joe et al. (2023) used a modified CAST procedure to investigate the unexpected startup of an emergency diesel generator (EDG). The event was 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 also during the planning, clearance activities, and work execution, all impacted by the implicit pressure to complete 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 an individual from one of the contracted groups that initiated the event with an error of commission. The event occurred when contractors, who were hired to install electrical equipment to complete an NRC-mandated update, opened the door to an electrical cabinet containing live connections to an EDG. This action triggered an unintended actuation of the EDG, which is an NRC-reportable event. The contractors had previously installed equipment in other cabinets and had not been properly briefed regarding the unique nature of this particular cabinet. The work had previously been scheduled to occur during the planned outage when this action would not have resulted in the unintended actuation of the EDG.

The importance of coordination and communication issues in this case led the researchers to utilize an alternative approach to conducting the CAST analysis. Johnson (2017) has identified coordination as a common issue arising in STPAs and CAST analyses and proposed modifying the basic CAST and STPA methodology to reflect this perspective.

Figure 2 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.

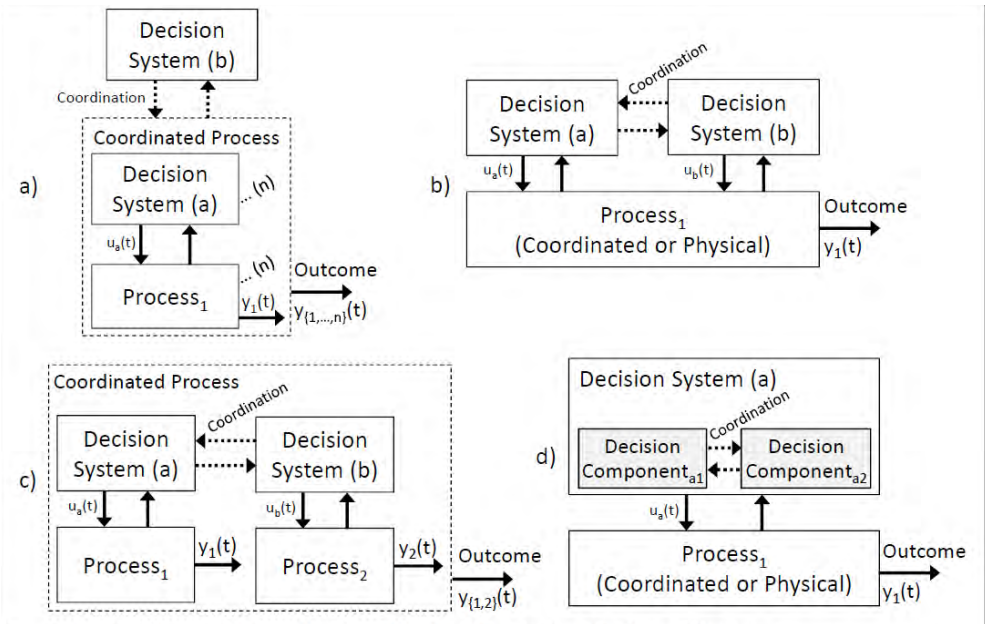


Figure 12. Fundamental Coordination Relationships in Sociotechnical Systems

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

Figure 2. Fundamental coordination relationships in sociotechnical systems (Johnson, 2017, Figure 12; used with author permission).

Figure 3 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 SCS, except they are organized in a hierarchy-by-time plot. Hierarchy, which is 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.

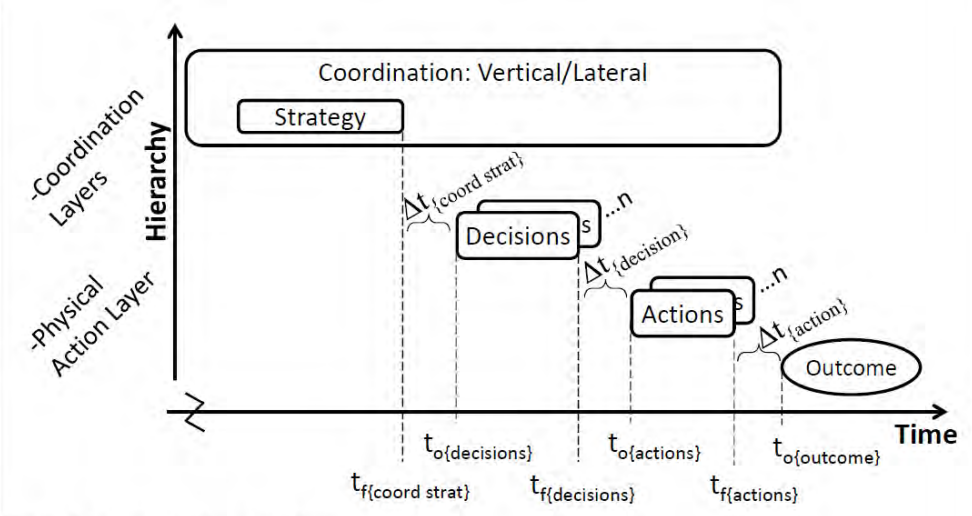


Figure 14. Coordination and Time

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

Figure 3. Modified SCS (redrawn from Johnson, 2017, Figure 14; used with author permission).

The resulting analysis gave clear indications of coordination failures at many levels. These were not evident from the original root cause investigation report conclusions. The initial clearances issued when the installations were due to be completed while the plant was offline properly indicated a low level of risk. However, coordination failures in the initial design process led to delays, resulting in the work being rescheduled after the plant was back online. Despite issuing new clearances and multiple opportunities for reviewing the installation, the significance of a high-priority safety-related component within the overall scope of work was repeatedly missed. This result solidified the importance of CAST analysis elements and led to the development of STOMP.

4.1.2.6 Other Publications Summarizing this Research

Over the last few years, researchers for this project have actively pursued additional opportunities to publish this research in conference papers (e.g., Dainoff et al., 2021), journal articles (e.g., Dainoff et al., 2023), LWRS newsletter articles[1], conference presentations, and conference panel sessions. Appendix A includes generic briefing paper researchers for this project have written that can be used as source material for future newsletter articles, handouts, and presentations.

4.2 STOMP Overview

4.2.1 Origins in STAMP and Open- vs. Closed-Loop Models

STOMP builds on STAMP, which is a system theoretically based accident causation model. Safety is considered a property driven by sets of constraints that maintain *control* over the system. Therefore, control (rather than reliability) is the primary focus of STAMP, and the primary unit of analysis becomes the SCS as illustrated in Figure 1. The system's SCS maps out the interaction between controllers and controlled processes. The safety level of a system depends on the extent to which safety constraints allow the system to avoid hazardous controlled processes. In this sense, the system can be considered under control—that is, the demands for observability (i.e., the quality of the feedback available to key decision

[1] LWRS newsletter articles are available at: https://lwrs.inl.gov/Newsletters/LWRS_Newsletter_Issue32_December.pdf and https://lwrs.inl.gov/Newsletters/LWRS_Newsletter_Issue36_Nov_2022.pdf

makers, including both human operators and automatic control systems) and controllability (i.e., the ability of decision makers to utilize that feedback to reduce surprises and prevent and or correct errors) are satisfied.

Thus, a systems theoretical approach frames the information flow dynamics in terms of coupled, closed-loop control systems that utilize feedback to adaptively pursue economic and safety goals and mitigate potential risks. As shown in Figure 4, this approach contrasts with approaches based on the root cause framework. The key difference is that a root cause framework models the system as an open loop. In the open-loop framework, defense in depth requires designers to anticipate specific variations (e.g., errors and violations) or hazards (e.g., weather events) in advance and to design barriers that will prevent disruptions to service and potential catastrophic outcomes. When an incident happens, the root cause approach reactively identifies potential causes and introduces new barriers. In contrast, the systems-theoretic framework assumes that defense in depth can be accomplished more resiliently through nested control systems.

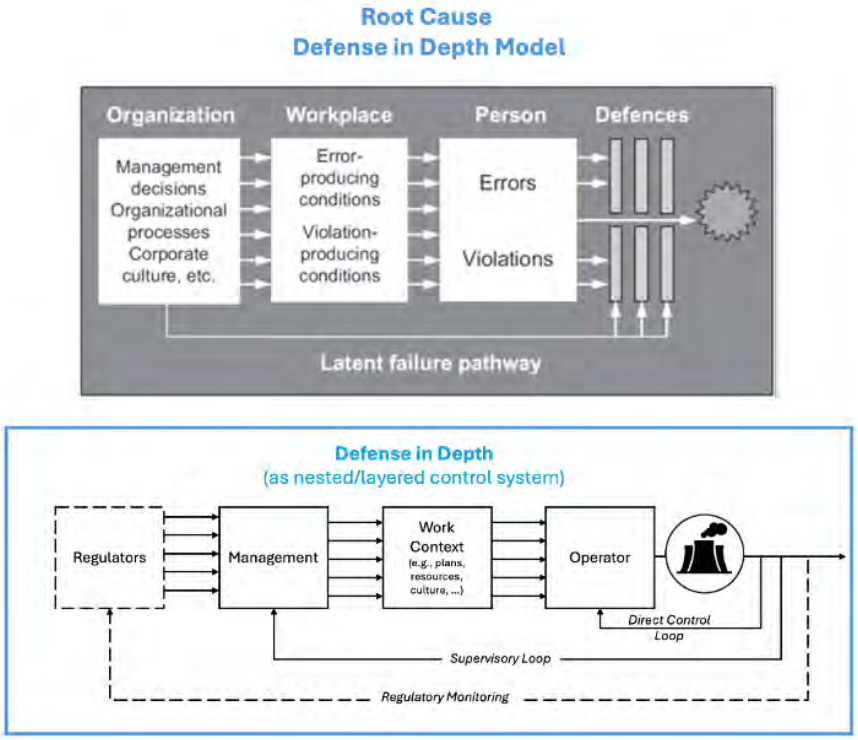


Figure 4. Contrasting a root cause model (open loop) with a control theoretic model (closed loop).

In applying a control theoretic approach to a large organization, it is important to recognize that these organizations typically involve a hierarchy of nested loops in which higher levels (e.g., leaders and managers) in an organization close the outer loops and lower levels in the organization (e.g., supervisors, workers) close the inner loops. This hierarchical coupling has been recognized by multiple authors, as shown in Figure 5 (Rasmussen and Svedung, 2000), Figure 6 (Leveson, 2011), and Figure 7 (Flach, Simpson and Kneeland, 2022).

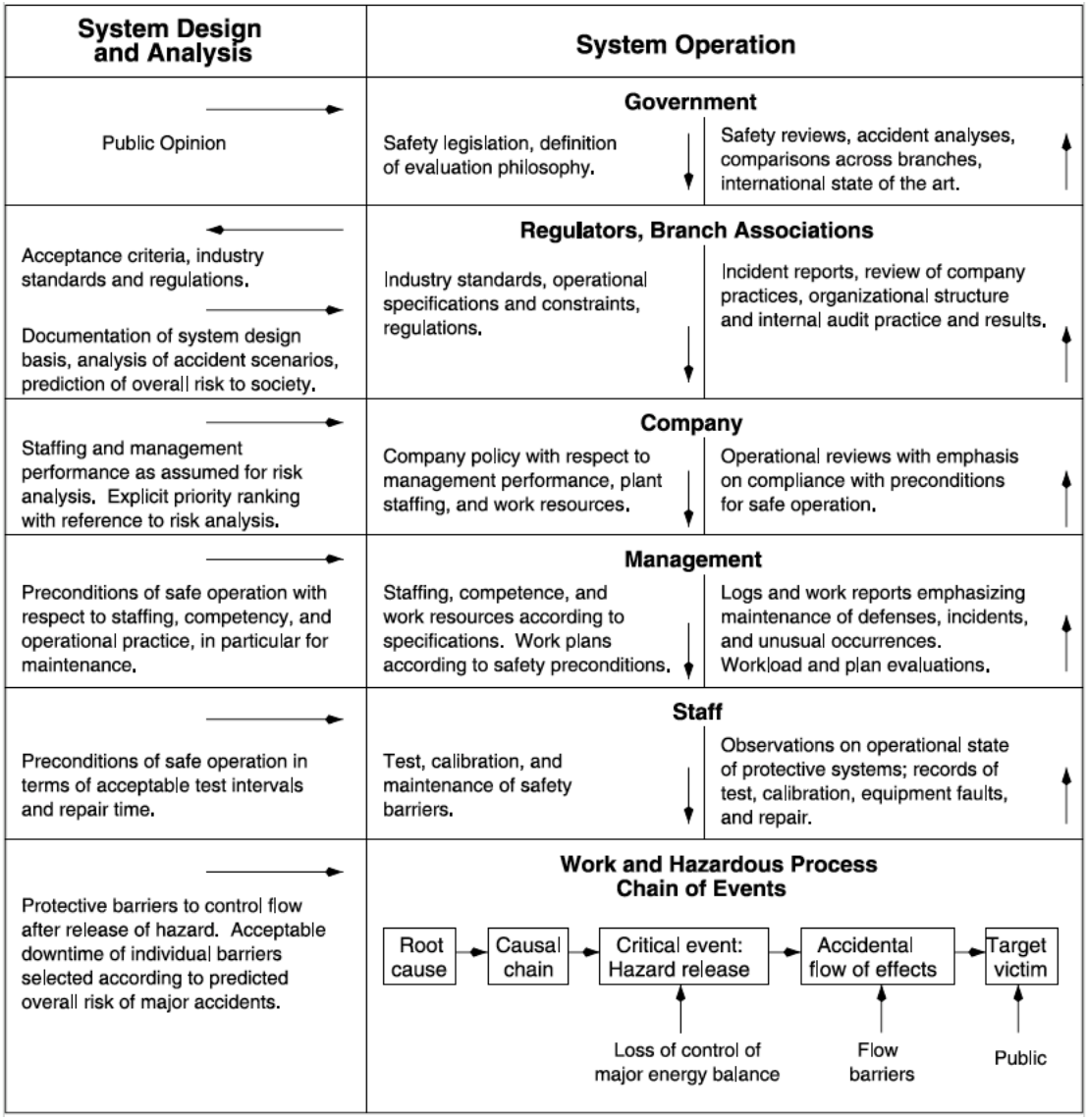


Figure 5. Rasmussen and Svedung (2000) hierarchical control model showing organizations as a hierarchy of control systems.

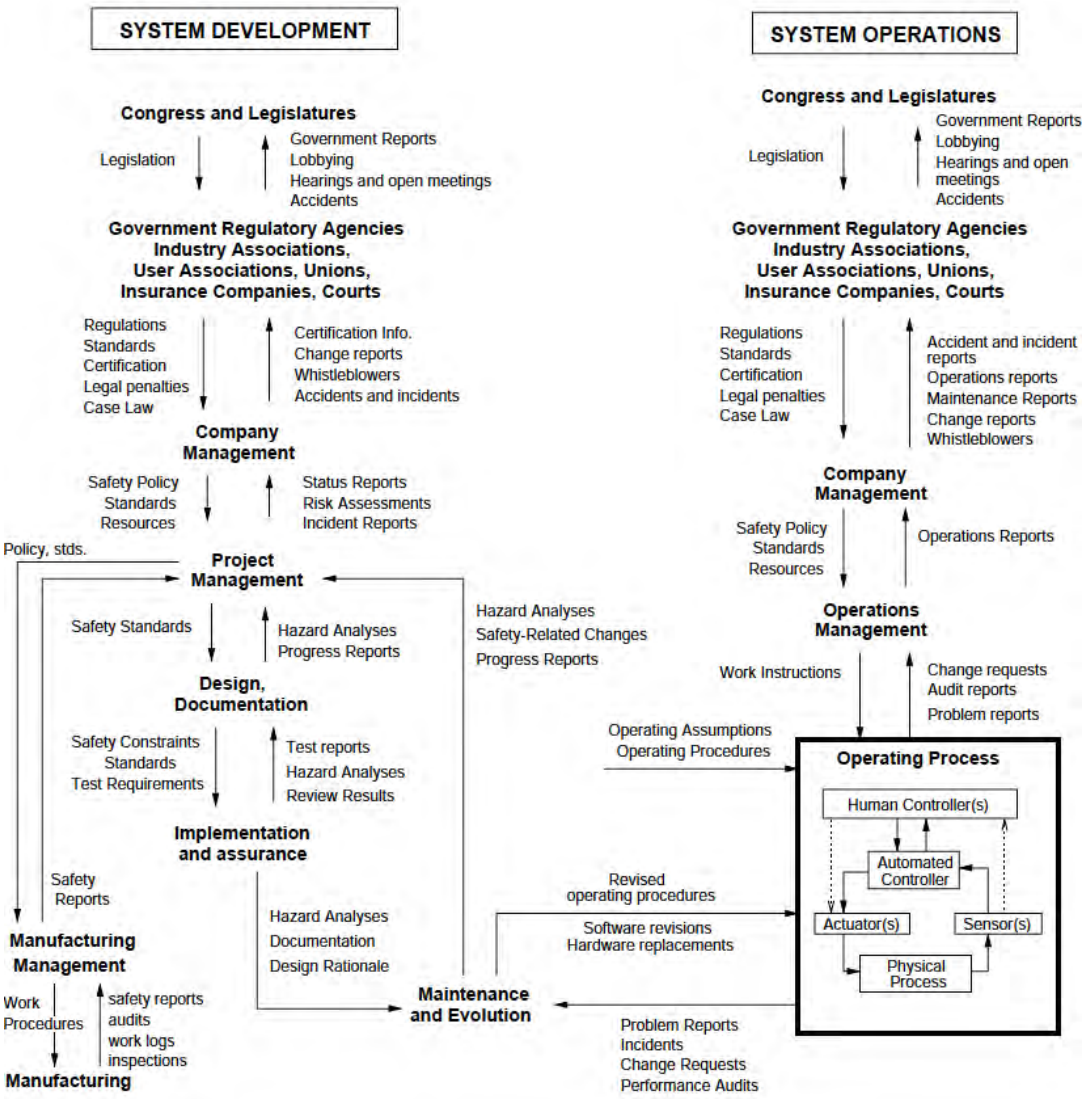


Figure 6. Levenson (2011) hierarchical control model showing organizations as a hierarchy of control systems.

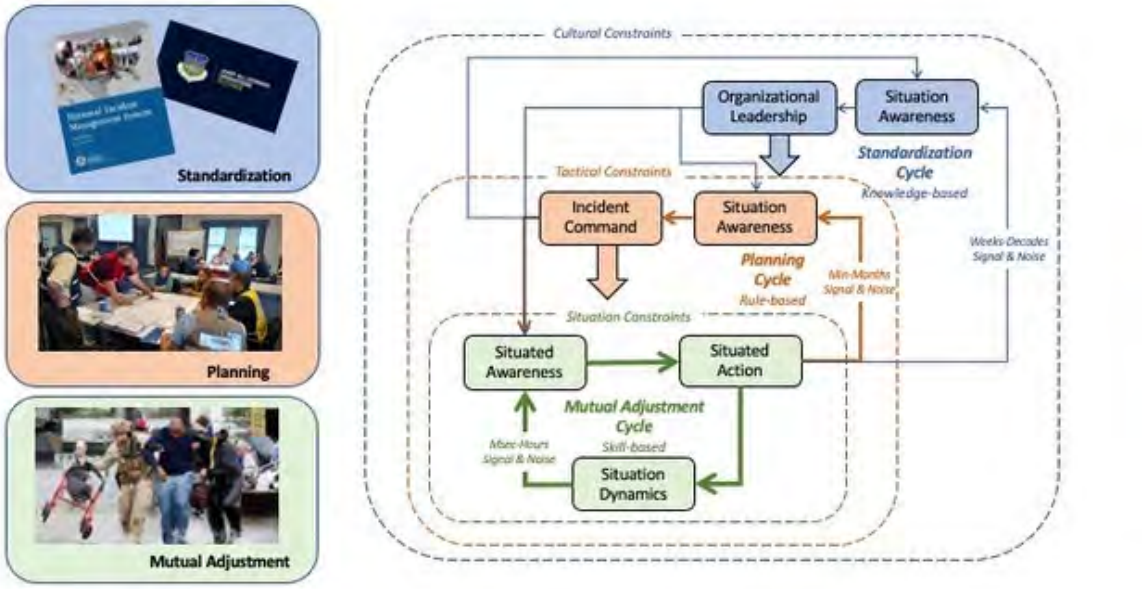


Figure 7. Flach, Simpson and Kneeland (2022) hierarchical control model showing organizations as a hierarchy of control systems.

As a result of the hierarchical layering of control systems, defense in depth is provided by a nesting of control loops in which outer loops monitor or supervise inner loops. Utilizing feedback, these nested loops are capable of a) anticipating, b) adapting to, and c) mitigating sources of variation that were not and could not have been anticipated by the system designers. In essence, the benefit of the closed-loop dynamics is that the system is capable of proactively identifying weaknesses and adapting (e.g., learning) so that it will be capable of resiliently pursuing economic goals, while mitigating risks (e.g., disturbances) that were not anticipated by the original designers.

4.2.1.1 Overview of the General Model

Although Figure 3 illustrates the hierarchical relations with an organization, the previous models do not make important aspects of the nesting and associated communications across levels in the hierarchy salient. Thus, this research project developed STOMP, illustrated in Figure 8 to highlight the communications within and across levels in the hierarchy. A key feature of this model is that the upper (or outer) loops set the context (e.g., degrees of freedom, field of possibilities, resources, boundary conditions) for the lower (or inner) loops. This top-down coupling allows a range of possibilities for higher levels in the organization to inform and constrain performance in the lower loops (e.g., sharing information and constraining authority).

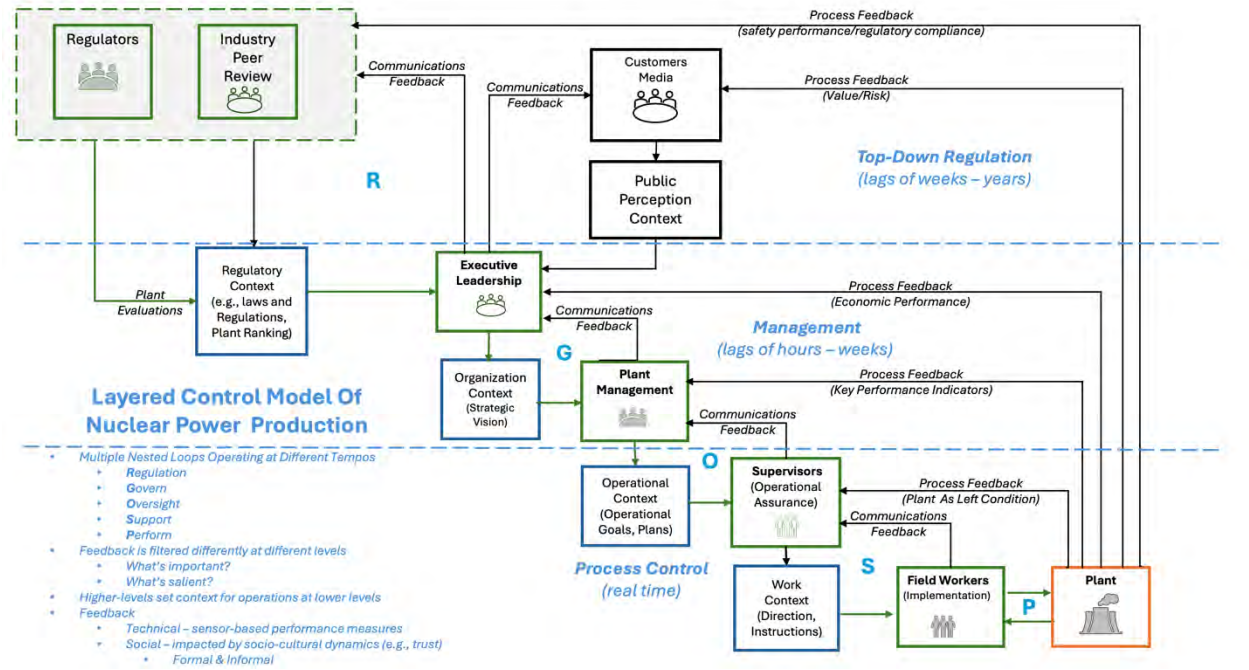


Figure 8. The sociotechnical system is modeled as a nested control structure where upper (outer) loops set the context (degrees of freedom, boundary conditions) for adaptation at lower (inner) loops and where there are both technical (process) and social (communications) feedback channels to close the loops.

In addition to the top-down coupling, there is a bottom-up coupling that effectively closes the loops. Information from lower levels feeds back to the higher levels in the form of sensor measurements of processes and through communications. Communications includes both formal communications (e.g., incident reports) and informal communications (e.g., emails and verbal conversations). The loops are nested in the sense that lower loops receive input from and provide feedback to upper loops. So, for example, the context for the operations loop is set by upper loops and information about activities in the operations loop is fed back to upper loops.

The nature of the couplings across layers ultimately determines the organization's capability to respond to the requisite variety in the work domain (e.g., commercial nuclear power). A limiting factor for contributions at the various levels to the overall resilience of the organization will be the access to accurate or complete information and the pace of processing that can be achieved. Typically, different levels will be tuned to pick up (i.e., process) information that will be somewhat different than the information available to other levels (e.g., different aggregations or chunks and/or different levels of abstraction). This reflects differences in the quality of the feedback and the tempo of action.

- Generally, *higher (outer) loops* both outside the immediate control of the utility and loops within the control of the senior leaders are tuned to integrate broad samples of information and to identify patterns and trends over long time periods (e.g., weeks to years). These loops tend to develop and set standards of operation to address the more stable (i.e., regular, predictable) aspects of a work domain (e.g., similar, frequent situations) and to set long-range goals.
- *Middle loops* are tuned to integrate information over intermediate time periods. These loops tend to be involved in setting short-term goals in terms of planning, scheduling, and supervising work. The people in this loop are typically *middle-level managers* and *top-level supervisors*.
- The *lowest (inner) level loops* tend to be most directly involved in carrying out the detailed work. The lowest level typically has the most direct, immediate feedback associated with the evolving situations

on the *ground* and the people in the lower loop are essentially the *supervisors* and *front-line workers* who directly perform the work.

The framing of the top-down and bottom-up couplings is intended to make it explicit that this organization is a *sociotechnical organization*. Framing the top-down coupling as setting the context for lower levels and the inclusion of two separate feedback channels (process feedback, communications feedback) in the bottom-up coupling is intended to make the importance of social factors apparent. The implication of this is that performance is not determined solely by technical factors. Social dynamics (e.g., culture, trust, generosity, fairness) that impact the top-down and bottom-up flow of information play an important role in shaping the quality of organizational performance.

It is important to recognize that this is a distributed and dynamic system. The constraints on all the various loops are changing as a function of internal (e.g., learning) and external factors (e.g., economic demands). Thus, the boxes do not represent static processes (e.g., fixed transfer functions). The system is constantly evolving. This is similar to the Joint Cognitive System (Hollnagel and Woods, 2005), which can be characterized in terms of three sources of constraint:

- *Human Factors*: Illustrated by the green boxes in Figure 8, represent the mental models and information processing capabilities (and limitations) of the teams of people at different levels of the organization.
- *Situation Factors*: Illustrated by the blue boxes in Figure 8, represent the social and organizational constraints on operations. This includes organizational constraints on roles and authority as well as constraints associated with processes, plans, and schedules that allow coordination across and within levels (e.g., multidimensional trust).
- *Technical Factors*: Illustrated by the orange box in Figure 8, represent the physical and engineering constraints on the technologies and energy production processes being controlled.

Figure 9 shows two models for visualizing the human factor elements of the organization in terms of mental models or situation awareness. The first model is Endsley's (1995c) model of situation awareness. The second model is from Thomas (2019), which is based on the work of France (2017), and depicts the internal dynamics associated with situation awareness and learning. The detailed dynamics of situational awareness in relation to the dynamics of closed-loop dynamical systems is discussed in Flach (2015; 2017). The important point is that the larger organization is capable of learning (i.e., this is a model of a learning organization). As noted at the start, this is a key attribute of the closed-loop dynamics. In essence, the system dynamics are not fixed or stationary. Thus, the ultimate effectiveness and safety of the system is not determined by the original designers or bounded by their ability to anticipate potential faults. The design is malleable (i.e., it is adaptive or self-organizing) and the ultimate quality of the design (the quality of learning) will be a function of the quality of the flow of information within and across levels. Ideally, the awareness will become increasingly well-tuned to the demands of the work domain, and the organization will become more efficient and safer with experience.

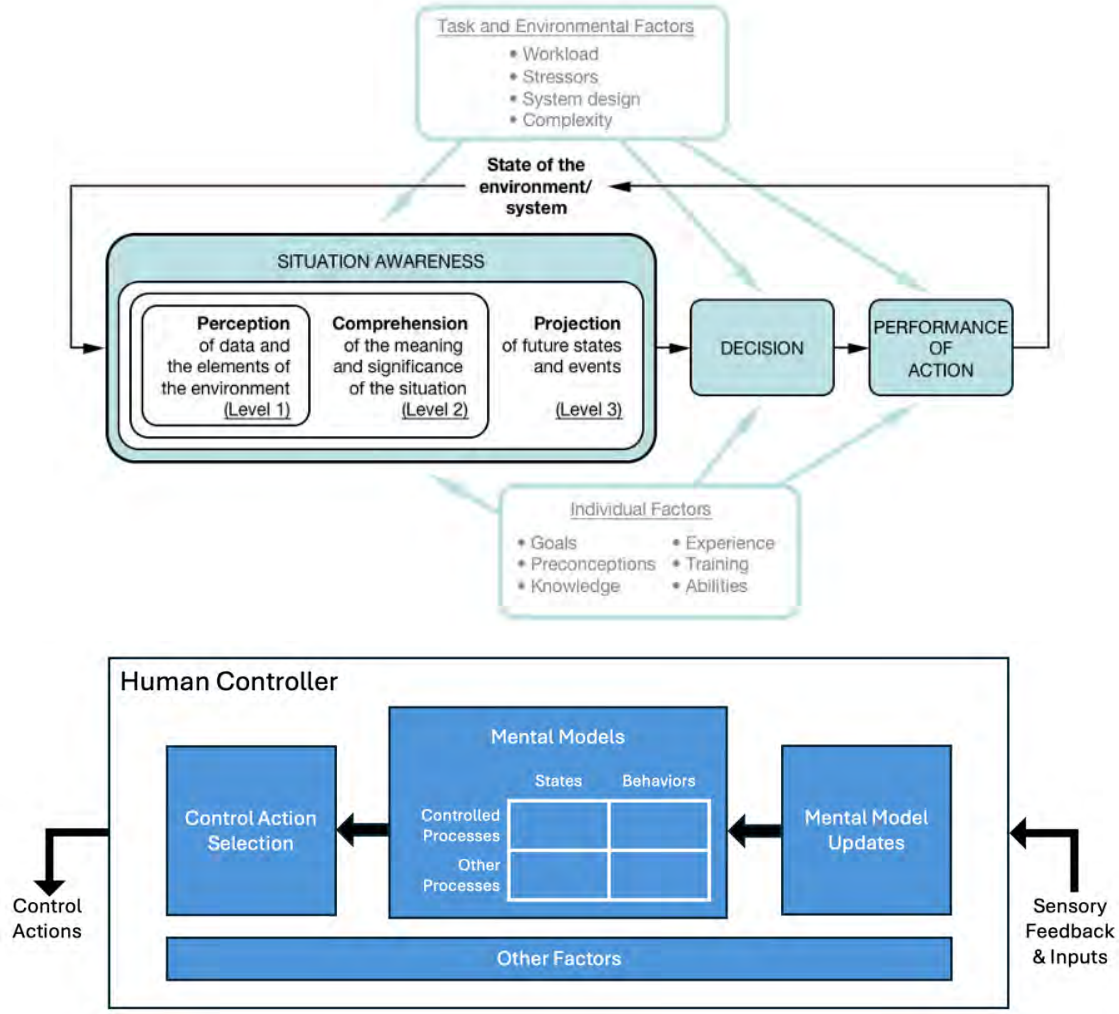


Figure 9. Two models representing the internal dynamics associated with learning and situation awareness.

As the human factor constraints evolve through experience and learning, the situational factors are also evolving to reflect the changing organizational culture and social dynamics. So too, the technical constraints on operations are also changing over time, as a function of both the natural aging and wear on equipment, and periodic replacements and upgrades of equipment. Thus, none of the boxes in the model have stationary transfer functions. All three sets of constraints are simultaneously shaping and being shaped by changes in the other constraints and on changes going on in the external ecology (e.g., energy demand and other economic concerns). Information is flowing both top down (e.g., standards, plans, and supervisory guidance) and bottom up (e.g., feedback in terms of communications and measured process states).

Advances in computational technologies offer new opportunities for enhancing the flow of information and in turn enhancing situation awareness at all levels of the organization. However, realizing these opportunities requires a broad sociotechnical systems approach for understanding the organizational dynamics (e.g., authority and reporting relations), the operational demands (e.g., process dynamics), and the technological opportunities. The control theoretic perspective presented in Figure 8 illustrates a useful

framework for assessing current information flows and for envisioning innovations to improve and enrich the flow.

More conventional approaches to root cause analysis have been criticized as being like a Smokey the Bear approach to preventing forest fires. By focusing on stamping out local fires (e.g., isolated causes), the Smokey the Bear approach might create more brittle systems (e.g., forests with excessive accumulations of undergrowth that may fuel more severe future fires). The alternative to the Smokey the Bear approach is to consider how to make forests healthier (e.g., more resilient to fires). Similarly, the control theoretic approach is an effort to strengthen the control loops in the system. This involves enriching the feedback within various loops (bottom-up information flow) to enhance the quality of decision-making, planning, and supervision (top-down information flow). This essentially makes the overall organization more resilient. By strengthening the control loops, the organization's capacity to deal with a wide variety of anticipated and unanticipated threats is increased. This not only reduces the numbers of potential causes but helps to ensure that, when inevitable errors happen, they are quickly mitigated to minimize the negative consequences and to avert the potential for more catastrophic impacts on the system.

4.3 Application to Tool Development

As an enhancement to conventional approaches to root cause analysis, this research is proposing a two-tiered approach to identifying weaknesses in control structures. The first step is to identify where the control weaknesses are with respect to the various control loops in Figure 8:

- The regulatory loop
- The governance loop
- The oversight loop
- The support/supervisory control loop
- The performance/operating loop

Note that an event may reveal weaknesses in multiple control loops.

The second step is to isolate specific factors associated with the human, situational, and technical components within the weak control loops. Again, the expectation is that there can be multiple factors that contribute to making a control loop weak. Identifying the components contributing to the control weaknesses will go a long way toward suggesting what type of concrete interventions will strengthen the control loop. It is important to realize that strengthening a control loop will not only reduce the likelihood of a specific event but increase the resilience of that loop. In other words, strengthening a control loop prevents a myriad of other untoward events from happening.

4.4 Findings from Model Development and Systems Analysis

4.4.1 Revising Proximal Event Tables

This section describes the evolution of the scheme for coding observations in STOMP that builds on the STAMP and CAST Framework.

4.4.1.1 CAST Dimensions

Implied in the logic of the CAST procedure is the assumption that each incident will be analyzed as an essentially independent entity. Consequently, the control structures resulting from each incident will be unique to that incident. Leveson (2019) emphasized the CAST procedure was not a cookbook; it was meant for an analyst to think carefully and in depth about the cause of an incident. Fundamentally, the CAST procedures are structured to ask questions about an incident; such questions will afford the possibility for such careful and in-depth thinking. Central to each procedure will be a control structure,

which will be unique to that incident. However, similar incidents will yield similar control structures. Likewise, the analyses resulting from the decomposition of the control structure will be unique to each situation.

On the other hand, the layered systems model is an evolution of CAST, which considers that NPP incidents share a common causal structure within a given plant and across the industry. This model leverages the redundancy inherent in this commonality to provide a procedure that compares incidents across and within plants. Consequently, the retrospective nature of CAST can be transferred into a more proactive tool. As such, the proximal events table is a major point of focus.

Figure 10, from the CAST Handbook (Leveson, 2019), depicts the process. The analysis is retroactive, being limited to the circumstances surrounding a particular event. The first stage, assemble basic information, is where the proximal event table is utilized. This information is used to model the SCS. A component-by-component analysis follows, after which the entire structure is examined. From these efforts, an improvement program is created.

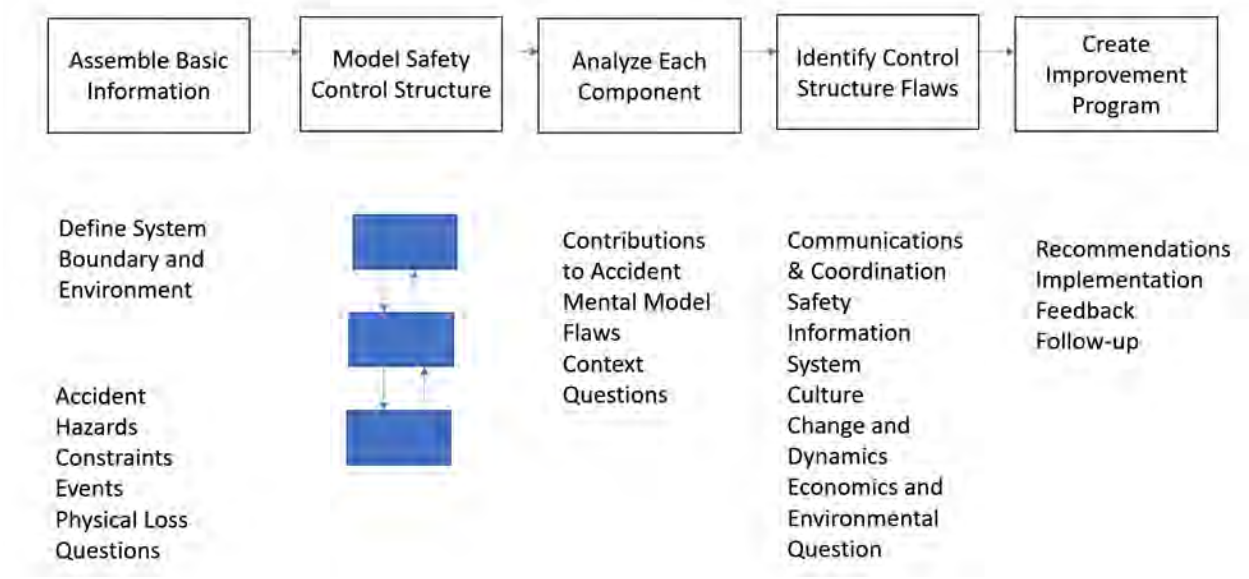


Figure 10. Steps in CAST process (Leveson, 2019 by permission).

Leveson's specific instructions are:

> *While not required to start a CAST analysis, identifying the proximate events preceding the loss may sometimes be useful in starting the process of generating questions that need to be answered.…Remember that the goal of listing the events is NOT to select…the cause of the loss. Instead, the goal is to generate questions for the investigation that will be used in the overall causal analysis. (Leveson, 2019, p 39.)*

As such, the actual information-gathering process is relatively unstructured, with much discretion in the analyst's hands. For this project, LWRS Program researchers conducted a CAST analysis of a reactor startup using an existing published root cause analysis (Dainoff et al., 2022). The control room task was to gradually increase steam pressure in the reactor by controlling the position of the turbine steam bypass valves, using a new DEHC for the first time. During the outage, this turbine control system had been upgraded from the analog version. This analysis followed the recommendations in the CAST Handbook (Leveson, 2019). Table 1depicts a skeleton version of the proximal events table, which was used to construct the SCS and subsequent analysis.

Table 1. Skeleton proximal events table, from Dainoff et al. (2022).

ID	Event	Questions
1	—	—
2	—	—

Note that there are only three columns in this table. The identification number of each event in the incident, a brief description of the event, and the analyst's questions regarding the possible significance of the event to the overall incident.

4.4.1.2 Additional Dimensions

A second CAST analysis was conducted of an incident in which maintenance workers opened a cabinet, inadvertently triggering the operation of an EDG. The analysis is documented in Joe et al. (2023) and briefly described in Section 3.1. As in the previous example, the study was based on an already published root cause investigation. In this case, however, initial examination of the root cause data suggested that coordination issues were central. Accordingly, the methodology was modified according to the recommendations of Johnson (2017), who proposed a levels of coordination model for STAMP.

Utilizing Johnson's (2017) method, four separate levels of coordination needed to be identified while constructing the proximal events table: work organization, clearance, design, and governance. Table 2 depicts a skeleton version of the proximal events table used in this study. The work process describes the actual maintenance work carried out, the design process describes the design of that work, the clearance process describes the required process reviews to keep workers safe during the work activities, and the governance process describes management control and coordination.

Table 2. Modified proximal events table from Joe et al. (2023).

ID	Step Title	Work Process	Design Process	Clearance Process	Governance Process	Questions	Notes
1	—	—	—	—	—	—	—
2	—	—	—	—	—	—	—

4.4.1.3 Adapting to the Model

Table 3 represents a preliminary version of the proximal events table as a component of STOMP. As such, it depicts a standardized framework for the data entry of critical attributes of each step of the incident under analysis. These elements will transform into information objects, as described in the following section.

Some of the table headings require explanation. Loop indicates the level of the layered systems model where the weakness is localized. Impact or severity will be coded according to predefined categories, and problem/failure mode is what did not go as expected from a human or equipment performance perspective. is defined in terms of what went wrong. Feedback represents the presence or absence of feedback within affected control structures, PSF/HF represents applicable performance shaping factors and/or human factors, affected contexts refers to the context component of the layered systems model, responsible organization is the organization that caused the issue or is responsible for the weakness, and the affected control structure will be coded according to a list of predefined control structures.

Table 3. Preliminary proximal events table.

Sequence #	Event #	Date/ Time	Step or Event Title	Affected Process or Equipment	Loop (GOSP)	Impact or Severity	Problem/ Failure Mode	Feedback	PSF/ HF	Affected Context	Responsible Organization	Affected Control Structure(s)
1	—	—	—	—	—	—	—	—	—	—	—	—
2	—	—	—	—	—	—	—	—	—	—	—	—
3	—	—	—	—	—	—	—	—	—	—	—	—
4	—	—	—	—	—	—	—	—	—	—	—	—
5	—	—	—	—	—	—	—	—	—	—	—	—
6	—	—	—	—	—	—	—	—	—	—	—	—
7	—	—	—	—	—	—	—	—	—	—	—	—
8	—	—	—	—	—	—	—	—	—	—	—	—
9	—	—	—	—	—	—	—	—	—	—	—	—

Note: GOSP = Governance, Oversight, Support, Perform.

5. PROTOTYPE DEVELOPMENT

As previously stated, the initial STOMP prototype was intended to support incident analysis by focusing on potential sociotechnical and organizational influences on human-system performance. After-the-fact incident analysis is necessary to train the prototype system because it allows the team to independently validate the results of the team's analysis using results from a previously performed root cause investigation that was performed by a trained expert who is independent of the team. The prototype included a relational database with functionality that facilitated the analysis of real plant events. Event reports from several utilities were fed into this prototype database, with each event being converted into information objects which would become inputs into an algorithm used to determine the most impactful causes of the events. Various iterations of the algorithm were fed data from the events so that it could identify causes and subsequently recommend corrective actions to address the organizational or programmatic weaknesses.

5.1 Information Objects

NPPs have a vast amount of data for every system, component, organization, process, equipment, or structure. All of this data can be further broken down into unique segments of information that represent an attribute of each type. These attributes create information objects. For example, a piece of equipment is an information object that has attributes such as make, model, manufacturer, and other attributes. A condition report may be described in terms of information about what, why, who, actions taken, etc.

The purpose of information objects is to integrate data from multiple sources into a common ontology or semantic structure. The common semantic structure can help detect weak signals that would not be otherwise discoverable from many independent databases. In other words, the common semantic structure is an essential foundation for unleashing the power of big data analysis (AI, ML, large language models [LLMs]). Using big data analytics, it becomes possible to derive prescriptive algorithms to specify interventions that will increase *observability* and *controllability* in the multiple nested loops identified in Figure 8.

The proximal events tables described in the previous sections provided an initial foundation for specifying information objects. Each row in a proximal event table can be considered an information object, and the columns represent attributes of that information object. This allows steps from one incident report to be compared to steps in other incidents. For example, information objects allow the human, or AI, analyst to see whether the steps involve the same subgroups in the organization (e.g., maintenance or operations) or whether they are similar in terms of human factors or performance shaping factors. In other words, these kinds of associations can be very meaningful with respect to choosing an appropriate intervention because they help the analyst answer questions, such as:

- Do the incidents involve a common unit or layer of control within the organization?
- Are there common causes of incidents in terms of human factors or performance shaping factors?

5.2 Introduction to the Database

In order to facilitate the development of the process, a database was created that allows the input of data in many different ways and then facilitates the analysis of the data by converting the data into information objects, with each information object being represented in terms of a common set of attributes (e.g., columns in a proximal events table). All events or event steps have been converted into information objects, with thousands of event reports having been captured already. Within the database, information objects are captured in code tables to ensure the consistency and transportability of data for comparison to any other nuclear plant data. A front-end GUI on the database allows for the human input of events through a proximal events table, which helps to break down the various steps of a complex event and convert them into the information objects necessary to feed an algorithm used to determine causes and corrective actions.

Table 4 shows the various attributes of an information object. In essence, this table is a hypothesis about critical semantic relationships in the database. Attributes in the global column reflect aspects of the incident (e.g., condition report) from which the data were obtained. The other columns reflect specific attributes of steps derived from the descriptions of the incident. These include step identifiers, attributes associated with the level within the organization structure (Figure 8) involved, attributes associated with the cause of the incident, and attributes associated with the severity of the incident.

Table 4. Attributes of an information object.

Global	Step			
	Identity	Level/Loop	Cause	Severity
Station Tracking Number Title Time Report Process Equipment Severity Report Type	Sequence Number Date/Time Title	Affected Process Feedback Signal Affected Loop Responsible Organization Affected Control Structure	Failure Mode Performance Shaping Factor Human Factor	Severity/Impact

The semantic structure illustrated in Table 4 provides a meaningful basis for making inferences from patterns in the database about the overall health of the organization. The attributes in the level/loop column help to localize problems within the nested control structure illustrated in Figure 8. The attributes in the cause column allow inferences about the nature of the problems. Attributes in the severity column allow inferences about the significance of the problem. Together these categories provide a basis for specifying the interventions needed to improve *observability* and *controllability*. Specifically, the level/loop attributes help to specify who or where in the organization interventions are needed. The cause attributes help to specify what types of interventions are required. and the severity attributes at the global and step level help to specify the priority or potential impact of interventions.

5.3 Case Study – Mispositioned Equipment

Some LWRS Program researchers on this team have many years of root cause analysis (RCA) experience, are familiar with numerous RCA techniques and methods, and have collaborated on RCA reference manuals, including International Atomic Energy Agency IAEA-TECDOC-1756 (2015). With permission from a nuclear plant, the research team selected a significant event to analyze using STOMP so that the outcome of using STOMP could be compared to the outcome generated using a traditional RCA method by unbiased event investigation experts.

In this case study an important piece of equipment was found to be unavailable due to a plant employees working on the wrong component. That is, a human error occurred in which workers inadvertently caused the incorrect piece of equipment to become unavailable when performing a tagout of a different piece of equipment for a surveillance. The plant performed a thorough RCA of the event using traditional RCA techniques and methods to identify root and contributing causes as well as corrective actions to prevent recurrence (CAPR) and other actions to address the contributing causes. This process traditionally takes a plant 30 days to perform including review and revisions to the report.

Utilizing the precise outcome of the RCA performed by the plant, the team plotted the causes on the layered loop model. Figure 11 plots the outcome of the root cause investigation as performed by the plant.

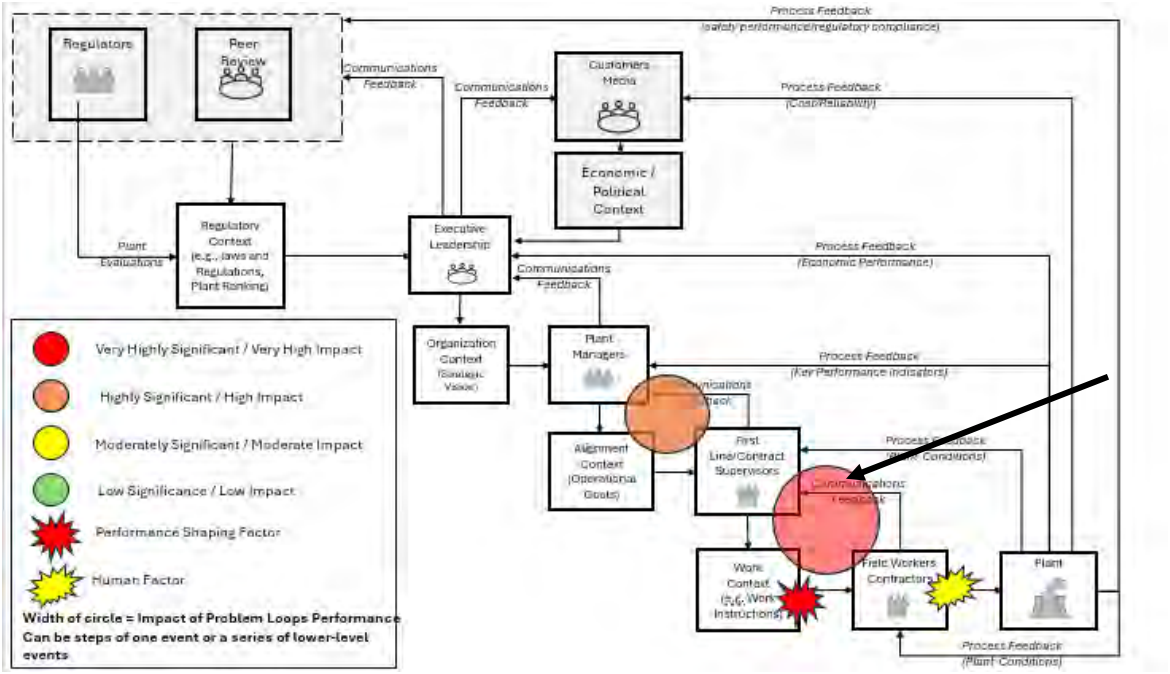


Figure 11. Layered loop model representing existing RCA conclusions.

As shown in Figure 11, the plant concluded that the root cause of the event was inadequate work practices and communications within the lowest two loops of the organization, with performance shaping factors of poor labeling and human factors of failure to adequately use verification tools. The plant's CAPRs included revising the context (guidance) utilized by the workers when manipulating the equipment to ensure the proper configuration of the equipment post manipulation. Contributing causes of this event included a lack of adequate oversight of the workers when performing critical evolutions. Other actions were taken by the plant to address the contributing causes, performance shaping factors and human factors identified during the investigation.

5.3.1 STOMP Analysis of Equipment-Mispositioning Event

The LWRS Program research team performed an independent STOMP analysis of the event to compare the outcome from the traditional RCA method. There were sixteen steps in the event timeline from the plant's analysis that the researchers used to populate sixteen distinct steps in the STOMP proximal events table. Figure 12 below shows one of the steps of the event as it is entered in the proximal events table.

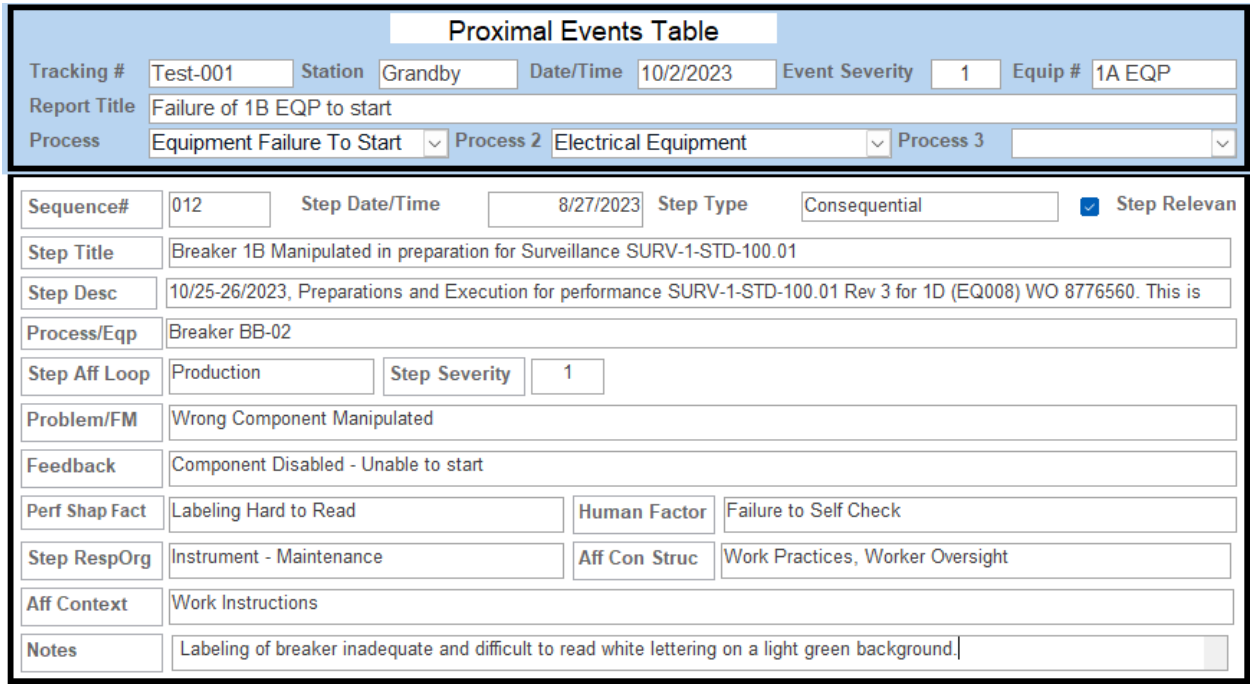


Figure 12. Proximal events table step entry

As each step from the event from the timeline was entered into the proximal events table, attributes from information objects were captured in the database using relational code tables, one corresponding to each attribute to ensure consistency for each entry in the proximal events table. These attributes serve two purposes. The first is to help identify the weak control structures that caused the event to occur. Identifying weak control structures helps identify corrective actions or interventions that can be taken in the future to prevent recurrence. The causes of the weak control structures are then plotted on the layered loop model. The attributes are also used to determine how significant the impact is on the outcome of the event, and what corrective actions or interventions are necessary to strengthen the respective weak control structures to prevent recurrence.

The second purpose for the attributes is to allow information automation to help in the transportability of the information so that the following could be more easily and accurately identified including:

- Extent of condition
- Extent of cause
- Previous similar internal events, including similar work orders
- Similar external operating experience
- Determining CAPR effectiveness (interventions)
- Trending of similar events

- Suggesting/selecting management observations
- Universal search or comparison of events in any nuclear or other industrial domain

Although attributes for each step of the proximal events table are not always available, thorough information gathering and subsequent analysis techniques from a complex event usually provide dozens of attributes. These can be utilized for comparison in many different dimensions allowing for better proactive trending of precursors to future events that were not considered before. For example, when the attributes of "responsible organization" and "affected process" are trended along with certain human factors, human error traps become more apparent and can be identified when plant feedback, such as condition reporting, identifies similar situations. Furthermore, these attributes can be used to search for external operating experience so that the plant can compare actions taken by other plants when determining actions that should be taken to arrest the developing trends.

The outcome of the STOMP analysis of the mispositioned equipment event was subsequently plotted on the layered loop model in Figure 13 below.

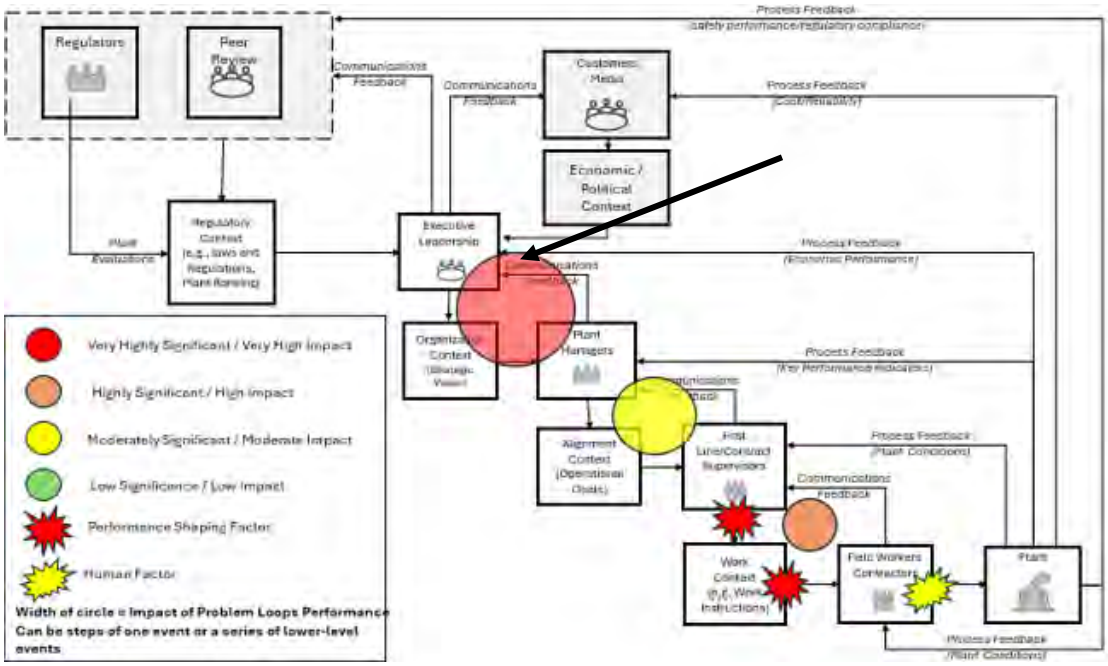


Figure 13. Layered loop model plot of mispositioned equipment event

As shown in Figure 13, the most significant or impactful control structure weakness occurred in the governance loop. The utility's executive leadership was not made aware of the plant leadership's lack of supervisory oversight that resulted in the equipment mispositioning. Analysis of the event revealed no context or key performance indicators (KPIs) available to executive leadership to determine if adequate observations or oversight were occurring for any work groups performing critical evolutions in the plant. The lack of executive leadership's knowledge of the continued poor performance of the responsible work group was due to unintentional filtering of the feedback from the lower loops, due to weak or non-existent context (e.g., no KPI to measure departmental engagement) that would ensure they were appraised of the problem sooner. The typical vehicle for this type of communication at U.S. NPPs is an MRM. Based on the significance and erosion of regulatory margin from this event, actions from this event would rise to this level within the organization to prevent recurrence. By taking corrective actions (i.e., interventions) that would add context, for example, KPIs for paired observations of critical evolutions, executive leadership would be able to leverage these KPIs to prevent many other similar events at all levels from occurring, thereby preventing future significant events as well. If this issue had been raised during an

MRM, for example, actions to correct this problem could have been taken sooner, which would have mitigated the event or prevented it from occurring altogether. Most importantly, the current result verifies the utility of STOMP in examining *observability* and *controllability*, which would otherwise be overlooked in other analytic approaches used to investigate incidents. The LWRS Program researchers compared these results to that of the original RCA and presented the differences in findings to key stakeholders at the plant who were knowledgeable in event investigation techniques. This included an experienced root cause analyst to get critical feedback on the conclusions from the STOMP analysis. Although different from the outcome of the utility's analysis, the plant RCA process stakeholders were intrigued with the outcome using STOMP and expressed interest in helping to evaluate more test cases to help the LWRS Program further develop this event investigation method.

One of the things that the research team learned from the analysis of this event, as well as others, is the importance of measuring the engagement of the workforce at all levels by analyzing the feedback to the levels above, as was evident by where the most significant cause of the event was located for this mispositioning event. Traditional RCAs of events are performed based on the information that is collected during the investigation. However, one strength of STOMP is that a lack of information is also factored into the analysis of the event. When there is a lack of reporting of issues through condition reports or management observations, it is also indicative of a problem within the organization as indicated by a deficiency in the feedback to the loops above, and therefore, the investigation must determine why the feedback has not been reported or captured. Without continuous unfettered feedback, the managers in the organization are making decisions potentially based on incomplete or inaccurate information. This will directly impact the context that they provide for the loops downstream of their decision-making.

The ultimate goal of this new process is to improve the safe and reliable performance of plants by reducing significant events. To further develop STOMP, significant events in which a full root cause investigation has been performed are needed so that socio-technical dynamics of the organization can be identified. When the dynamics of the organization are understood, this process can be used to proactively analyze low level events and near misses to 1) identify the inadequate control structures **before** an event occurs, and 2) recommend interventions that will strengthen the respective control structures. The same attributes that are assigned to each step of a complex significant event can be assigned to condition reports or other information reporting sources (e.g., management observations, equipment reliability data) so that they can be plotted on the layered loop model and to expose weak, weakening, or non-existent control structures in the respective loop that causes the issues to manifest themselves as the likely direct cause of a similar event.

6. PATH FORWARD

The inferences illustrated in Figure 13 were based on the intuitions of a domain subject matter expert using STOMP. The next step in the development process will be to formalize these intuitions in terms of logical or computational formulae that will be the basis for an automated inference engine or algorithm using big data analytics (i.e., AI/ML). These algorithms could then be used to identify socio-technical-organizational weakness that go beyond specific incidents to reflect control weakness in a plant, a collection of plants, or across the entire commercial nuclear industry.

Because an NPP is a sociotechnical organization, or system, improvements to the flow of information can be made with respect to the social, organizational, and technical aspects of the system. On the social side, efforts toward creating a just, blame-free culture, or to improve the safety climate, will generally improve the flow of information. While these social factors are important, the focus of this research moving forward will be on opportunities to utilize emerging information processing technologies such as natural language processing (NLP), LLM, AI, and ML to improve information flow as illustrated in Figure 14.

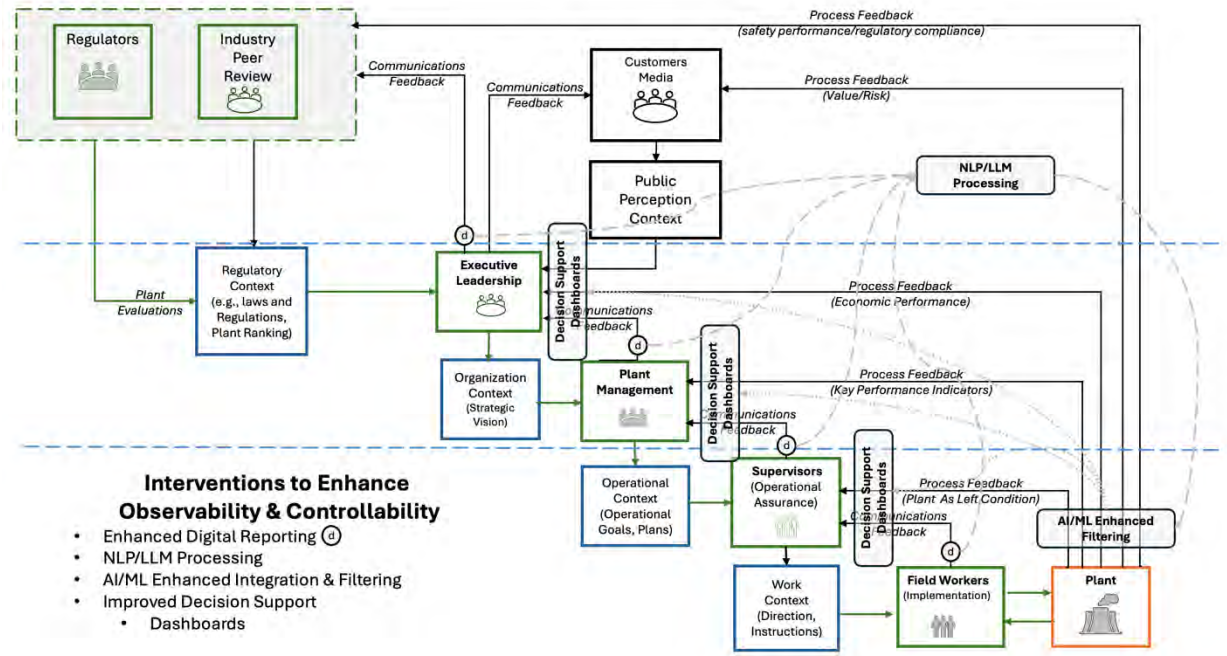


Figure 14. Illustrates potential interventions to improve observability and controllability within a multilayered organization.

Currently, information flow in the organization is limited by the bandwidth of the existing information automation and methodologies used by human experts at each level of the organization. Because of the limitations on human attention, memory, and sensemaking capabilities, it is obvious that all the available information (e.g., the multitude of condition reports) is not being fully utilized. Advanced information technologies that have a much wider bandwidth and greater pattern recognition capabilities can be employed to process (e.g., detect trends not visible to current experts) and filter data (e.g., selectively channel information to the appropriate organizational levels in a form that is compatible with human sensemaking capabilities). Note that the computational technologies are not being envisioned as replacements of human expertise. Rather, they are being envisioned as opportunities to enhance the accuracy and timeliness of information flow and to detect weak signals that are otherwise not detectable, thus, empowering human expertise. In essence, these technologies enhance the quality of information available to experts and allow experts to focus their attention where it will have the highest value relative to improving situation awareness and ultimately improving performance of the organization.

As shown in Figure 14, NLP/LLM technologies can be used to process and digitize the vast databases of information (e.g., condition reports, detailed accident investigations, and other data sources). This enriched database can then be processed using AI/ML technologies to detect correlations and patterns that may be indicative of weaknesses (i.e., inadequate feedback or flawed mental models) that were not detectable without these advanced computational tools.

A few years ago, researchers sponsored by the LWRS Program at Idaho National Laboratory (INL) developed a nuclear-specialized AI program called MIRACLE (Machine Intelligence for Review and Analysis of Condition Logs and Entries). This tool employs ML and NLP to review and categorize nuclear data. LWRS researchers have been working with MIRACLE so that its capabilities can provide insights pertinent to all levels of the organization, which will be analyzed further. For example, when condition reporting feedback in the supervisory control loop is analyzed using MIRACLE, unanticipated filters affecting feedback to supervisors can be corrected more quickly, allowing them more time to direct their attention to actions that will have the highest value relative to improving plant performance. During this evaluation, MIRACLE will also help identify which levels of the organization (e.g., leadership,

management, supervisors, workers) are responsible for the reported condition and for implementing the corrective actions. From a human and organizational factors perspective, of particular importance is how those who are responsible for the reported condition change how they address the performance shaping factors affecting that level of the organization to prevent the adverse condition from recurring.

From a systems-theoretic perspective, this research augments the corrective action program by identifying not only the affected loop but the organizational weaknesses within the affected loop. The first step is to identify which level contains the control weaknesses within the organization being evaluated, which may include:

- Executives who set the priorities
- Plant managers who plan the work
- Supervisors who oversee the work
- Workers who execute the work.

The products of these advanced computations can then be made available to human operators in well-designed GUIs (e.g., dashboards) tuned to the specific questions, tempos, and levels of abstraction that will be most useful at different levels of the organization to enhance situation awareness and expertise.

7. SUMMARY AND CONCLUSIONS

The goal of this research effort is to improve nuclear safety and reduce operating and maintenance costs through the real-time and proactive correction of social, organizational, and technical factors that are precursors to adverse events. The fundamental premise of this research is that the means for achieving this goal is to leverage the power of advanced digital processing capabilities to enhance reliability and efficiency in the management of NPPs. Thus, the focus of this research has been to develop a new model that makes the interdependencies between multiple layers of the organization more explicit. STOMP (Figure 8 and Figure 14) depicts the organization as a set of nested control loops in which outer loops set the context (or degrees of freedom) for activities within inner loops, and in which inner loops provide useful feedback to support decisions made in the outer loops. Performance in terms of safety, efficiency, and resilience depends on the *observability* and *controllability* potential within these nested control loops.

The focus of the research team's most recent efforts has been to construct an ontology (semantic structure) that provides a foundation for discovering meaningful patterns associated with the quality of the nested control structures. This semantic structure will be used to localize weaknesses within the multilayered organization and to describe the nature of those weaknesses in a way that will lead to interventions that will enhance *observability* and *controllability*, or in other words will improve communication and coordination.

While the current research has focused on deriving a semantic structure from incident and condition reports, STOMP has broad implications for the use of advanced computational methods (e.g., AI, ML, NLP, LLM) to process and filter information to enhance communications within and across levels of the organization. The semantic structure also has important implications for the design of GUIs tuned to the specific questions and decisions made within different levels of the organization. Finally, the semantic structure provides a framework for learning from incidents and designing appropriate training interventions to improve the quality of control within the organization.

8. REFERENCES

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., 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)*, 162-170, (virtual) Providence, RI. https://doi.org/10.1080/00295450.2022.2138065.

Dainoff, M., Hettinger, L., Hanes, L., and Joe, J.C. (2023). "Addressing Human and Organizational Factors in Nuclear Industry Modernization: A Sociotechnically Based Strategic Framework." *Nuclear Technology*, 209(3), 295-304, https://doi.org/10.1080/00295450.2022.2138065.

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.

Endsley, M.R. (1995c). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors,* 37(1), 32–64.

Flach, J.M. (2015). Situation Awareness: Context Matters! Journal of Cognitive Engineering and Decision Making, 9(1), 59 -72.

Flach, J.M. (2017). Supporting Productive Thinking: The Semiotic Context for Cognitive Systems Engineering (CSE). Applied Ergonomics, 59B, 612-624.

Flach, J.M. Simpson, B. & Kneeland, C. (2022). The dynamics of resilient decision making in organizations: A multi-layered model. *Proceedings of the International Conference on Naturalistic Decision Making.* Orlando, FL.

France, M. E. (2017). *Engineering for Humans: A New Extension to STPA*. Massachusetts Institute of Technology.

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.

Hollnagel, E., and Woods, D. D. (2005). *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*. CRC press.

International Atomic Energy Agency. (2015). Root Cause Analysis Following an Event at a Nuclear Installation: Reference Manual, IAEA-TECDOC-1756, Vienna, Austria.

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." INL/RPT-23-74217-Rev000, Idaho National Laboratory, Idaho Falls, ID. https:/doi.org/10.2172/1879683.

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

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.

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. and Thomas, J. (2018). "STPA Handbook." https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.

Rasmussen, J. (1986). *Information Processing and Human-Machine Interaction*. New York: North-Holland.

Rasmussen, J., and Svedung, I. (2000). *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.

Thomas, J. (2019). "System-Theoretic Process Analysis (STPA): Engineering for Humans." https://psas.scripts.mit.edu/home/wp-content/uploads/2019/04/STPA-Engineering-for-Humans.pdf

APPENDIX A
BRIEFING PAPER

Briefing Paper

By Jeffrey Joe, John Flach, Pat Murray, and Mary Detroff

August 2024

LWRS LIGHT WATER REACTOR SUSTAINABILITY

The Socio-Technical-Organizational Modeling Process

Improving Plant Performance by Reducing Unplanned Significant Events

Introduction

The U.S. commercial nuclear industry is actively working to lower operations and maintenance costs while at the same time maintaining their outstanding safety and reliability record. Reducing costs associated with complying with various reporting requirements is a particular focus area. For example, when adverse events occur, they are required to be reported and corrected, thus leading to higher operating costs. The goal of this research effort is to improve nuclear plant performance and reduce operating and maintenance costs through the real-time and proactive correction of social, organizational, and technical factors that are precursors to adverse events before they occur.

Research developing analytic methods and tools to support the assessment and management of sociotechnical risks in nuclear power plants (NPPs) is being conducted as part of the Department of Energy's Light Water Reactor Sustainability Program. In partnership with industry, this research reduces compliance costs through effective information and work automation, and through improving organizational situation awareness. That is, the fundamental premise of this research is that compliance costs can be reduced by developing a new model that makes the interdependencies between multiple layers of the organization more explicit.

Summary of Research

By extending and adapting the Systems-Theoretic Accident Modeling and Processes (STAMP) Framework (Leveson, 2011) to describe human and organizational processes as control structures, as seen in Figure 1, a multilayered model was developed to make the socio-technical and organizational constraints on managing and operating a NPP more explicit. As seen in Figure 2, the Socio-Technical Organizational Modeling Process (STOMP) characterizes the organization as a set of hierarchical control loops in which higher loops set the

Figure 1. Extending Levenson's (2011) generic control structure to describe human and organizational processes as control structures.

U.S. DEPARTMENT OF ENERGY

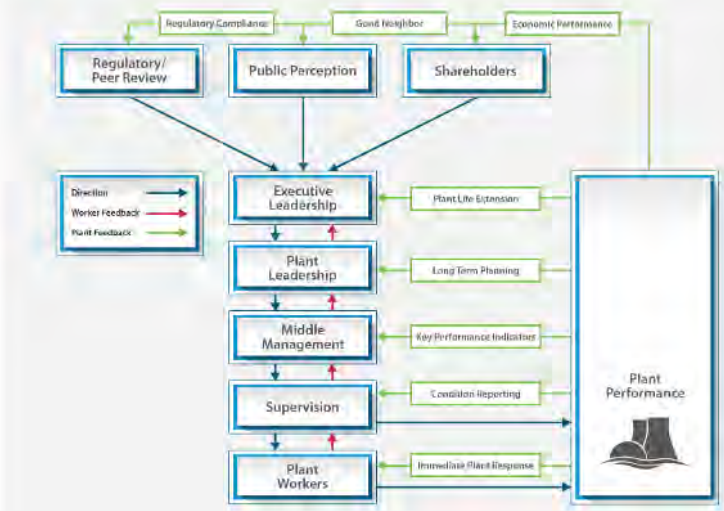


Figure 2. Hierarchical control structure of a nuclear facility.

context (or degrees of freedom) for activities within lower loops, and in which lower loops provide useful feedback to support decisions made in the higher loops. Performance in terms of safety, efficiency, and resilience depends on the observability and controllability potential within these nested control loops.

A scheme (i.e., ontology or semantic structure) for analyzing and coding incidents (e.g., condition reports) was also developed with the goal of localizing problems within the multilayered organization, identifying contributing factors, and recommending potential interventions. Table 1 illustrates critical semantic relationships in the database. Variables in the global column reflect aspects of the incident (e.g., condition report) from which the data were obtained. The other columns reflect specific variables of steps derived from the descriptions of the incident. These include step identifiers, attributes associated with the level within the organization structure involved, attributes associated with the cause of the incident, and attributes associated with the severity of the incident.

Global	Step			
	Identity	Level/Loop	Cause	Severity
Station Tracking Number Title Time Report Process Equipment Severity Report Type	Sequence Number Date/Time Title	Affected Process Feedback Signal Affected Loop Responsible Organization Affected Control Structure	Failure Mode Performance Shaping Factor Human Factor	Severity/Impact

Table 1. Coding categories of the relationships in the semantic structure.

The semantic structure illustrated in Table 1 provides a meaningful basis for making inferences from patterns in the database about the overall health of the organization. The attributes in the level/loop column help to localize

problems within the nested control structure illustrated in Figure 2. The attributes in the cause column allow inferences about the nature of the problems. Attributes in the severity column allow inferences about the significance of the problem. Together these categories provide a basis for specifying the interventions needed to improve performance.

Preliminary Analysis

The research team used the schematic structure to perform a detailed analysis of a significant event at a commercial NPP and plotted the outcome of our analysis on the layered loop model to highlight the areas of weakness. The team compared its results to that of the original root cause analysis and presented the differences in findings to a root cause expert from that utility to get critical feedback on the conclusions. Although different from the outcome of the analysis performed by the utility, the expert was intrigued with the outcome and expressed interest in helping to evaluate more test cases to further develop STOMP.

The findings from this analysis provide an early indication that by strengthening a control loop, an organization will not simply be reducing the likelihood of a specific event, but the organization will be more resilient and less susceptible to unsafe operations. The organization's capacity to deal with a wide variety of anticipated and unanticipated threats is increased, because the organization will make better decisions when they have even better organizational situation awareness. The practical result is the potential ability to reduce incidents by 30%, with accompanying cost savings (Joe, Hettinger, Yamani, Murray and Dainoff, 2023).

Next Steps

Integration with Artificial Intelligence

While the current research has focused on deriving a semantic structure from incident and condition reports, STOMP has broad implications for using advanced computational methods (e.g., artificial intelligence, machine learning, natural language processing, large language models) to process and filter information to enhance communications within and across levels of the organization.

Thus, the next step in the development process will be to formalize the logical or computational formulae utilizing the STOMP coding scheme that will be the basis for an automated inference engine or algorithm using big data analytics (i.e., artificial intelligence and machine learning). These algorithms could then be used to identify socio-technical-organizational weakness that go beyond specific incidents to reflect control weakness in a plant, a fleet plants, or across the entire commercial nuclear industry.

Developing Interfaces and Improving Organizational Learning

The semantic structure also has important implications for the design of graphical user interfaces tuned to the specific questions and decisions made within different levels of the organization. Finally, the semantic structure provides a framework for learning from incidents and designing appropriate training interventions to improve the quality of control within the organization.

Conclusion

Although nuclear power plants are engineered to have high reliability, by improving organizational effectiveness, plant performance will improve even further, reducing costs and increasing efficiency and safety. This research has developed STOMP, which can be combined with artificial intelligence, as means to identify and correct weaknesses in organizational control structures in order to improve overall NPP performance.

Contact

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

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

References

Flach, J., Dainoff, M., Murray, P., Hettinger, L., Yamani, Y., and Joe, J.C. (2024). *Mapping Data to Support Optimum Work Automation: The Socio-Technical-Organizational Modeling Process*, INL/RPT-24-80094, Idaho National Laboratory: Idaho Falls, ID

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