INL/RPT-22-69058-Revision-0

Using Systems Theoretic Process Analysis and Causal Analysis to Map and Manage Organizational Information to Enable Digitalization and Information Automation

September 2022

Marvin Dainoff, Patrick Murray, Jeffrey C Joe, Anna Hall, Johanna H Oxstrand, Larry Hettinger, Yusuke Yamani, Craig A Primer

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/RPT-22-69058-Revision-0

Using Systems Theoretic Process Analysis and Causal Analysis to Map and Manage Organizational Information to Enable Digitalization and Information Automation

Marvin Dainoff, Patrick Murray, Jeffrey C Joe, Anna Hall, Johanna H Oxstrand, Larry Hettinger, Yusuke Yamani, Craig A Primer

September 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

INL/RPT-22-69058

Light Water Reactor Sustainability Program

Using System-Theoretic Accident Model and Processes and Causal Analysis to Manage Organizational Information to Enable Digitalization and Information Automation

September 2022

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-22-69058

Using System-Theoretic Accident Model and Processes and Causal Analysis to Manage Organizational Information to Enable Digitalization and Information Automation

Marvin J. Dainoff, Patrick J. Murray, Jeffrey C. Joe, Anna Hall, Johanna Oxstrand, Larry J. Hettinger, Yusuke Yamani, and Craig Primer

September 2022

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

ABSTRACT

The nuclear industry has identified data digitalization and information automation as topics needing focused research. In response, Light Water Reactor Sustainability (LWRS) Program researchers are developing and evaluating methods for effectively mapping and managing plant data through System Theoretic Process Analysis (STPA), System-Theoretic Accident Model and Processes (STAMP), and Causal Analysis. The results provide an optimized process for converting data to information enabling deeper insight, and more effective action – thereby allowing utilities to operate safely and cost-competitively. This research includes developing methods to evolve plant data into useful plant insights and validates the use of STPA and STAMP using high-level safety constraints in the United States Nuclear Regulatory Commission's problem identification and resolution process (i.e., a plant compliance information gathering activity).

Researchers are also investigating how human and technology integration principles, digitalization, and information automation enable the conversion of data to information or "data evolution". The next step in this research, described in the following sections of this report, is to map out data evolution in other plant compliance activities – event investigations and root cause analyses. This LWRS Program-supported research and development contributes to the comprehensive guidance for utilities considering or undertaking full nuclear plant modernization.

CONTENTS

FIGURES

TABLES

ACRONYMS

CAP	corrective action program
CAST	causal analysis based on STAMP
CCU	Cardiac Care Unit
CWA	cognitive work analysis
DEHC	Digital Electro-Hydraulic Controller
DOE	Department of Energy
HTI	human technology integration
I&C	instrumentation and controls
IDEAS	intervention design and analysis scorecard
ION	integrated operations for nuclear
INL	Idaho National Laboratory
LWRS	Light Water Reactor Sustainability
MEAH	means-end abstraction hierarchy
NGT	nominal group technique
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
R&D	research and development
RCA	root cause analysis
RPV	reactor pressure vessel
SCS	safety control structure
STAMP	system theoretic accident model and process
STPA	systems-theoretic process analysis
U.S.	United States
WDA	work domain analysis

USING SYSTEM THEORETICAL ACCIDENT MODEL AND PROCESSES AND CAUSAL ANALYSIS TO MANAGE ORGANIZATIONAL INFORMATION TO ENABLE DIGITALIZATION AND INFORMATION AUTOMATION

1. INTRODUCTION

The United States (U.S.) Department of Energy (DOE) Light Water Reactor Sustainability (LWRS) Program Plant Modernization Pathway is conducting research and development (R&D) that lays the groundwork for the digital transformation of the nuclear industry, resulting in an advanced concept of integrated operations that allows for commercial nuclear power plants (NPPs) to operate cost-competitively with other means of generating electricity. A recent work by Hunton et al. (2020) provided a compelling business case against the like-for-like replacement strategy of individual instrumentation and control (I&C) systems. They found that the cost to maintain systems in their current form is economically unsustainable. As seen in Figure 1, using the cost of a replacement circuit card as an example, the cost to maintain the systems in their current form is much greater than previously estimated due to increasing obsolescence management costs.

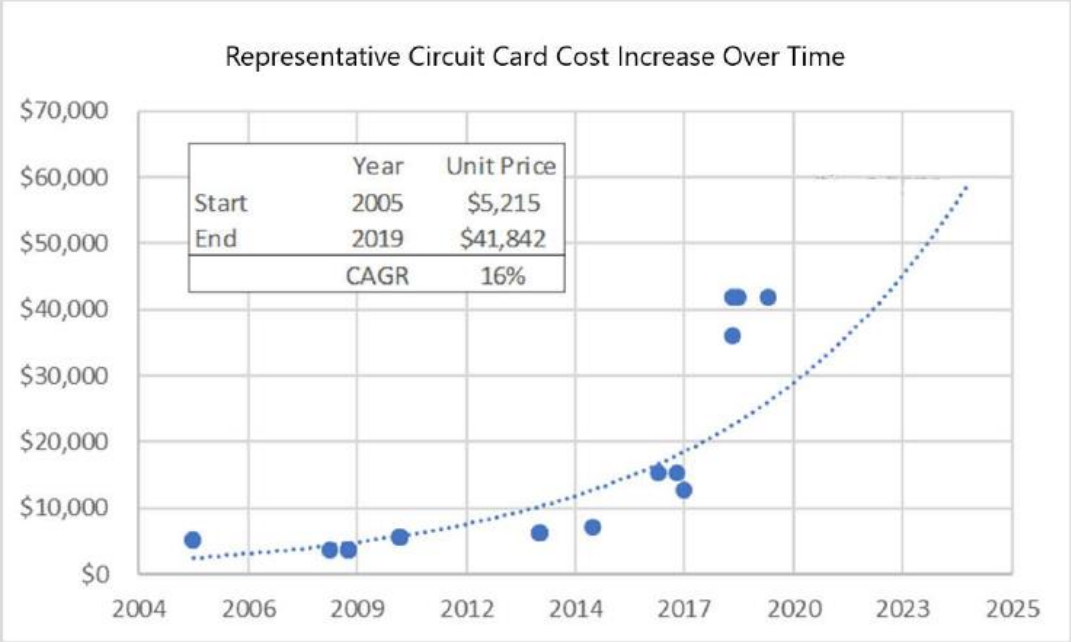

Figure 1. Representative example of circuit card cost escalation over time.

Thus, LWRS Program researchers at Idaho National Laboratory (INL), in collaboration with utility partners, are actively working to support the digital transformation of the current U.S. fleet. The LWRS Program provides recommendations based on R&D results through which the current nuclear fleet can transition to an economically sustainable future. For example, LWRS Program researchers at INL have developed a modernization roadmap for nuclear utilities to follow. As shown in Figure 2, the high-level objectives focus on modernization solutions within a sustainable business model, which will achieve the high-level goals of extending the life and improving the performance of the existing fleet through modernization techniques and improved processes. The Plant Modernization pathway's roadmap

identifies four distinct research areas: I&C (digital) architecture, data architecture and analysis, human and technology integration (HTI), and integrated operation for nuclear (ION). HTI has the responsibility integral to a systems engineering approach to combine these areas into a more integrated and organized set of solutions.

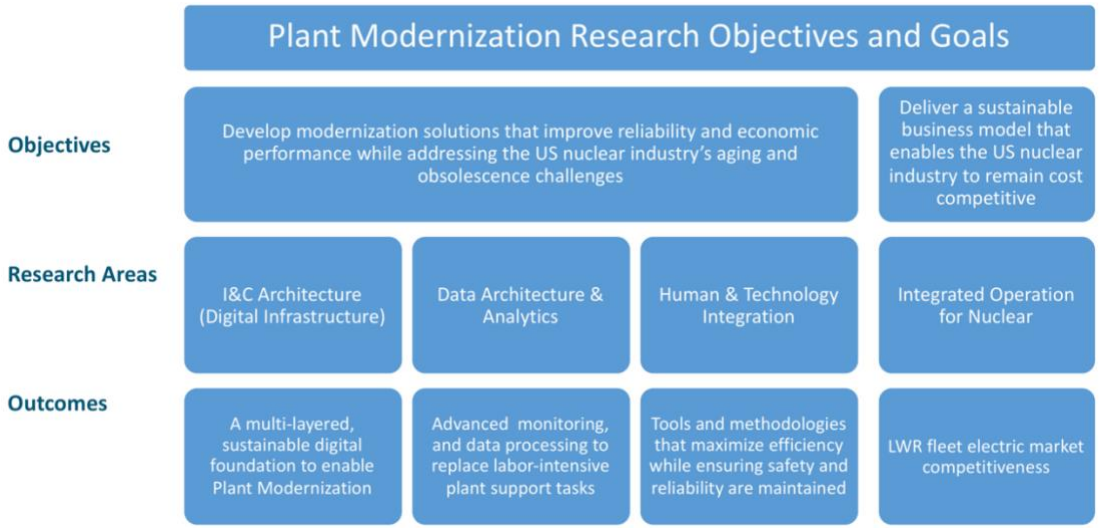

Figure 2. R&D roadmap for the LWRS Plant Modernization Pathway.

1.1 Conceptual Framework

To enable the coordination of the R&D focus areas in the pathway, LWRS Program researchers developed the human and organizational factors approach to nuclear modernization, which is described in detail by Dainoff et al. (2020). There are many excellent sources of human factors engineering guidance in the nuclear energy domain, and Dainoff et al. (2020) does not replace these sources. Rather, the goal for that report was to supplement this guidance by identifying methods to achieve the integration, consensus, and coordination called for in these publications.

Building on a traditional human factors engineering foundation, Dainoff et al. (2020) employed a human and organizational factors approach to the broad area of sociotechnical systems relevant to nuclear modernization. This approach is based on a literature review focused on the tools and methods that might be applicable. This review was constrained by limiting consideration to those methods for which there was evidence of active communities of practice in active engagement solving real world problems. As such, Dainoff et al. (2020) developed a strategic framework for the effective integration of human and organizational expertise within nuclear industry modernization efforts based on the following sociotechnical systems literature:

- Macroergonomics (Kleiner et al. 2015)
- Cognitive systems engineering
    - Cognitive work analysis (CWA) (Rasmussen, Pejtersen, and Goodstein 1994)
    - Work domain analysis (WDA) (Rasmussen, Pejtersen, and Goodstein 1994)
    - Resilience engineering (Woods and Hollnagel 2006)
    - System-theoretic accident model and processes (STAMP) (Leveson 2011) and system theoretic process analysis (STPA) (Leveson and Thomas 2018)
- Naturalistic decision-making (Klein, Orasanu, Calderwood, and Zsambok 1993).

- Macrocognition and cognitive task analysis (Crandall, Klein, and Hoffman 2006; Schraagen, Militello, Ormerod, and Lipshitz 2008)

- Human-systems integration (Booher 2003).

The goal of the sociotechnical systems approach, as applied to systems design, is the joint optimization of social-organizational and technical subsystems. Additionally, an argument from the domain of resilience engineering describes the interdependence of three system performance criteria: effectiveness (accomplishment of mission), efficiency (optimization of resources), and safety (avoidance of injury or damage). Excessive emphasis on any one criterion at the expense of the others is likely, in the long run, to result in overall system failure (Hollnagel 2006; Hollnagel and Woods 2005).

Sociotechnical systems theory provides a pathway to these goals and is foundational for several core disciplines within the human factors engineering community, including macroergonomics, cognitive systems engineering, macrocognition and cognitive task analysis, and human systems integration (Dainoff 2009). As shown in Figure 3, the specific methodologies include WDA, STPA, concept mapping, interviews, nominal group technique (NGT), intervention design and analysis scorecard (IDEAS), and consensus. Note that Figure 3 itself is an example of concept mapping.

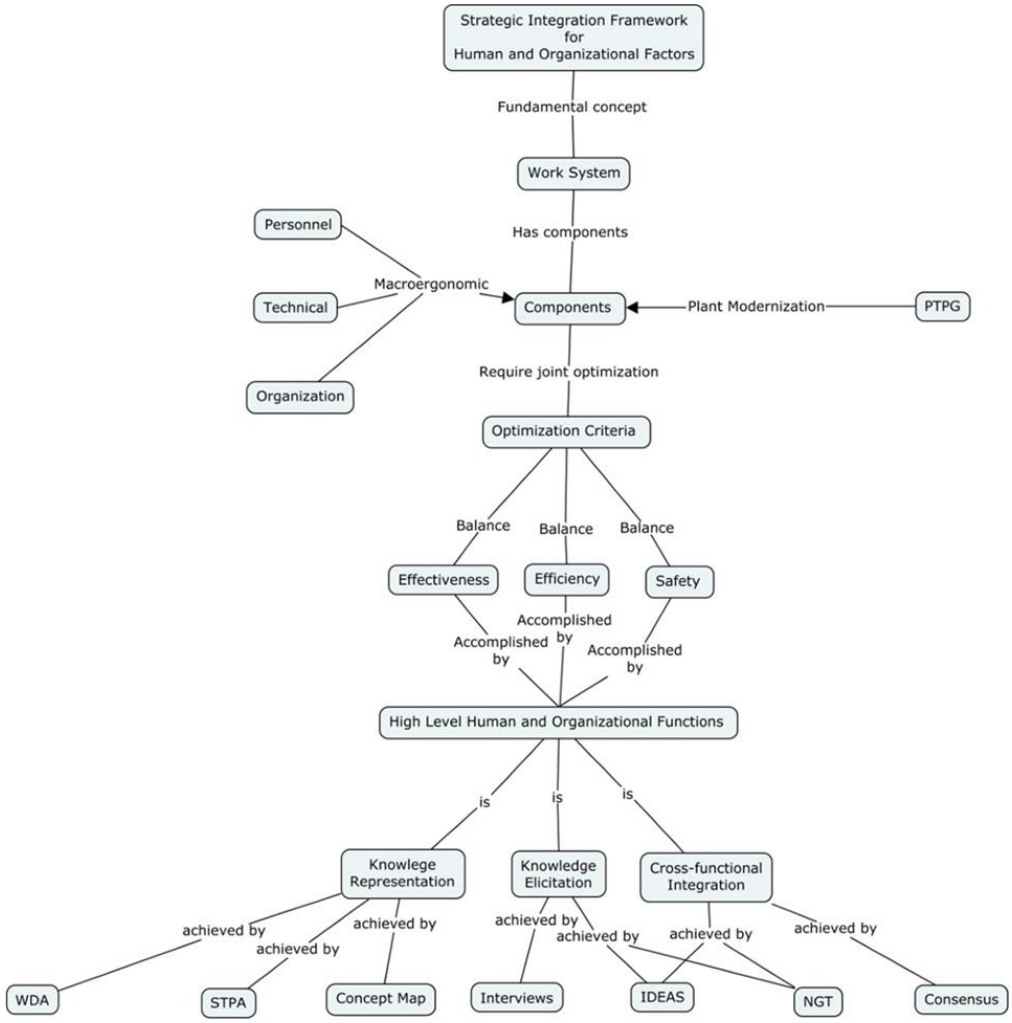

Figure 3. Strategic integration framework presented as a concept map[1].

[1] This figure was created using Cmap tools (cmap.ihmc.us)

1.2 Information Automation

More recently, LWRS Program Plant Modernization Pathway researchers developed an approach accounting for HTI issues throughout the various phases of system design, testing, and implementation (Dainoff, Hettinger, and Joe 2022). The approach also looked at how HTI helps promotes effective design. Specifically, these researchers developed and demonstrated an approach to the design and implementation of advanced, automated systems intended to increase operational efficiencies at NPPs. This research also proposed automating the mapping of data from plant systems and processes to application needs, thereby significantly reducing the human workload currently required to execute these tasks.

One key insight from Dainoff, Hettinger, and Joe (2022) is that—as seen in Figure 4—when examining existing systems, the control structure produced in an STPA can be used to define high-level safety constraints prior to implementing specific system functionality, which is important when assessing digitalization and information automation aspects of data evolution.

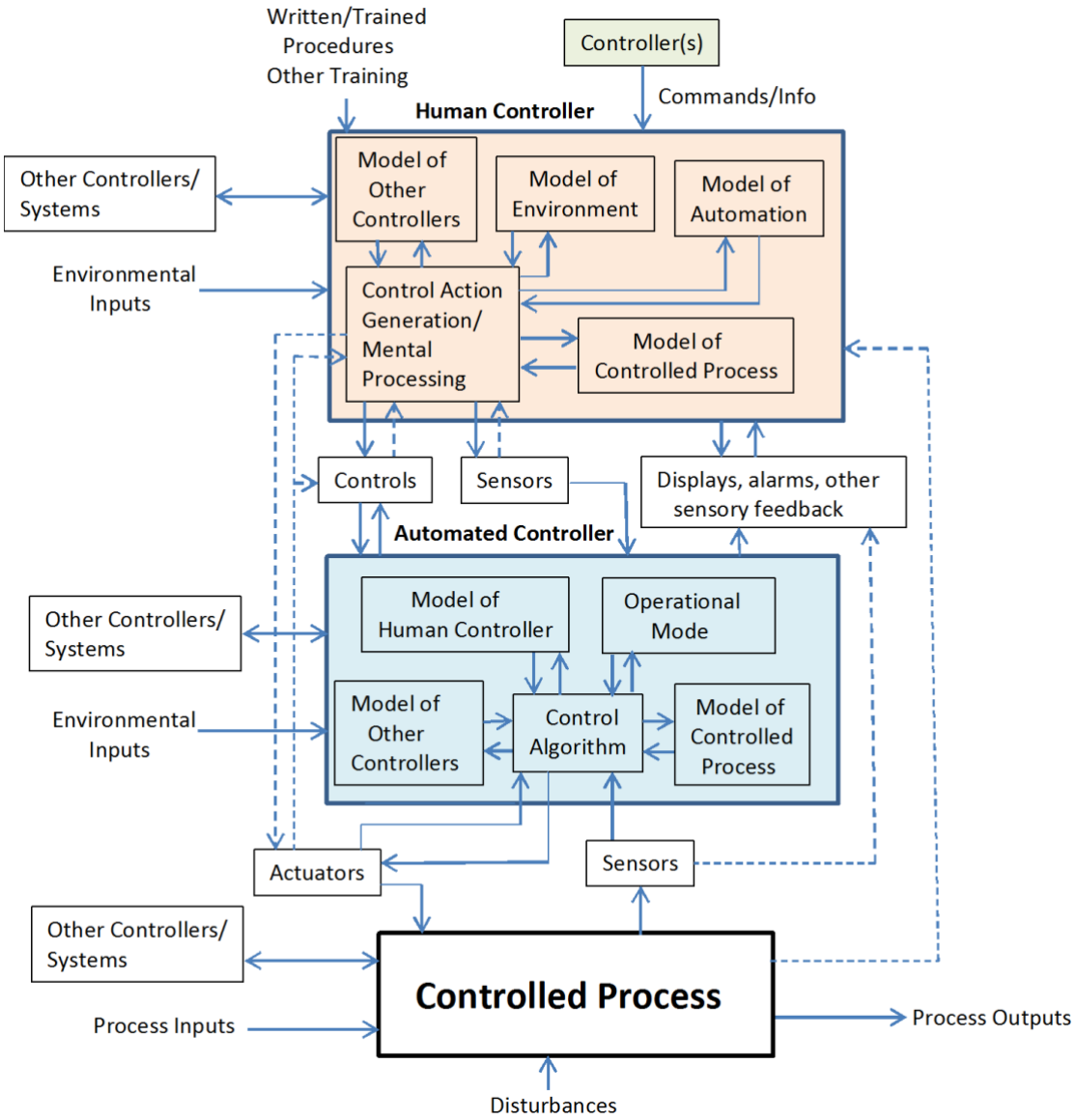

Figure 4. Generic human and automated controllers (Leveson 2020, Figure 10).

Information automation and human factors help NPPs integrate their operations and achieve full nuclear plant modernization. This research reduces operations and maintenance costs by improving work management systems and streamlining work processes.

1.3 Digitalization

Digitalization is another important concept for the LWRS Plant Modernization Pathway that first needs to be differentiated from digitize. To digitize something is to convert information from an analog format into a digital format, but to digitalize is to use digital technologies (i.e., technologies that are based on that information in a digital format) to synthesize work processes as a means to integrate operations. Digitalization is a step that comes after digitizing. Figure 5 shows how the media and medium in which music and other audio recordings are played have gone through the process of digitization (e.g., from vinyl albums and cassette tapes to compact discs and.mp3 files) and then digitalization (e.g.,.mp3 files that are streamed over the internet via a music service provider).

Figure 5. The digitization and digitalization of recorded audio and music.

In the specific context of the LWRS Program, digitalization describes the process and methods to map and manage digitally formatted data to achieve ION. The commercial nuclear industry still has many paper-based work processes, which are very labor-intensive, manually performed activities. In addition, much of the equipment in an NPP, while safe and reliable, is often not digitized or, if digitized, not digitalized. Without a means to easily connect this equipment into a digital infrastructure, equipment monitoring must be performed by people walking around the plant making surveillances. So, in the context of NPPs, the first step is to digitize, for example paper-based procedures to computer-based procedures, and analog gauges and meters to digital ones. Once the data has been digitized in NPPs, the next step is to digitalize the data. Digitalization involves using digital technologies to map, manage, and convert the data into information that enables organizations to gain insights on the status of their work and processes such that they can make better decisions and take more effective actions (i.e., data evolution).

The commercial nuclear industry has long recognized the importance of digitization and has been digitizing many aspects of their operations. For example, paper-based strip chart recorders in the control room are now largely digital recorders, as are many other non-safety related I&C systems, from single-loop interface modules to control valves to digital turbine control and digital feedwater control systems. Many utilities are also actively exploring the transition from paper-based procedures and work packages to computer-based procedures and electronic work packages. While these changes to digitize technologies used to operate the plant are an important first step, the nuclear industry must move a step further towards digitalization to achieve the goals under ION (Thomas et al. 2020). Digitalization is a means of automating the evolution of data to information to insights to actions so that work processes can be more integrated and cost-effective because the nuclear industry needs to operate more efficiently to be even more cost-competitive with other electricity generation technologies.

1.4 Research Goals

The overarching goal of this LWRS Program–supported R&D project is to provide planning tools and comprehensive guidance to utilities considering or undertaking full nuclear plant modernization. The results of this research will provide the nuclear industry with a comprehensive and usable solution, including guidance, lessons learned, methods and planning tools.

Currently, this research is working to provide guidance on digitalization and information automation to enable the evolution of data to information, insight, and action—thereby allowing utilities to operate safely and cost-competitively with all other electrical generation sources.

As mentioned previously, LWRS Program researchers recently started investigating how HTI principles, digitalization, and information automation enable data evolution (Dainoff, Hettinger, and Joe 2022). These researchers are currently in the process of validating the use of STPA to define high-level safety constraints in the U.S. Nuclear Regulatory Commission's (NRC's) problem identification and resolution process (i.e., a plant compliance information gathering activity). The next step in this research, which is described in the following sections of this report, is to map out data evolution in a use case to identify inefficiencies in another aspect of plant compliance information gathering and communication activities—event investigations and root cause analyses (RCAs).

2. APPLICATION OF CAST TO UNDERSTAND CAUSAL ANALYSIS IN EVENT INVESTIGATION

This section describes the application of STPA, and causal analysis based on STAMP (CAST) to understanding causal analysis in corrective action program (CAP) reportable events.

2.1 Introduction

STPA is a specific method derived from a more general model of causality called STAMP developed by Leveson and her colleagues at the Massachusetts Institute of Technology (2011, p. 13). This model changes the emphasis in system safety from preventing failures to enhancing behavioral safety constraints. Accident causality is extended to the interaction among components, and the focus is on control rather than reliability. Leveson considers her work an extension of the groundbreaking work in CWA by Rasmussen, Pejterson, and Goodstein (1994).

CAST is, as the title indicates, a STAMP-based method specifically aimed at accident analysis. It does not look for single causes but rather examines the entire sociotechnical system to identify weaknesses in the safety control structure (SCS). Its goal is to: "… get away from assigning blame and instead shift the focus to why the accident occurred to prevent losses in the future" (2011, p. 345). In traditional accident analysis, it is difficult to avoid hindsight bias. Leveson (2011) makes the fundamental assumption that most individuals involved in accidents do not come to work planning to create a problem. Instead, 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.

An example presented as part of a CAST tutorial illustrates these principles. Leveson, Malmquist, and Wong (2020) describe a case where a major hospital carried out a heart transplant procedure. The patient was handed off to the surgeon by the Cardiac Care Unit (CCU) nurse, and surgery was carried out without the patient being given immunosuppression medication. While the patient survived the surgery, he died soon after from transplant rejection. The typical root cause analysis would blame both the nurse and surgeon. The nurse did not give the medication nor tell the surgical team that it had not been given. The surgeon started surgery without checking to see if the medication was given despite going through a checklist prior to surgery.

However, a CAST analysis determined that it had been several years since a transplant had been done in that hospital. The hospital was trying to develop a new capability. Moreover, it was standard procedure for preoperative antibiotics to be administered in the operating room, not in the CCU. Therefore, there was no expectation on the part of the CCU nurse that she was required to administer medications. Moreover, while the required medication order was entered in the Electronic Health Record, the Electronic Health Record structure provides no indication of (a) who has responsibility for administration or (b) if and when the medication was actually administered. Hence, other staff members who would normally have responsibility for trouble-shooting—such as the circulating nurse or surgical fellow—had no basis for challenging their expectations that the medication had been given.

Finally, in examining the role of the operating room administration—which is also a node in the SCS—it became clear that there had been several similar medication errors in the past, but the resulting RCA always stopped at the point of blaming medical staff. The concept of "blame and shame" is apparently built into medical culture as an approach to error mitigation.[2]

[2] In the narration of the above case, Leveson (2020) indicated that the initial submission of this study for publication was rejected by the journal editor without review. The editor simply commented that everyone knows that medical errors are due to a few bad apples.

2.2 CAST Application to DEHC-Related SCRAM Incident

In this section, a simplified version of CAST will be applied to a detailed RCA of a SCRAM[3] incident related to a new digital I&C system, the Digital Electro-Hydraulic Controller (DEHC). The description will be generic but based on actual records. This application is unlike STPA, which examines the entire domain of interest. Instead, CAST focuses on those components relevant to the event. Having said that, the CAST process is necessarily iterative, since examining weaknesses in the SCS may require an addition of additional components.

The example is particularly pertinent since it relates to a loss (i.e., SCRAM) associated with a digital upgrade. An unexpected SCRAM at an NPP can challenge many mitigation and recovery systems, as well as invoke human error precursors, uncovering other collateral issues that further challenge plant safety. The investigators of the original incident noted that digital upgrades have unique attributes and risks that present different technical challenges than analog modifications. Technical challenges are less obvious and take a more advanced level of expertise and validation than challenges caused by failures of analog equipment.

2.2.1 The Event

The day shift operations crew of Unit Bravo of a two-unit NPP was in the process of a post-outage reactor startup, in which their task was to gradually increase steam pressure in the reactor by controlling the position of the turbine steam bypass valves, using the new DEHC control for the first time. During the outage, this turbine control system had been upgraded from the analog version. Although this modification had been recently performed at Unit Alpha, changes were made to add additional capabilities to this new digital controller, based on feedback from the operations department after having utilized the new digital controller on the other unit.

The crew employed a standard procedure, Method A. The procedure specified the sequence: Control X is activated until a predetermined pressure level is achieved, then Control Y is activated. However, the panel operator discovered that, while attempting to control reactor pressure in accordance with the written procedure, Control Y was unavailable (i.e., the pushbutton was greyed out on the new digital controller human system interface). As a result, reacting to the unanticipated condition, he activated Control Z, which closed all of the steam bypass valves immediately, triggering a reactor water level transient and an automatic reactor SCRAM.

In the ensuing investigation, it became clear that the Method A procedure documentation had not been modified to reflect the new capabilities of the DEHC. Specifically, Controls X and Z had been modified for emergency use and, when activated, resulted in steam flow rates different than was the case for their previous analog version.

Also, the previous evening, the night shift operations crew had realized similar problems with Method A. However, they were able to recover and go on to use an alternative approach (Method B) to accomplish their task. They did not communicate their negative experience with Method A to the other operations crews.

2.2.2 CAST Outline

Figure 6 depicts the basic outline of a CAST analysis. This figure is modified from the CAST Handbook (Leveson 2019). Additional information on CAST can be found in a tutorial (Leveson, Malmquist, and Wong 2020) and in an example of an analysis of a radiation therapy accident (Silvis-Cividjian 2022.)

[3] A SCRAM is a term that the U.S. nuclear industry uses for a reactor trip.

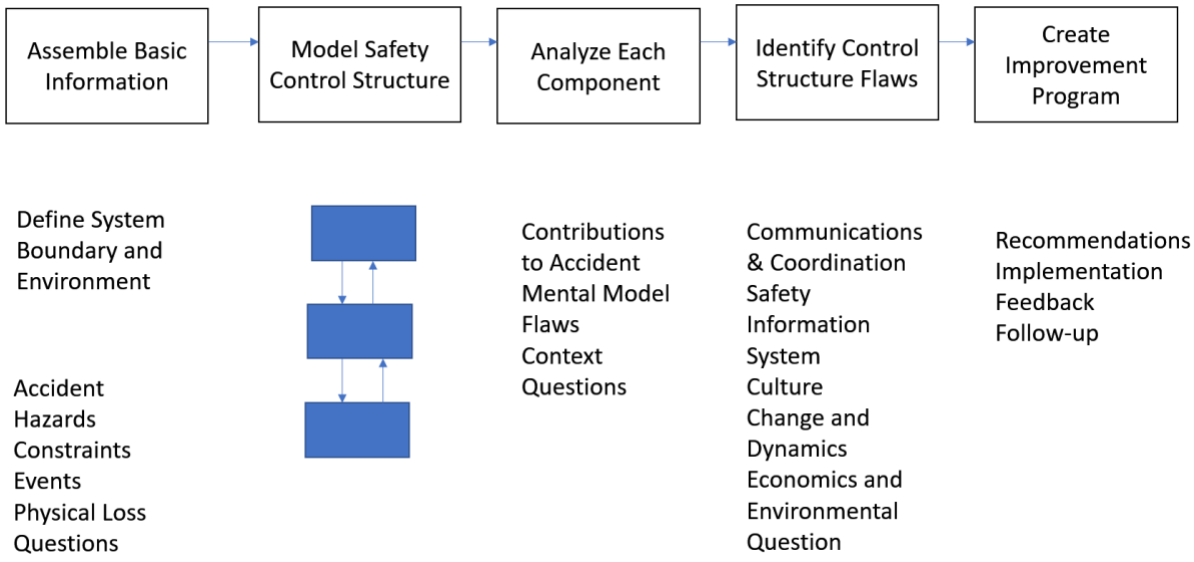

Figure 6. Basic outline of CAST process[4].

2.3 Part 1. Assemble Basic Information

The system boundary includes the actual SCRAM event as well as the earlier process of upgrading the controller and the operating procedures (i.e., Method).

An important first step is defining hazards and safety constraints. Inherent in the STAMP model, relevant to both STPA and CAST, are the relationships among hazards, constraints, and the SCS.

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

Table 1 on the next page lists the hazards and safety constraints for this example.

[4] Modified from Leveson, 2019, p. 34.

Table 1. System hazards and safety constraints.

System Hazard #1: Uncontrolled change in reactor reactivity
Safety Constraints:
Reactivity levels must always be controlled within the safety parameters of the plant's design basis
Reactor safety systems must be available and function properly in the event there is an unplanned or uncontrolled change in reactivity
Means must be available to contain radiation in the event that reactor safety systems are unable to maintain the reactivity within the design basis parameters
Plant procedures and processes need to ensure that modifications that can affect reactivity levels are fully vetted to prevent unplanned reactivity excursions
U.S. NRC regulations require a reactor licensee to have and follow effective procedures and processes in order to operate a nuclear reactor
System Hazard #2: Reactor pressure vessel (RPV) level
Safety Constraints:
Reactor water level must be maintained within the design basis levels to protect the core and to prevent unplanned releases of radioactive water
DEHC system must route steam properly to maintain design basis reactor water levels
Reactor safety systems must be available and function properly to ensure that reactor water level is maintained within the plant's design basis, in the event normal operating systems fail to maintain proper water level

A major step in the analysis is collecting information about the event. The goal is to be comprehensive, seeking as many contributing factors as possible to avoid similar events in the future. A typical procedure is to construct a proximate events table. Table 2 presents proximal events leading to a SCRAM for this exemplary case. In constructing this table, the focus should not be on selecting one or two causes. Instead, the purpose of the table is to generate questions for the investigation. This table is meant to be the primary input to the investigation.

Table 2. Proximal events leading to SCRAM.

ID	**Event**	**Questions**
1	Shift operations request modification of DEHC to allow more precision in Method A and emergency capability for Controls X and Z. Request based on lessons learned from previous experience.	What was the process for reviewing submissions to the engineering modification process?
2	Modification team submits a request to vendor. Vendor delivers DEHC with new control sequence W-Y to afford more precision in Method A, but Controls X and Z are omitted.	What was the process for transmittal and review of requests between the modification team and vendor? What was the reason for Controls X and Z being omitted?
3	Modification team tests functionality of Controls W and Y. Requests vendor to add modified Controls Y and Z. Controls are added and functionality tested.	Is making modifications during the testing procedure a normal method of operation?
4	Procedure writing team generates many procedure changes for DEHC. Method A procedure is not changed. There was no clear owner of the changes for the Method A procedure so that each change could be tracked and reviewed by a knowledgeable individual.	Why was Method A not changed?

ID	Event	Questions
5	Overall validation of DEHC procedures was carried out on simulators. However, only standard test protocols are followed. Validation of Method A is not carried out.	Why was Method A not validated?
6	Procedure revision process was not followed by the procedure reviser, procedure reviewer, and procedure approver, reducing the effectiveness of barriers put in place to prevent inadequate procedure revisions.	Why were these standard review procedures not followed?
7	The procedure was modified to be equally applicable to Units Alpha and Bravo despite differences in function of DEHC between units.	Who authorized this modification?
8	Qualified departmental reviewer does not review Method A. Senior management and corporate management approves modifications.	Was the fact that Method A was not changed the reason for the lack of qualified review by department and management?
9	Training does not develop revised instructions for Method A.	See previous question.
10	Operations procedures were revised by a non-station person unfamiliar with the site procedure revision process	Why did the plant allow a non-station person to revise operations procedures that could have a consequential impact on the station?
11	During startup, the night shift has problems using Method A; Sequence X followed by Y with pressure increasing too rapidly. However, they recover, stop work, and use an alternative, Method B, using different controls. They do not document their problems in their operations log.	Why did they not document their problems?
12	Day shift uses Method A to continue to increase steam pressure. Control X is activated but, being concerned about the resulting excessively rapid rise in pressure, the operator executes Control Y to stop activation. However, Control Y is inoperable. The operator then activates Control Z, which results in a rapid shut down of all values, creating a flow transient, and a subsequent SCRAM by the automatic reactor control system.	Were there differences between circumstances between the evening shift and day shift that led the evening shift to be able to shut down the operational sequence without SCRAM but not the day shift? Why was this sequence not simulated during pre-startup training?
13	Units Alpha and Bravo, which have conjoined control rooms with operators that are cross licensed on both units, used two different versions of the DEHC in which the same controls (X, Y) had different functional characteristics.	Why was this allowed? Why wasn't there a human factors expert on the team to review this significant change to the DEHC?

At this point, the CAST sequence described in Figure 6 will be split in two. Parts 2 and 3—modelling the SCS and analyzing individual components—will be done separately for the engineering modification phase and the actual SCRAM events. Parts 4 and 5—model SCS flaws and create improvement programs—will be applied to both sets of analyses.

2.4 Part 2. Model Safety Control Structure for Engineering Modification

Figure 7 depicts the SCS for the Engineering modification process. Following this analysis, a second CAST analysis will be performed on actual events leading to the SCRAM. A CAST analysis has the flexibility to divide the process into multiple portions if this seems appropriate.

The SCS follows the same control-theoretic logic as in STPA. Boxes in white are controllers, and boxes in grey are controlled processes. Outward arrows from controllers represent instructions or directions, but these instructions may include directing the flow of information—either from the controller or from the controlled process—to another source (e.g., a controller or controlled process). Inward arrows represent feedback, either to a controller, or directed information from a process.

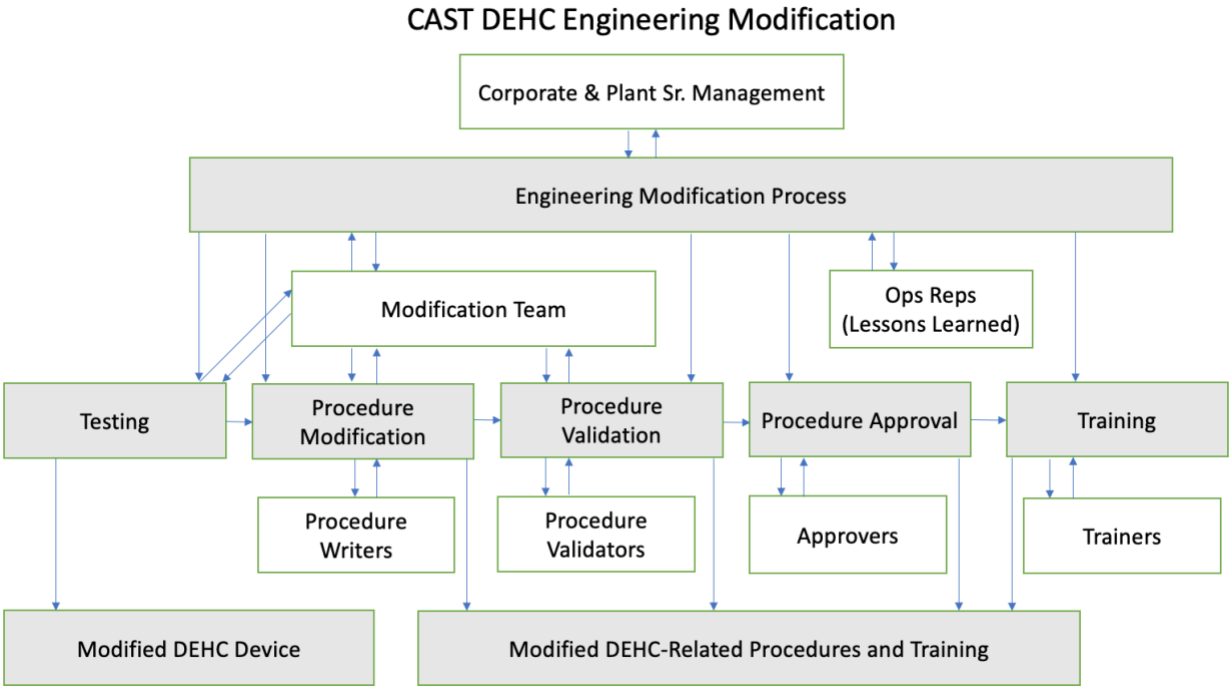

Figure 7. SCS for DEHC engineering modification process.

The SCS reflects the information obtained from the proximal events (Table 1) expressed in terms of controllers or controlled processes. In this example, corporate and senior management approved and controlled the engineering modification but did not think to challenge the fact that there would be operational differences in DEHC functionality between Units Alpha and Bravo. The engineering modification process is additionally controlled by inputs (requests) from the operations representatives and modification team. Since this SCS is limited to this particular incident, inputs from other controllers are not shown. CAST can be considered an iterative process; a subsequent analysis may require expanding the SCS.

The modification team also provides inputs and direction to testing, procedure modification, and procedure validation and receives feedback from each. In terms of the last two controller processes, two other sets of controllers, procedure writers, and validators, are also linked to these processes. In these cases, the modification team performs a supervisory function, while different individuals do the actual writing and validation (e.g., computer simulation). The procedure approval process reflects inputs from different levels of reviewers and approvers including a qualified department reviewer, a multidiscipline review, and senior management. Finally, there is a training process, controlled by a trainer. All of these intermediate processes, derived from the initial modification process, resulted in a modified DEHC

device, and a set of revised procedures and associated training materials. These are made available to shift personnel for operational use.

Having described the basic control structure, the next step is to examine possible reasons why this structure did not prevent the SCRAM. There are two steps to this process. The first (Part 3), looks at individual controllers and the roles they played in the incident. The second (Part 4) examines the control structure as a whole and the interactions among components.

2.5 Part 3A. Analyze Individual Components: Engineering Modification

Table 3 summarizes the results of this analysis and indicates each controller's responsibility within the SCS. Contributions reflect the extent to which actions, lack of actions, and decisions contributed to the hazardous state. Process flaws refer to either individual mental models or procedural flaws. Context refers to environmental or behavior-shaping factors that influence a controller.

Table 3. DEHC modification SCS individual controllers.

Controller	Responsibility	Contribution	Process Flaws	Context
Operations	Present equipment and procedure change recommendations to modification team.	Overconfidence by modification team that operations' plant experience would be a barrier to prevent technical flaws.[5]	Awareness of conflict between old and new versions of same controls?	Digital upgrade for a new and unfamiliar process.
Modification Team	Review submitted modifications, coordinate development process, coordinate testing process, coordinate and review procedure revision and validation.	Use of new sequence W-Y was not reflected in change in procedure and not validated. Nature of revised Controls X and Z not reflected in change in procedure and not validated.	Controls X and Z omitted from initial equipment build but added in during testing. Did not have knowledgeable shift representative available for review. Documentation procedures not followed. Chain of accountability not established.	Digital upgrade for a new and unfamiliar process. Inherently less transparent than previous electromechanical and analog control system.
Procedure Writer	Revise procedures based on information from modification team.	Method B revision did not include new procedures and redefinition of previous controls.	The possibility that information provided by modification team was overlooked. No single point of accountability for specific procedures.	Many different individuals were adding content to procedure changes.
Procedure Validators	Validate, using simulators, revised procedures.	Method B revision was not validated.	Why was a method that was part of the start-up process and used new logic not validated?	Digital electronics are very complex with many alternative pathways. There is always a cost-benefit

[5] Operations individuals are included on the modification team for their plant experience and technical expertise; however, their role in the administration of the procedure changes did not prevent important elements from being missed.

Controller	Responsibility	Contribution	Process Flaws	Context
				decision as to what is to be validated.
Approvers	Procedure quality reviewer verifies over all accuracy. Senior management and corporate representatives sign off on overall project.	Modification approval process did not catch the procedure revision deficiencies.	Unclear roles and responsibilities to assess or enforce quality or decide the threshold for overall approval is met.	Production time pressure.
Trainers	Develop training materials reflecting modifications.	Training for Method B using properly revised procedures not given.	Lack of awareness in upstream processes (modification, validation, and approval).	n/a

2.6 Part 3B. Model Safety Control Structure: SCRAM

As seen in Figure 8, the SCS is straightforward. The operators began to raise reactor pressure as part of its startup. They used the Method A procedure, starting with the X control, which opened the steam bypass valves more quickly than the operator expected, but when he went to use the Y control, which normally stopped valve motion, it was inoperative (i.e., pushbutton was greyed out). As a result, he operated the Z control, which also closed the valves at an unexpected rate, resulting in a unit SCRAM. The previous evening, the night shift had come close to experiencing the same effect. They stopped work but then successfully continued using an alternative method. They did not document their challenges with Method B nor discuss them in detail during shift turnover.

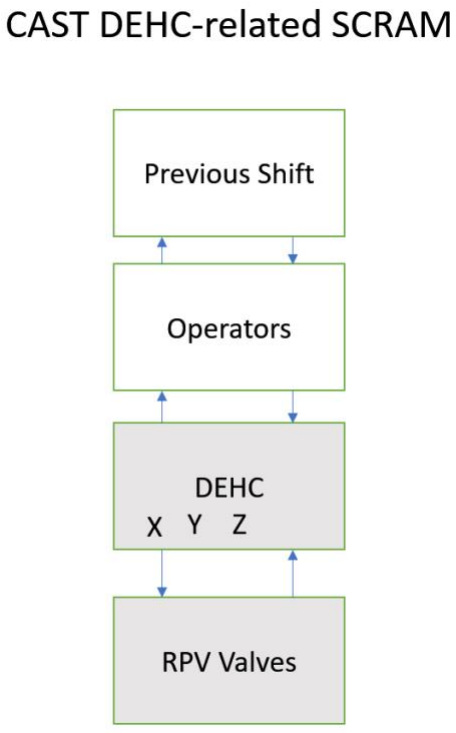

Figure 8. SCS for SCRAM incident.

2.7 Part 3C. Analyze Individual Components: SCRAM Incident

Table 4 on the next page shows the results of an analysis of the individual components of the SCRAM incident.

Table 4. Results of the analysis of individual components.

Controller	Responsibility	Contribution	Process Flaws	Context
Night (Previous) Shift Operators	Document problems that might impact overall operations.	Did not document or communicate shift issues with Method A.	Did not believe the incident rose to the level of needing to be reported.	Possible cultural bias against reporting near miss.
Day Shift Operators	Increase steam pressure following standard operating procedures.	Followed Method A which resulted in SCRAM.	Believed Method A to be an accurate set of instructions.	n/a

2.8 Part 4. Identify Control Structure Flaws

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

The process for hand-off between the project manager and plant technical leadership was not discussed in the formal report of the incident. However, there were clearly several deficiencies in communication and coordination.

- Despite a common procedure document, Units Alpha and Bravo used two different versions of the DEHC in which the same controls (X, Y) had different functional characteristics. Given that the same operators worked at 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 missing.
- It is unclear who was responsible for ensuring that existing procedures for modifications were actually followed by the project team.
- Just-in-time training of operators prior to startup did not cover Method A. Moreover, the training materials used in this training did not reflect an accurate representation of DEHC. Specifically, Controls X and Z were not shown. Why were updated drawings not provided to the training personnel?

The process of converting to digitalization has particular challenges. Expected benefits of digitalization might be counteracted by performance deficiencies as operators stumble to understand controls. Compared to traditional analog systems, it is easier in digital systems to modify or add controls even through frequent software updates can potentially change the control structure substantially. Additionally, modified or added controls may interactively influence controlled processes. Unfortunately, testing for unexpected and emergent effects of added features, such as interactive effects on controlled processes, becomes more and more difficult as systems become more complex above and beyond the normal challenges of change management. In digital systems, it is relatively easy to add additional

controls and have them interact with other controls. For example, following an accident aboard the *USS McCain*, the U.S. Navy removed digital touchscreen throttle equipment and replaced them with more familiar analog equipment (Eckstein 2019). At the same time, testing for unexpected and emergent effects becomes more and more difficult as systems become more complex above and beyond the normal challenges of change management. Accidents tend to be more likely when there has been a major change in the control structure (Levenson 2019.)

The impact of production and cost pressures should also be considered. As discussed in Dainoff et al. (2020), the optimization of any work system requires a balance among effectiveness (achieving mission), efficiency (minimizing time and expense), and safety. In the present example, it appears that excessive effort on efficiency backfired, resulting in a decrease in both safety and effectiveness. That is, the safety control system did not support the safety constraints that were supposed to guard against Hazard #2: RPV levels.

2.9 Part 5. Create Improvement Program

It should be recognized that, to reap the expected benefits of digitalization, an enhanced approach to manage the digital implementation process needs to be considered. This will necessarily involve costs in addition to the traditional engineering modification process. This should be integrated into the change management process associated with plant modernization.

> *The modification process should not be a one-size-fits-all process. Complex technical digital modifications should be treated differently and more rigorously due to the fact that digital upgrades have unique attributes and risks that present different technical challenges than analog modifications.*

There are also important human operator performance differences that are relevant to the transition from analog and digital controls. After many hours of experience with analog controls, operators develop "muscle memories" and their control actions become automatic. Digital controls will have a different "feel". For example, digital controls lack tactile feedback that analog controls offer. In times of stress or high workload, operators may revert to previously highly overlearned habits and may rely more on easily accessible cues to support their performance. At the very least, extensive training on the new systems is required.

2.9.1 Focus on Individual Controllers

As in STPA, it is sometimes useful to take a more detailed examination (i.e., scenarios) of the potential mental model and process flaws contributing to an accident. In this case, we will expand upon the procedures laid out in the CAST Handbook (Leveson 2019); although, our analyses will remain within the overall STAMP framework (Leveson 2019).

There will be three components in this analysis. The first will expand the controller box of the SCS by depicting a more detailed view of the human controller's actions and model of their operational world (i.e., mental model). The second will utilize a portion of the means-end abstraction hierarchy (MEAH) to aid in visualizing the human controller's actions and beliefs. Finally, for a human controller, a key problem is how that person visualizes the information in their environment to make an informed decision. Ecological interface design provides an approach to examining the visualization problem.

2.9.1.1 Human Controller Model

Figure 9 redoes the SCS of the SCRAM incident seen in Figure 8, except that, for this analysis, an expanded view of the human controller is employed as described in France (2017).

In modelling SCSs, the fact that both human and machine controllers are modelled within the same framework is a positive benefit. However, for a more detailed examination, it can be useful to examine an operator's mental model using the logic depicted below. Here, mental model can be defined as a

conceptual representation of a system's operation (Craik 1943), which allows for describing, explaining, and predicting the function of the system (Rouse and Morris 1986).

As seen in Figure 9, the three components are:

- How did the operator choose which control action to perform?
- What does the operator know or believe about the system (i.e., what is their mental model)?
- How did the operator come to have their current knowledge or beliefs?

In Figure 9, the mental model corresponding to the evening shift operator has three subcomponents. The process state subcomponent refers to the operator's beliefs about the current state of the system. In this case, we infer that this belief refers to the operator's judgment that Method A is the appropriate procedure to increase pressurization. The process behavior subcomponent refers to the employee's belief about what the system can do. In this case, it is inferred that this belief refers to the operator's assumptions that Controls X, Y, and Z will work as they have in the past. Finally, for this example, the environment subcomponent might refer to the operator's general perception that the digital system will not be much different from the previous analog system.

The current contents of the operator's mental model will affect the decision as to which control action to perform. Likewise, the receipt of new information can result in the operator updating any or all three of the subcomponents of their mental model.

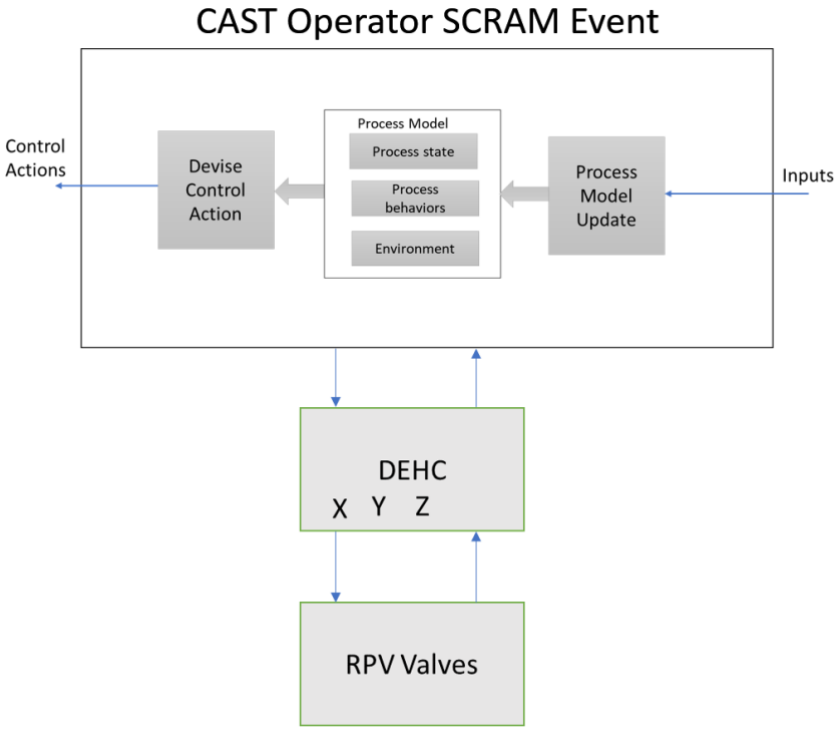

Figure 9. Human controller model in SCRAM SCS.

2.9.1.2 The Work Domain: Abbreviated Means-End Abstraction Hierarchy

The MEAH is a way of visualizing the set of action possibilities in the overall work domain. As an example, a road map is a method of visualizing action possibilities for getting from Point A to Point B. In this case, lower nodes are the means of achieving the ends at the next higher node. While the STPA and

CAST handbooks do not include a reference to the MEAH, Leveson (2020) discusses it. See Dainoff, Hettinger, and Joe's work (2022) for a more complete description.

Figure 10 contains a comparison of the MEAH structure of the DEHC, which was actually in place at Unit Bravo during the SCRAM compared with the unmodified procedure that the operators followed. As is appropriate for CAST, these depictions are limited to what is directly relevant to the incident.

At the left side of Figure 10 at the level of functional purpose, the DEHC in place during the incident had two relevant functions: a standard method for pressurization and an alternative method. However, the available incident report documentation gives no indication of the intended use of these controls. It should be noted that these controls acted to move bypass valves more rapidly than did the Unit Alpha controls with the same designation. Therefore, in Figure 10, the standard method is labelled N for "New", and the alternative method is labelled U for "Unknown".

At the level of object-related processes, the DEHC pressurization process required the activation of Control W followed by Control Y. This method is unique to Unit Bravo. For the alternate method, only the individual functions of the controls are listed.

Finally, at the level of physical objects, the DEHC contained the physical implementation of the pressurization logic W-Y for Method N. For Method U, the objects are listed as X' and Z' to emphasize that they operate differently than the controls with the same names at Unit Alpha.

The righthand side of Figure 10 depicts the existing procedure supplied to both units and used by the Unit 2 operators during the incident. Method A was the procedure employed, which specifies control sequence logic X-Y-Z-Y.

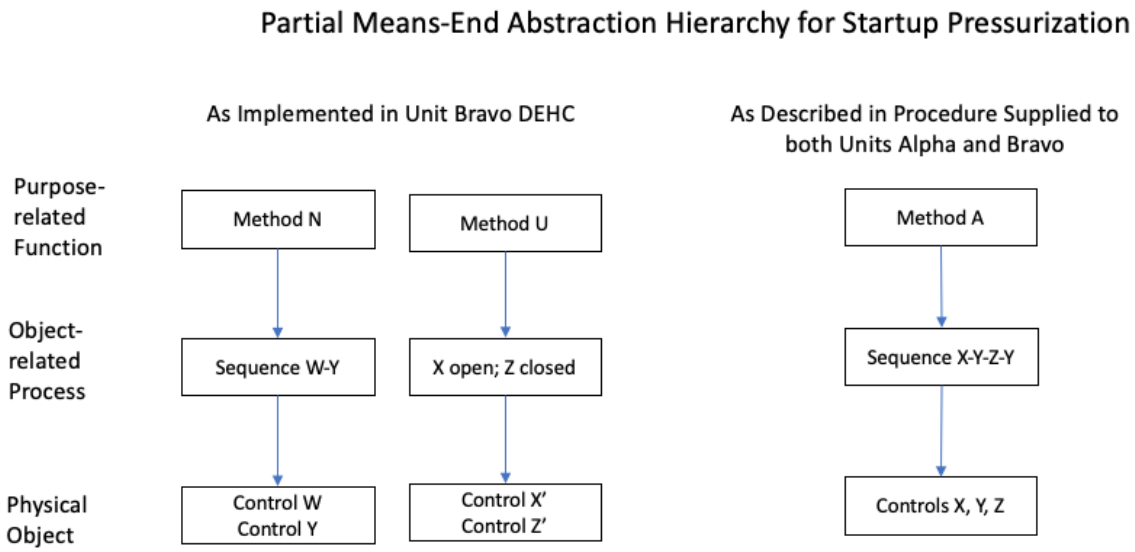

Figure 10. Comparing MEAH for delivered DEHC and available procedure documentation.

2.9.1.3 Visualization Problem: Ecological Interface Design Approach

In considering how the operator must move through the control sequence specified by Method A as described in Figure 9 and Figure 10, the visualization problem is central. The operator must integrate information from available interfaces—in this case the DEHC display and the printed procedure documents—and extract meaningful courses of action. The field of ecological interface design considers the visualization problem in depth; the dynamical control logic proposed by Bennett and Flach (2011) provides a useful approach. This approach provides an alternative way of looking at the information

contained in the work domain and control structure. See Dainoff, Hettinger, and Joe's work (2022) for a more complete description.

As seen in Figure 11, this logic embodies a three-part relationship between (1) the ecology or work domain; (2) the representation of that domain (i.e., the user interface), and (3) the underlying cognitive constructs (mental models) used to understand the domain.

The major components in this logic framework are, reading from left to right, work domain, user interface, and user mental model. These components are connected by two perception links and two action links. Together, these elements reflect the dynamic linkage that always exists between perception (e.g., what do I experience?) and action (e.g., what do I do?).

The relationship between the representation (interface) and the elements of the domain are considered the meaning of the domain, whereas the relationship between the representation and the concept (i.e., mental model) is considered the interpretation of the domain. In this case, the definition of "meaningful" is quite practical, referring to "revealing possibilities for action and associated consequences." These possibilities and consequences are objective properties of the work domain. On the other hand, "interpretation" refers to the individual's beliefs about the situation, as contained in their mental model. This logic is particularly relevant to safety-critical systems such as NPPs in the sense that the user's mental model must be aligned with the physical constraints of the domain.

This logic allows a somewhat different perspective on situation awareness as it is commonly understood (see, for example, Endsley 2011). Understanding the situation is reflected by WDA in which the elements in the domain of interest are organized in meaningful chunks, using the definition of meaningful just discussed. Awareness is understood through the SCS obtained through STPA or CAST, which uses the information structure of the work domain as a template or map upon which to superimpose potential control actions that can accomplish the desired goal. The resulting control structure diagram can be used to establish possible mental model structures. The integration of situation plus awareness can be achieved by considering the user interface. The meaningful chunks discovered in the WDA must be represented in the interface in such a way that the control actions can be effectively carried out with the known cognitive capabilities of the human user (See Bennett and Flach 2011, Ch. 5).

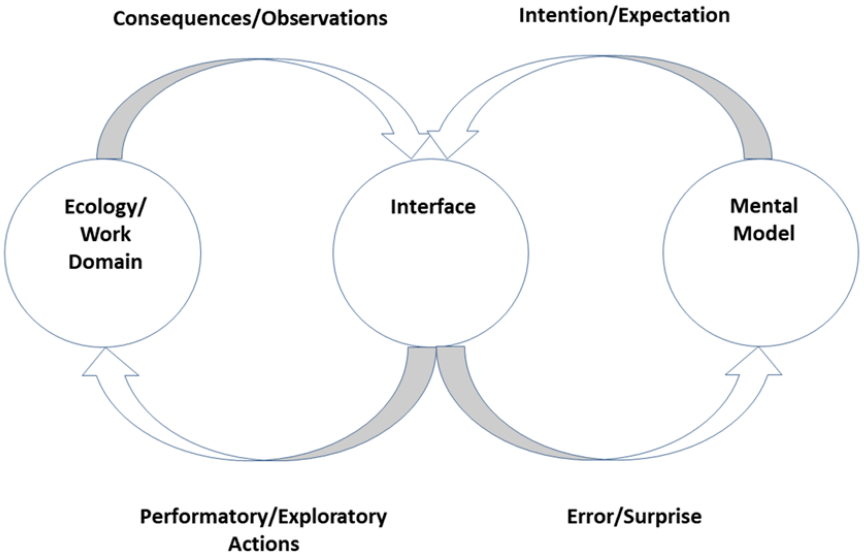

Figure 11. Three-part control logic for ecological interface design.[6]

[6] Modified from Bennett and Flach (2011, Figure 2.3).

2.9.1.4 Integration: How Might the SCRAM Have Happened?

The three-part logic of Figure 11 will now be used to integrate the expanded SCS of CAST using the human controller model (see Figure 9) together with the abbreviated view of the work domain using the MEAH.

The three components allow for the three-way interaction among the work domain, user interface, and the user's mental model. In describing this scenario, assume that the operator has received instructions to begin the pressurization process. For simplicity, only one operator will be considered in this example. On the right is the controller mental model, described in detail in Figure 9. A control action originated by the operator is labelled intention/expectation, and it is a query addressed at the interface. In the current case, the interface would include the written set of procedural documents. The operator is searching for a procedure to initiate pressurization. This logically requires a second performatory/exploratory link to the work domain and the corresponding appearance of an observation (i.e., the Method A procedure). The feedback signal (error/surprise) indicates that the operator has successfully found a procedure to execute. The mental model is updated, and an intention control action is sent to the user interface (in this case, the printed document) representing the operator's intention to review the document. As seen in Figure 11, the interface provides an incorrect mapping of the actual work domain for the DEHC for Unit Bravo since it refers to an older procedure employing a different set of controls. However, error/surprise feedback does not reflect this discontinuity since the information in the procedure agrees with the operator's beliefs about the X-Y-Z-Y sequence that is present in their mental model. In particular, the operator has successfully used this procedure previously while working in Unit Alpha.

Accordingly, an intention control action to examine the interface—in this case the DEHC control panel—and search for Control X to initiate the pressurization process. Control X is located, and the performatory control action to operate the control is carried out. The action occurs on the RPV values, which are physical objects in the work domain. The consequences/observations of the action appear on the DEHC display panel as a rapid opening of the RPV valves. This observation is processed as a surprise since the behavioral component of the operator's process model (middle portion of Figure 9 was for a lower rate of opening; this is judged to be too rapid to control. According to the operator's understanding of the process state for Method A, Control Y should halt the movement of the RPV valves. Accordingly, based on this aspect of the mental model, the operator generates an intention control action to execute Control Y. However, in executing the performatory action of operating Control Y, he observes that Control Y is inoperable (i.e., greyed out). This observation is again processed as a surprise. This surprise updates the operator's process model (right side of Figure 9, informing them that something is clearly wrong). In something of a panic, the process model tells the operator that Control Z is supposed to have the function to close the RPV valves, so he generates an intention to locate Control Z on the DEHC display. Since, Control Z is an emergency control, the performatory control action of activating it operates to rapidly shut down RPV valves. This causes a transient pressure wave that is detected by the automatic reactor safety system, and a SCRAM is initiated.

It should be noted that the preceding sequence of events requires making inferences about a hypothetical construct, the operator's mental model. These inferences are generated through observation of operator behaviors and interviews. In this case, these are reasonable given the actual observations and interviews. However, in other situations, it might be useful to be more speculative. This will be the case for the next example, which examines the night shift operator's lack of documentation of a similar experience with Method A. In this case, assumptions will be made that are not always justified by evidence. The rationale for this is to emphasize that the purpose of CAST is not to establish individual or legal responsibility for events, but rather to understand a wide range of possible causal factors with the goal of addressing such factors to avoid future accident.

2.9.1.5 Night Shift Operator Does Not Document Problems with Method A

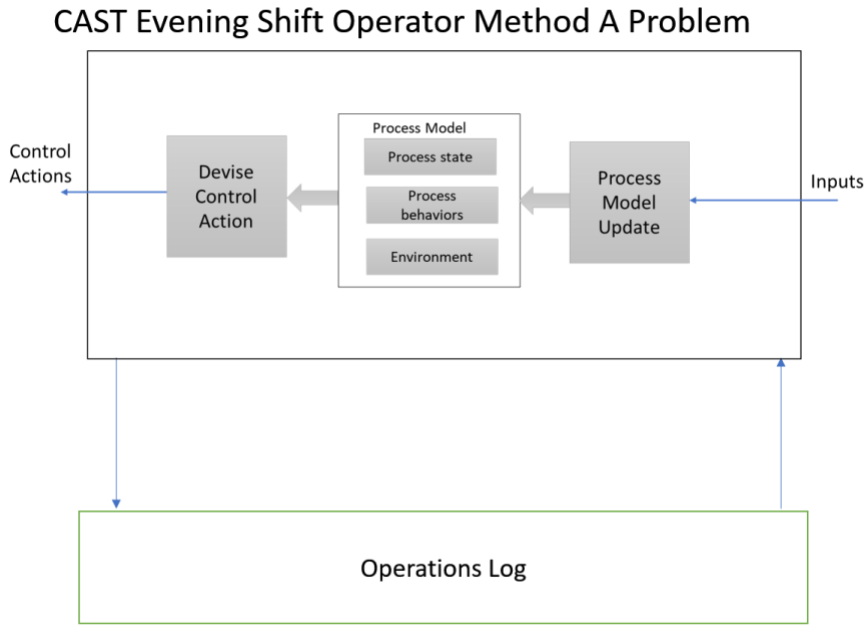

Figure 12. Component of SCRAM SCS related to previous shift.

Figure 12 depicts that portion of the SCS associated with the decision of the evening shift operator to report or not report difficulties with the Method A procedure.

In this case, the focus of analytic interest is not on the actual operational events. Recall that the situation was the same as for the day shift, but the operator was able to slow down the rate of pressure increase without causing a SCRAM. The team then stopped work and resumed pressurization using an alternative—Method B—which does not employ any of the controls used by Method A. This analysis will focus on the events after the resumption of work; namely the decision not to document the problem. In hindsight, had this been reported, it is likely that the SCRAM would not have occurred. However, in the spirit of CAST, the goal of the analysis is to examine why it might have made sense for the operator to make this decision. As in the previous case, for the purposes of this example, we focus on only one operator.

In Figure 12, the mental model corresponding to the evening shift operator has three subcomponents. The process state subcomponent refers to the operator's beliefs about the current state of the system. In this case, we infer that this belief refers to the operator's judgment about the seriousness of the event that just occurred. The process behavior subcomponent refers to the employee's belief about what the system can do. In this case, it is inferred that this belief refers to the operator's judgment of the consequences of entering or not entering the information about the event in the log. Finally, for this example, the environment subcomponent might refer to the operator's perception of management climate regarding documentation of what might be considered an operator error.

With this as background, two hypothetical scenarios of what might have caused the operator to not log the incident will be presented. These are strictly hypothetical for the purposes of this report. In an actual CAST investigation, interviews and other information would be used to ground the scenario development. Table 5 depicts two scenarios that might account for the event not being written up.

Table 5. Hypothetical scenarios accounting for absence of log entry.

Scenario	Mental Model		
	Process State	**Process Behavior**	**Environment**
1	This was an error on my part	It is not good for my record to be tagged with an error	The management climate tends toward blame for mistakes
2	This was a minor glitch from which we recovered with no problem	This event was no worse than a lot of things that happen around here	Too much work to do to take the time to write up a minor glitch

The three-part control logic (see Figure 11) can be used to look at each scenario in more detail. In these particular examples, a distinction must be made between the work domain and a WDA. There is always, in principle, a work domain. There may or may not be a formal WDA. In these cases, presenting formal analyses, which would be speculative and hypothetical, would seem to be less useful.

Scenario 1. Three-Part Analysis

Using Figure 11 combined with Figure 12, the analysis starts with the problems with Method A controls having been dealt with and Method B being used successfully. The perception of the discontinuity between previous experience with Method A and current experience generates an update (Figure 12, righthand side) with the operator's process model of Method A. At this point, a different process model—one reflecting the performance evaluation system in the plant—becomes active. In this case, the use of Figure 12 will have to be extended a bit to reflect purely cognitive activity in the form of problem-solving. The interface will represent the operator's active memory of previous interactions with supervisors as well as of published personnel documents. Thus, the operator generates a potential intention/expectation control action of entering the recent Method A in the operating log, and explores, in their memory, the relevant meaningful contents of the work domain. These observations, compared with the process model (i.e., state, behavior, and environment), indicate that this action might be considered an operator error, and that errors, in the past, have tended to affect an individual's performance ratings. This mental model does not include perceived support from management regarding reporting all problems in an attempt to learn from them and keep them from occurring in the future. Moreover, there did not seem to be any immediate negative consequences from the way in which the problem was handled; work went on as normal. Consequently, the operator generates an intention to not enter the event in the log nor to discuss it on shift turnover despite being aware that other components of the process model require these actions. This represents a conflict in the process models.

Scenario 2-Three-Part Analysis

This analysis starts from a similar situation as Scenario 1. The operator's mental model of Method A has been updated as being problematic and generated a potential intention to create an entry in the log. In this case, the interface reflects the perception of strong production pressure to get the startup completed quickly, and this includes an awareness of other required tasks. The operator explores other problems handled in the past without stopping to write them down in a log or report and observes that this one was probably no worse. The operator generates a second intention regarding how much time it would take to complete the log entry and how far behind other work tasks would be. The mental simulation of this exercise (exploration plus observation) reinforces the previous observation of the lack of seriousness of the event. Consequently, the operator updates his process model to reflect that the Method A problem was below the threshold of needing to be reported.

3. CONCLUSIONS AND RECOMMENDATIONS

LWRS Program researchers have been investigating how HTI principles, information automation, and digitalization enable data evolution, which is a prerequisite for ION. These researchers have been investigating how STPA and other sociotechnical systems theories can address human and organizational factors in NPP modernization activities in ways that previous human factors engineering guidance has not covered in detail but has stated needs to be addressed. The objective of this report was to map out data evolution in a use case to identify inefficiencies in plant compliance information gathering and communication activities. This analysis provides a preliminary technical basis for the merits of using STAMP (in this case, CAST) and other HTI methods, such as CWA and WDA, to help integrate the human factor engineering knowledge we have with respect to NPP control room design and then to expand that knowledge to improve other aspects of how NPPs outside of the control room are operated and maintained.

The strategy reflected in this more detailed examination of the DEHC event is that causality is almost always complex in real world events. However, we can also assume that this detailed examination has the potential for revealing underlying patterns that may be common to a wide variety of incidents. More detailed analysis requires selecting an appropriate sample of cases. One potential pattern, which seemed to be present in the analysis of the engineering change request, is that of conflicting mental models, leading to the omission of writing up the critical event in a log or report. These conflicts may occur within work groups or across work groups, and potentially broadly throughout the NPP organization. In fact, in an NPP, conflicting mental models about the status of behavioral safety constraints is particularly problematic because some of the constraints are grounded in laws of physics. Related patterns involve coordination issues and presence of silos. CAST allows analysts to identify these issues and then offers a framework to mitigate the issues by considering the SCS. CAST, and more broadly STAMP, offers a system-theoretic method that allows for the maintenance of the integrity of an SCS in an NPP.

3.1 Next Steps

LWRS Program researchers are continuing to investigate the merits of using STPA and other HTI methods and theories to enable the digital transformation of commercial NPPs. Some activities that we are currently performing include: 1) validating the use of STPA to define high-level safety constraints in the NRC's problem identification and resolution process (i.e., a plant compliance information gathering activity), and 2) exploring the similarities and differences between STPA and psychological theory. As discussed in Appendix A, both STPA and psychology are fundamentally interested in understanding the cause-and-effect relationship between a controller (e.g., a person) and a controlled process (e.g., the environment and people around them). As is often the case when two disparate areas of expertise begin to collaborate, which had historically not worked together because they were not thought to be sufficiently similar, the goal of this exploratory effort is to discover whether new insights and lessons can be garnered and shared from this cross-disciplinary investigation.

LWRS Program researchers are also actively working on more broadly disseminating this research. In addition to authoring four other LWRS Program technical reports (Dainoff et al. 2020, Hettinger et al. 2020, Kovesdi et al. 2021, Dainoff et al. 2022), we wrote a conference paper (Dainoff et al. 2021) which was subsequently invited to be published as a peer-reviewed journal article. As of the publishing of this report, the manuscript is still under review, and while we are optimistic that it will be accepted for publication (the editor invited us to revise and resubmit after the initial peer review), we include it in this report as Appendix B because it succinctly establishes the theoretical foundation for the work described in this report.

Moving forward, LWRS Program researchers supporting this project are planning to perform the following R&D activities.

1. *Develop, and then evaluate, a method to optimize information automation based on the STPA methodology.*
   As mentioned previously, Dainoff et al. (2022) developed an approach to the design and implementation of advanced, automated systems intended to increase operational efficiencies at NPPs. This research also proposed automating the mapping of data from plant systems and processes to application needs, thereby significantly reducing the human workload currently required to execute these tasks. The Dainoff et al. (2022) report and analysis of the DEHC event in this report lay the foundation for the use of STPA and other HTI methods to optimize information automation. We will continue to refine this research, and then we will evaluate its efficacy in additional use cases.
2. *Conduct a full-scale pilot to demonstrate the effectiveness of digitalization and information automation to enable data evolution.*
   As the technical bases and validity of using STPA and other sociotechnical systems theories to address human and organizational factors in NPP modernization activities is further established in use cases, LWRS Program researchers will also work perform a full-scale pilot of this sociotechnical approach to demonstrate its effectiveness in automating information processing to enable data evolution to support ION.
3. *Demonstrate operations and maintenance cost reductions via use of full nuclear plant modernization guidance at a nuclear utility.*
   As the proof-of-concept for using sociotechnical systems theories to address human and organizational factors in NPP modernization activities is established, the next important research question to answer is the extent to which improvements in how NPPs are modernized through information automation and digitalization lead to meaningful operations and maintenance cost reductions. When this question is answered affirmatively, LWRS Program researchers will then develop additional guidance on full nuclear plant modernization and will share that with the commercial nuclear industry.

The overarching goal of this LWRS Program–supported research and development project is to provide planning tools and comprehensive guidance to utilities considering or undertaking full nuclear plant modernization. The results of this research will provide the nuclear industry with a comprehensive and usable solution, including guidance, lessons learned, methods, and planning tools. LWRS Program researchers have been investigating how human and technology integration principles, information automation, and digitalization enable data evolution. This research is currently working to provide guidance on digitalization and information automation to enable the evolution of data to information, insight, and action—thereby allowing utilities to operate safely and cost-competitively with all other electrical generation sources.

4. REFERENCES

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

Booher, H. 2003. *Handbook of human systems integration*. New York City, NY: Wiley.

Craik, K. 1943. *The Nature of Exploration*. Cambridge, UK: Cambridge University Press.

Crandall, B., Klein, G., and Hoffman, R. 2006. *Working minds: A practitioner's guide to cognitive task analysis*. Cambridge, MA: MIT Press.

Dainoff, M. 2009. Can't we all just get along? Some alternative views of the knowledge worker in complex HCI systems. *International Journal of Human-Computer Interaction*, 25(5). 328-347. https://doi.org/10.1080/10447310902864944

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

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

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

Eckstein, M. 2019. "Navy Reverting DDGs Back to Physical Throttles, After Fleet Rejects Touchscreen Controls." U.S. Naval Institute News. https://news.usni.org/2019/08/09/navy-reverting-ddgs-back-to-physical-throttles-after-fleet-rejects-touchscreen-controls

Endsley, M. 2011. *Designing for Situation Awareness: An Approach to User-Centered Design*. Boca Raton, FL: CRC Press.

France, M. 2017. *Engineering for Humans: A New Extension to STPA*. Cambridge, MA: Massachusetts Institute of Technology.

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

Hollnagel, E. 2006. Resilience – the challenge of the unstable. In *Resilience Engineering: Concepts and Precepts*.

Hollnagel, E., and Woods, D. 2005. Joint cognitive systems: Foundations of cognitive systems engineering. In *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*.

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

Klein, G., Orasanu, J., Calderwood, R., and Zsambok, C. 1993. *Decision making in action: Models and methods*. Norwood, NJ: Ablex.

Kleiner, B., Hettinger, L., DeJoy, D., Huang, Y., and Love, P. 2015. Sociotechnical attributes of safe and unsafe work systems. *Ergonomics*, 58(4), 635-649. https://doi.org/10.1080/00140139.2015.1009175

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

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

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

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

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

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

Rouse, W., and Morris, N. 1986. On looking into the black box: Prospects and limits in the search for mental models. *Psychological Bulletin*, 100(3), 349–363. https://doi.org/10.1037/0033-2909.100.3.349

Schraagen, J., Militello, L., Ormerod, T. and Lipshitz, R. 2008. *Naturalistic Decision Making and Macrocognition*. Burlington, VT: Ashgate.

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

Thomas, K., Remer, S., Primer, C., Bosnic D., Butterworth, H., Edwards, C., Foote, G., Drøivoldsmo, A., Rindahl, G., McDonald, R., and Lawrie, S. 2020. "Analysis and Planning Framework for Nuclear Plant Transformation," INL/EXT-20-59537, Idaho National Laboratory.

Woods, D., and Hollnagel, E. 2006. *Resilience Engineering: Concepts and Precepts*, Boca Raton, FL: CRC Press.

APPENDIX A
CROSSWALK BETWEEN STPA AND PSYCHOLOGY

The purpose of this appendix is to propose that similarities exist between engineering's STPA and psychological theory. In attempting to understand how a system operates and by extension fails, be it technological systems or mental processes, the two share similar historical underpinnings that led away from one school of thought and towards another. The ways in which STPA shares attributes with several branches of psychology are discussed, including developmental psychology, Gestalt psychology, social psychology, and cognitive science. The concluding comments point to meaningful ways that psychological theory has contributed to our understanding of complex systems.

STPA Defined

STPA, as outlined by Leveson and Thomas (2018), is a hazard analysis technique that uses a systems-level approach to improve safety within complex systems. Technological advances in recent decades have increased exponentially, with complex software and greater digital connectedness bringing about increased vulnerability for failure. Historically, within technical systems such as process control, analog technology provided hard-wired and isolatable control of operations. The introduction of digital I&C to produce greater efficiencies and better safety outcomes has increased the complexity of functions, such that systems are no longer deterministic in the way that the older legacy systems were. STPA is a systems engineering tool that improves upon earlier chain-of-events causality models and helps identify failures beyond isolated component failures (France 2015). In addition, STPA serves to find the causes of accidents before product deployment, by considering not only component failures (that include technical, managerial, and social factors), but also system failures stemming from interactions between components. Importantly, STPA highlights the fact that the advanced technological systems brought about by the introduction of software produce functional complexities and failures beyond the sum of their constituent parts. STPA is an applied tool borne from STAMP, a model of accident causation (Leveson 2011).

STPA as Nature Versus Nurture

STPA is an evolution from older, traditional models of safety (e.g., in electromechanical systems) that took a decompositional or reductionist approach in which the independent components of the system were analyzed separately. Using these methods, any interactions between components, including with the environment, were assumed to be direct and occur in known ways. That STPA considers both component parts and the interactions within the system as a whole (i.e., unknown interactions between the components), can reasonably be likened to the evolution of the nature vs nurture debate within developmental psychology theory. This describes the degree to which psychological traits or behaviors are a product of either known inherent properties of an individual (nature), or environmental interactions (nurture).

Broadly speaking, the building blocks or component parts of a technological system would be analogous to the "nature" of the system, while the interactions between them and in different contexts would be analogous to "nurture". In developmental psychology, while biological and genetic predispositions were at one time favored when explaining behavior, including psychological dysfunction, most contemporary psychologists now consider the impact of both and the ways in which context-dependent interactions influence the individual (system) in qualitatively different ways. For example, epigenetics considers how interactions with the environment impact the expression of genes to produce behaviors (Holliday 2006). The evolution of hazard analysis within technological systems has followed a similar trajectory to developmental psychology in that STPA represents the acceptance that engineering models should examine not only the physical or functional individual aspects that constitute the system

(nature) but also the interactions that arise from all these aspects working together in a context-dependent manner (nurture).

STPA As Gestalt Psychology

One of STPA's guiding principles is that the system be treated as a whole because "emergent properties" will manifest, which are more than simply the sum of its parts. To this end, the STPA handbook (Leveson and Thomas 2018) quotes the popular adage "the whole is more than the sum of its parts." This saying has deep roots within psychological Gestalt theory, which champions that human psychology cannot be understood merely by studying parts of the whole but rather by the whole itself. The German term gestalt is typically credited to the works of Wertheimer, who in 1912 reported that optical illusions within the study of visual perception could not be explained by looking at the component parts of the image but only by considering the image as a gestalt (translation: pattern or whole; Newby 2021).

This breakthrough in understanding the nature of perception within the human mind stood against traditional schools of psychological thought at the time, such as psychological structuralism, which focused on analyzing the structure of the mind by breaking down mental processes into their basic component parts (Schultz and Schultz 2004). This is similar to the creation of STPA in response to the reductionist models within systems engineering that assumes the examination of individual components will not distort an understanding of the system overall. Gestalt theory has since been applied to almost every major branch of psychology, including learning, motivation, and social psychology with great success, providing unique insights to mental processes and "emergent properties" that would not otherwise have been uncovered were individual elements examined alone.

STPA As Social Psychology

Further, the emphasis STPA places on understanding relationships within a system resembles that of social psychology, which uses relational methodologies to understand how minds are influenced by the presence of other minds (Gergen 1973). STPA was brought about to address the shortcomings within traditional systems engineering models that relied on the assumption that each individual component is independent and uninfluenced by the other components. Core assumptions of social psychology, stemming from the turn of the 20th century, include that behavior is a product of the individual plus the influence of other people within the social environment. Moreover, the individual's mental processes are shaped by a socially conditioned perspective of the world. Taken together, the interrelatedness emphasized within STPA is expressed within the study of social psychology.

STPA as Cognitive Science

Perhaps the most striking aspect of STPA in the ways it reflects psychological theory is in its likeness to cognitive science, specifically models of working memory. As mentioned, STPA was brought about to address problems that began to occur in systems engineering and with flawed systems design, due to the "emergent properties" that arose from complex systems. The solution presented by STPA is to introduce a control structure, separate from the components, that acts to control system and resulting emergent properties (Figure 13a). Importantly, the controller does this via a feedback loop to gather information about its control actions.

Consider now Baddeley and Hitch's 1974 model of working memory (Figure 13b), which was brought about to address the shortcomings in prior information-processing multistore models of short-term memory, which were deemed too simplistic. Working memory is a vital cognitive function that allows persons to store and manipulate information in the mind for small durations, which makes goal-directed behaviors possible (Chai et al. 2018). Indeed, working memory is a paragon of a highly complex system in which vast amounts of sensory data are received (via multiple modalities), processed, stored, manipulated, and then further processed in support of most all cognitive tasks, including holding a

conversation, writing a shopping list, and following a set of instructions. One of the key updates that Baddeley and Hitch made to short-term memory theory in the 1970s was to introduce the "central executive", a central control center to supervise and govern the sensory-based components of the system, i.e., the phonological loop for speech information, the visuospatial sketchpad for visual information and the episodic buffer as a multisensory storage system (Baddeley and Hitch 2001). The central executive is considered the most important aspect to the function of the system because it controls the actions of its ancillary systems. Note the active feedback loops from each component to the central executive, as well as the interactions between components. This re-insertion of information about the system's function from component structures into the control structure (feedback loop) is common to both STPA and Baddeley and Hitch's model of working memory. Placing the two side by side demonstrates the similarities in structure and function (Figure 13).

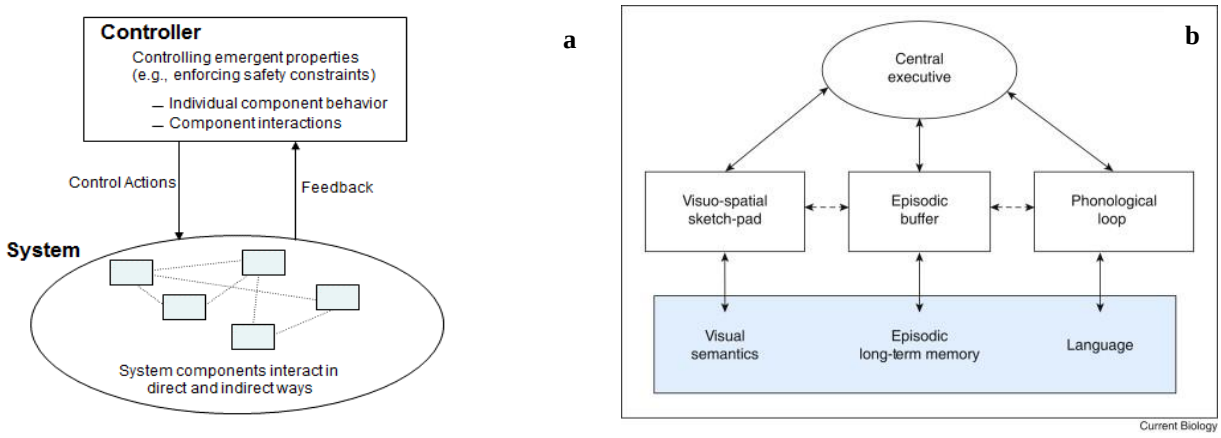

Figure 13. STPA model (a) from The STPA handbook (Levenson and Thomas 2018) and (b) the model of working memory from Baddeley (2010).

Within engineering systems, the controller enforces constraints that prioritize safety. Within Baddeley and Hitch's working memory model, the executive function has a limited capacity, which acts as a constraint on the system. In considering other disciplines that use systems theory methods, the STPA authors cite cybernetics, which, among other definitions, is the study of processes of communication and control (self-regulation) found within biological and artificial systems (Wiener 1948). Cognitive science is a comprehensive authority on processes of communication and control found within mental functions, many of which represent complex systems.

Concluding Comments

That systems engineering and phenomena of the human mind are alike in important ways is not new. Indeed, engineers as far back as the late 1940s understood the shared properties of biological and non-biological systems (Guttman 1991). Of course, STPA is useful for systems engineering that involves the design and creation of systems from scratch in the way that psychological science does not. Further, it should be recognized that the technologically sophisticated components contained within artificially built systems that STPA is used upon often have been developed to work optimally as an individual unit, perhaps by different companies and vendors, at times blind to how it will be used or how it will perform within a larger system, whereas the composition of the systems of the mind have developed in unison. Certainly, this is one of the greatest challenges of modern complex systems that contain multiple agents, especially intelligent systems. Here a specific comparison of STPA to several psychological schools of thought has been presented, in a bid to highlight psychology's rich history and valuable contributions to understanding the structure and design of systems of the human mind.

References for Appendix A

Baddeley, A. 2010. Working memory. Current Biology, 20 (4), R136-R140.

Baddeley, A., and Hitch, G. 2001. Working memory in perspective. Psychology Press.

Chai, W., Abd Hamid, A., and Abdullah, J. 2018. Working memory from the psychological and neurosciences perspectives: A review. *Frontiers in psychology*, 9, 401. https://doi.org/10.3389/fpsyg.2018.00401

France, M. 2017. *Engineering for Humans: A New Extension to STPA*. Cambridge, MA: Massachusetts Institute of Technology.

Gergen, K. 1973. Social psychology as history. *Journal of Personality and Social Psychology*, 26(2), 309-320.

Guttman, H. 1991. Systems theory, cybernetics, and epistemology. *Handbook of Family Therapy*, 2, 41-62.

Holliday, R. 2006. Epigenetics: A historical overview. *Epigenetics*, 1(2), 76-80.

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

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

Newby, S. 2021. Is the 'whole' different from the sum of its parts? Gestalt Psychology and the Theory of Perception. NewbyCore. https://www.newbycore.co.uk/post/is-the-whole-different-from-the-sum-of-its-parts

Schultz, D., and Schultz, S. 2004. A history of modern psychology (8th edition). Ft. Worth, TX: Harcourt Brace Publishers.

Wiener, N. 1948. Cybernetics. *Scientific American, 179(5)*, 14–19. http://www.jstor.org/stable/24945913

APPENDIX B
JOURNAL MANUSCRIPT

This appendix is a copy of a manuscript that LWRS Program researchers wrote to disseminate more broadly the R&D we have been performing. As of the publishing of this report, the manuscript is still under review, and while we are optimistic that it will be accepted for publication (the editor invited us to revise and resubmit after the initial peer review), we include it here because it succinctly establishes the theoretical foundation for the work described in this report.

Addressing Human and Organizational Factors in Nuclear Industry Modernization: A Sociotechnically-Based Strategic Framework

Marvin Dainoff,[a]* Lawrence Hettinger,[b] Lewis Hanes,[c] and Jeffrey Joe[d]

[a]*Marvin J. Dainoff, LLC, Medway, MA.*

[b]*LLC Engineering, Harvard, MA.*

[c]*Consultant, Columbus, OH.*

[d]*Idaho National Laboratory, Idaho Falls, ID.*

*dainofmj@miamioh.edu

Addressing Human and Organizational Factors in Nuclear Industry Modernization: A Sociotechnically-Based Strategic Framework

The modernization of nuclear power plants will require an advanced concept of operations, involving an integrated set of tightly coupled systems in which all stakeholders act in a coordinated manner. For this modernization effort to be enabled, we developed a human and organizational factors approach, based on a broad sociotechnical framework. Starting from core human factors principles, we conducted a literature review of the methods and approaches relevant to the modernization problem. These included core disciplines such as cognitive systems engineering, systems theoretic accident modeling and processes (STAMP), human systems integration, resilience engineering, and macroergonomics but also related topics of safety culture and organizational change. From this literature, we developed a conceptual framework centered around the work system with its four interacting components: people, technology, process, and governance. In an effective work system, these four components are jointly optimized according to three systems criteria: efficiency, effectiveness, and safety. System failure may result from excessive emphasis on any one criterion. The actual work of attaining joint optimization in a given work system can be accomplished by utilizing three high level functions: knowledge elicitation, knowledge representation, and cross-functional integration. We illustrated the utility of this approach by applying it to practical problems and case studies.

Keywords: Modernization, human factors, sociotechnical, organizational

I. PATHWAY FOR DIGITAL TRANSFORMATION

The Plant Modernization Pathway of the U.S. Department of Energy Light Water Reactor Sustainability Program contains a strategic action plan [2] that lays the groundwork for a digital transformation of the nuclear industry, embodying an advanced concept of operations with an end point vision as follows: "…the digital infrastructure for a nuclear plant must be designed as an integrated set of systems that together enable a technology centric operating model" (see Figure 1). Designing and operating such integrated systems will, of course, require new, automated, technologies. In addition, a new way of working, both in the design and operational phases, will be required. A sustained commitment from top management in terms of visible priorities and goals must percolate downward to the level of systems engineering in design and operations. For this effort to succeed, a strict discipline is required for the integration of multiple tightly coupled functions to ensure that all stakeholders in the systems engineering process are participating in a coordinated manner.

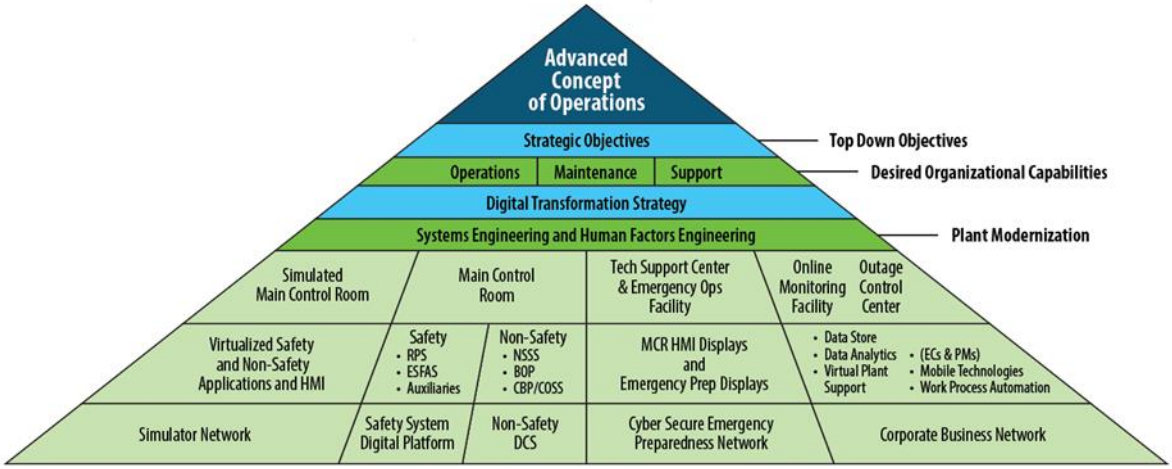

Figure 1. Technology Centric Plant Operations Model [2].

More recent work by Hunton and his colleagues [3] has provided a compelling business case against the like-for-like replacement strategy of individual I & C systems. They found that the cost to maintain systems in their current form is economically unsustainable. This seems to be primarily due to the cost of maintaining obsolescent components which continues to increase over time at an exponential rate.

Joe and colleagues [4] have extended the model in Figure 1 by providing a framework for a synthesized approach to R&D supporting the Plant Modernization Pathway.

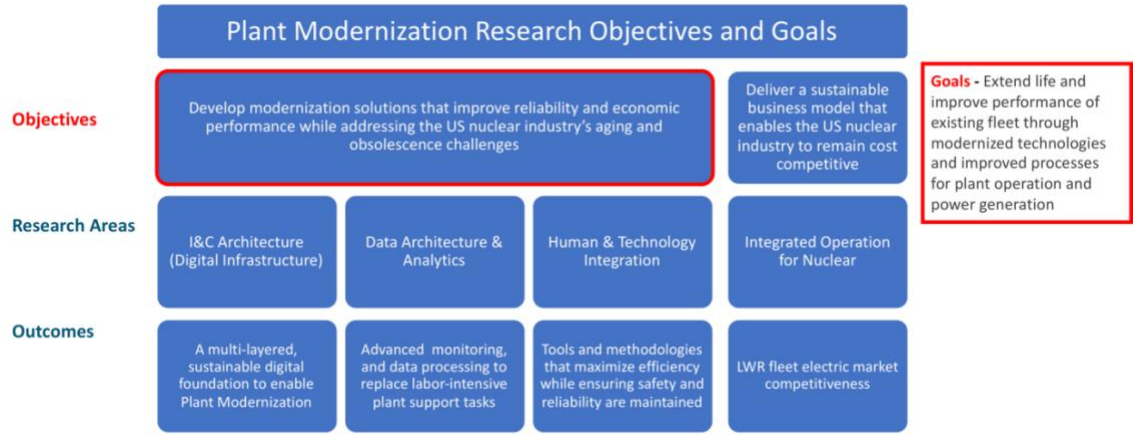

Figure 2. Conceptual Overview of the LWRS Plant Modernization Pathway, with its Objectives and Goals Highlighted [4].

As indicated in Figure 2, the high-level objectives focus on modernization solutions within a sustainable business model which will achieve the high-level goals of extending life and improving performance of the existing fleet through modernization techniques and improved processes. Within the Pathway, four distinct research areas are identified: I&C (Digital) Architecture, Data Architecture and Analysis, Human and Technology Integration, Integrated Operation for Nuclear (ION). The third of these areas –Human and Technology Integration – has the responsibility integral to a systems engineering approach, for the synthesis of all of these areas into a more integrated and organized set of solutions. This is the primary focus of the current paper.

Figure 3 [5] depicts a more detailed and refined set of potential strategies for plant modernization. Two separate but related aspects of the strategy are indicated. Capability development (top half of Figure 3) consists of a planning process that focuses the transformation on those core capabilities that truly define value in the eyes of the ultimate customer. Capability involves the synthesis of four PTPG dimensions (people, technology, process, governance) with respect to resources needed, resources on hand, and resources that need to be developed. From an analytic perspective, capability starts at the individual function level, with functions becoming successively more integrated at higher levels. From a concept of operations perspective, however, the starting point is the highest level (stack model) one can achieve, applying a set of basic principles that reflect the end-state vision and effectively propagate downward. The bottom of Figure 3 reflects components of the work reduction focus, which will be systematically applied.

To enable the coordination required by the models depicted in Figures 1, 2 and 3, we developed the human and organizational factors approach to nuclear modernization described in detail in [1]. The remainder of this paper discusses findings from that report. We must emphasize that there are many excellent sources of human factors engineering guidance in the nuclear energy domain. These include [6], [7], [8], and [9]. We do not attempt to replace or modify these sources. Rather, the goal is to supplement this guidance by identifying methods to achieve the integration, consensus, and coordination called for in these publications.

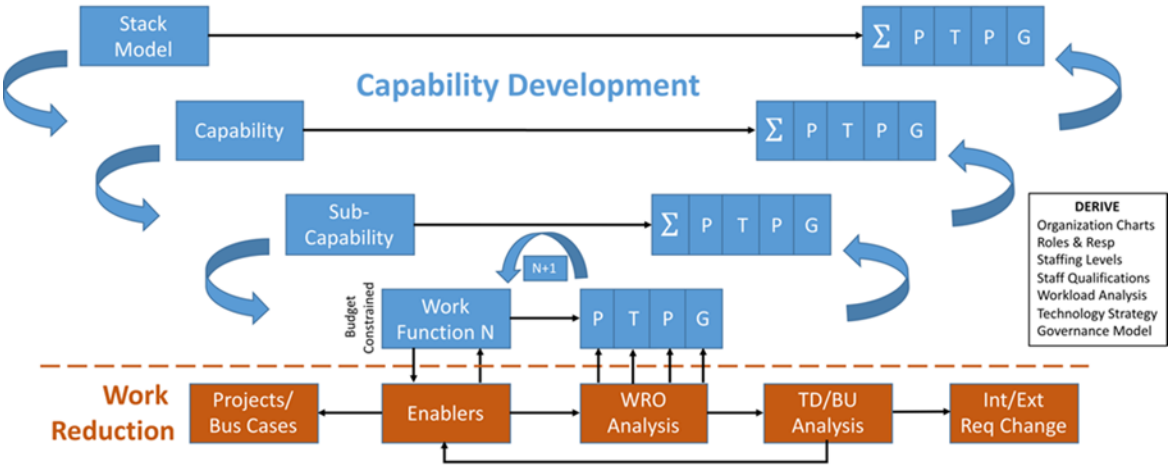

Figure 3. A Model of Integrated Operations Merging Capability Development and Work Reduction Strategies [3].

II LITERATURE REVIEW

Building on a traditional human factors engineering foundation, we employed a human and organizational factors approach to the broad area of sociotechnical systems relevant to nuclear modernization. This approach is based on a literature review focused on the tools and methods that might be applicable. This review was constrained by limiting consideration to those methods for which there was evidence of active communities of practice in active engagement solving real world problems.

Historically, the concept of the sociotechnical system was established to stress the reciprocal interrelationship between humans and machines and to foster the program of shaping

both the technical and social conditions of work in such a way that efficiency and humanity would not contradict each other any longer [10].

The goal of the sociotechnical systems theory, as applied to systems design, is the joint optimization of social-organizational and technical subsystems. Additionally, an argument from the domain of resilience engineering describes the interdependence of three system performance criteria: effectiveness (accomplishment of mission), efficiency (optimization of resources), and safety (avoidance of injury or damage). Excessive emphasis on any one criterion at the expense of the others is likely, in the long run, to result in overall system failure [11], [12].

Sociotechnical systems theory provides a pathway to these goals and is foundational for several core disciplines within the human factors engineering community, including macroergonomics, cognitive systems engineering, macrocognition/cognitive task analysis, and human systems integration [13]. Out of these core disciplines has emerged the "toolkit" of methods and techniques described in the next section of this paper. [Methods and techniques associated with these disciplines that will be referred to later are included in brackets.]

II.A. The Core Sociotechnical Disciplines

Macroergonomics, as its name suggests, was an expansion of traditional human factors and ergonomics to include social and organizational issues. The macroergonomic concept of a work system [14] including the interaction of the social, technical, and organizational components has, as modified by the PTPG framework above, become our basic unit of analysis.

Cognitive systems engineering is a form of systems engineering and, as such, requires understanding and description at multiple levels of analysis. Several subdisciplines of cognitive systems engineering are considered. They include: cognitive work analysis, [Work Domain Analysis] which had its origins in nuclear engineering [15], resilience engineering, which emerged from the post-accident analysis of the Columbia shuttle disaster [9], and STAMP-

system theoretical accident model and process [16], which has its origins in each of the previous developments [STPA-System Theoretic Process and Analysis].

Macrocognition/Cognitive Task Analysis is described as the collection of cognitive processes and functions that characterize how people think in natural settings [17], [18]. It is derived from the seminal work of Gary Klein on naturalistic decision-making [19]. A particular focus of this approach is the deep respect for the expertise of the subjects of their analysis as well as the recognition that this expertise is often distributed across multiple actors [Concept Maps, Structured Interviews, Consensus].

Human systems integration emerged within the context of the acquisition of large military and transportation systems and is simultaneously a high-level conceptual model for systems design and a formal U.S. Department of Defense requirement [20]. Although systems engineering and management theory have usually considered the interaction among people, technology, and organization to describe the top level of any complex system, it is through human systems integration that the most dramatic organizational benefits (in terms of increased performance and reduced costs and risk) can be achieved. These insights are reflected in the USS Zumwalt case study presented in [1].

II.B. Safety Culture and Organizational Change

The separate topics of safety culture and organizational change are not specifically included in the sociotechnical systems disciplines but provide important context. They were, therefore, included in [1].

Safety culture is specifically identified as a focal point for attention by the NRC [21] as well as IEEE 1023-2004 [7], NUREG 0711 [6], and IAEA [22]. However, the scientific validity of safety culture as a concept has recently been called into question [23]. At issue is the extent to which the factors included by the above references can be included within the integrated systems

engineering framework specified in, for example, the Electric Power Research Institute Digital Engineering Guide [4]. Specifically, the challenge is to develop a set of top management core values upon which the modernization program is based, and which can integrate safety culture concepts into the systems engineering framework.

It is a truism that the modernization of the nuclear industry will require major changes. Therefore, it would be prudent to pay some attention to the literature on organizational readiness for change [24]. A practical benefit is the identification of a method [25] for accomplishing a change that combines user participation with an organizational goal alignment [IDEAS-Intervention Design and Analysis Scorecard].

III. CONCEPTUAL FRAMEWORK

Based on the sociotechnical systems literature, we developed a strategic framework for the effective integration of human and organizational expertise within nuclear industry modernization efforts (See Figure 4).

The basic unit of sociotechnical systems analysis is a work system. According to macroergonomic theory, a work system contains three components, personnel, technical, and organization and management. However, the four PTPG dimensions (people, technology, process, governance) identified in the capability building framework of the Plant Modernization Pathway [2] can be mapped into the three components of the work system. An effective work system will jointly optimize these components. Joint optimization can be operationally defined, in the language of resilience engineering [9], in terms of the interdependence among the three major systems performance criteria: effectiveness (accomplishment of mission), efficiency (optimization of resources), and safety (avoidance of injury, damage). As previously stated, excessive emphasis on any one criterion to the exclusion of others will, in the long run, likely lead to system failure. Case studies presented in [1] relating to the Boeing 737 MAX, Deepwater

Horizon, and USS McCain provide evidence of examples where an excessive emphasis on efficiency (particularly time pressures) over safety had catastrophic effects.

The practical work of actually bringing about joint optimization in the daily interactions within the work system can be described in terms of three problems: knowledge representation (how information about the work system is presented to those who need to operate on it), knowledge elicitation (how represented information is obtained from those who have the required expertise), and cross-functional integration (how information can flow freely between groups and help support collaboration and prevent silos).

Knowledge representation, knowledge elicitation, and cross-functional integration can be considered high-level human and organizational factors functions. These functions were applied to a set of practical problems described below. *The intention was to elucidate how these functions could be used to enhance the practical work of stakeholders in the modernization design and operation in the same way that traditional human factors engineering enhances the practical work of control room operators.*

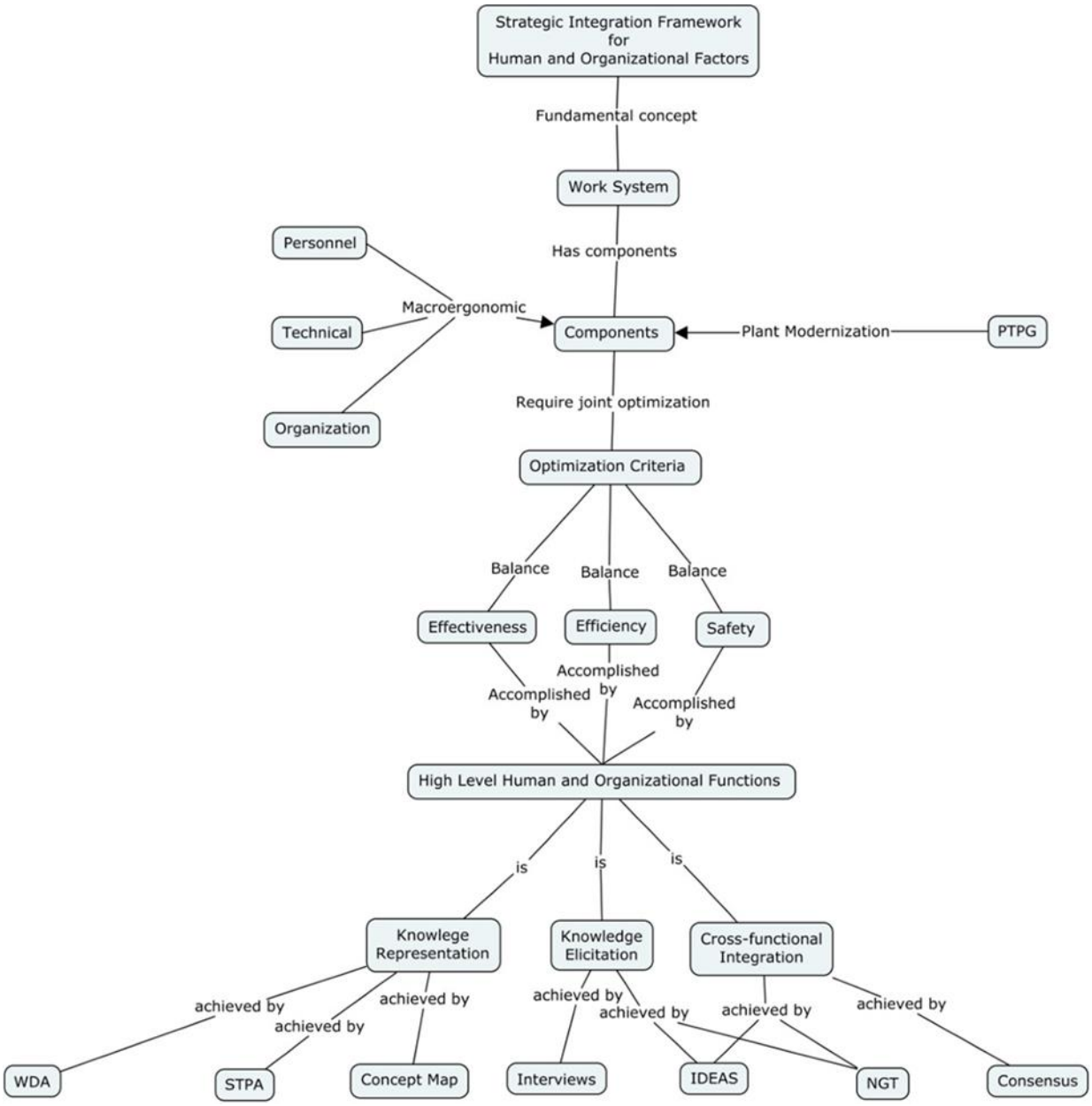

Figure 4. Strategic integration framework presented as a concept map. This figure was created using Cmap tools (cmap.ihmc.us).

As shown in Figure 4, the specific methodologies-supporting the basic three functions above include: Work Domain Analysis, STPA-Systems Theoretic Process Analysis, Concept Mapping, Interviews, Nominal Group Technique, IDEAS-Intervention Design and Analysis Scorecard, Consensus. Note that Figure 4 itself is an example of a Concept Map application.

IV. EXAMPLES OF APPLICATIONS

The practical problems identified in [1] included: top management consensus and the need for core values; human factors engineering program management; obtaining tacit (undocumented) knowledge. new skills and capabilities of current employee; PTPG (people, technology, process, governance) integration; the silo problem. For each of these problems, proposed solutions involved a combination of at least two and usually three of the high-level human and organizational functions.

In the following sections, we will briefly describe two of these problems and associated solutions.

IV.A. Problem 1: Human Factors Engineering Program Management

The centrality of the cross-functional integration issue for HFE within the systems engineering process has been clearly stated. Section 4 of the EPRI Digital Engineering Guide [4] emphasizes that systems engineering is a collaborative enterprise in which no single perspective or discipline may be allowed to dominate. Accordingly, it is essential that HFE is a part of the system engineering process, and, as such, should be well-integrated into the modification process from the beginning and not treated as a stand-alone process. In addition, HFE should be involved in gathering user input to design, for performing required design verification, and providing a structured process for accomplishing these functions. The solutions discussed below are intended to enable that structured process.

IV.A.1. Solution 1 to Problem 1. Systematic Approach to Identification of Stakeholders Needs—the IDEAS Tool (Knowledge Elicitation, Cross Functional Integration)

EPRI Digital Engineering Guide [4] requires that, as a starting point it is necessary to identify potential HFE impacts, and stakeholder needs. If there are any HFE impacts, identify the

stakeholders that may be affected by the change, and solicit participation from affected stakeholders.

The IDEAS (Intervention Design and Analysis Scorecard) tool, originally created for the development of health and safety interventions, represents a methodology for accomplishing these requirements [25]. As slightly modified for use in NPP, the tool represents a framework for developing an overall end point vision, concept of operations, and migration plan while considering HFE impacts and stakeholder needs.

The methodological framework assumes two levels of participation:

1. A design team, which identifies a focus area, evaluates needs and impacts, and, based on needs assessment, develops a set of alternative solutions.
2. A steering committee, to which the alternatives are submitted and who provides guidance and support throughout the process.

To summarize the process, the steering committee develops the overall general problem statement. The design team, through iterative and participative steps involving multiple stakeholders, defines the problem and conducts a systems analysis identifying needs, impacts, and contributing factors. From this input, a set of functional objectives are developed which address the needs and impacts developed in the previous step. Next, a set of selection criteria are developed to assess potential alternative solutions. Once the selection criteria are defined, the design team develops sets of proposed alternatives. The design team then assesses and/or combines proposed alternative with respect to selection criteria. The outcome is a rating of each of the three alternatives on each of the selection criteria. This becomes the set of prioritized business cases for each of the alternatives. These are, in turn, submitted to the steering committee.

The steering committee reviews the alternatives, provides feedback to the design team, and makes a decision. This step includes the possibility of continued dialogue with the design team, resulting in possible modifications. The steering committee then implements the decision. Having done so, it then monitors and evaluates the impact of the decision. Modifications are made if necessary; typically with further involvement of design team.

The IDEAS tool provides a structured process by which the individual stakeholders can communicate their impacts and needs to the HFE team, and other stakeholders. When appropriate, Nominal Group Technique [26], a structured method allowing each member of a group to have an equal opportunity to contribute, could be used at specific steps in the process. In addition, the tool can be easily adapted to the increased complexity of the NPP modification process. For example, identification of possible alternative solutions would likely need to be expanded to include input from vendors or other outside experts. Nevertheless, this tool provides a framework by which knowledge elicitation from stakeholders can be accomplished in a collaborative coordinated manner. At the same time, this information must be mapped into a form which affords efficient problem solving.

IV.A.2. Solution 2 to Problem 1. Representing the HFE Program Management Problem Space (Knowledge Representation)

This solution can be considered an extension of the previous solution in which the knowledge representation of the HFE program management problem space is characterized. Assume that the IDEAS tool discussed in Solution 1 has been utilized in this situation. The raw materials comprising the discussions and documentation utilized in would be represented in the upper left box of Figure 5—Actual Goals and Task Content of Domain. The initial process of summarizing and integrating this material, typically by different stakeholders, would be represented by the lower left box of Figure 5 – CES Approximation of Domain. As alternative

automation possibilities become conceptualized, more formal representations, equivalent to the Display in Figure 5 are created. Effectively, the aim of these representations is to enable formation of mental models of proposed alternatives by participants. This would be the expectation initially for members of Design Group, and ultimately for the members of Steering Committee.

In the original report [1], Work Domain Analysis [27], was used as an example of an effective formal knowledge representation for this problem. However, Work Domain Analysis, as a component of Cognitive Work Analysis, has been widely used in the nuclear industry and elsewhere, and it is, therefore, not necessary to describe it further in this paper.

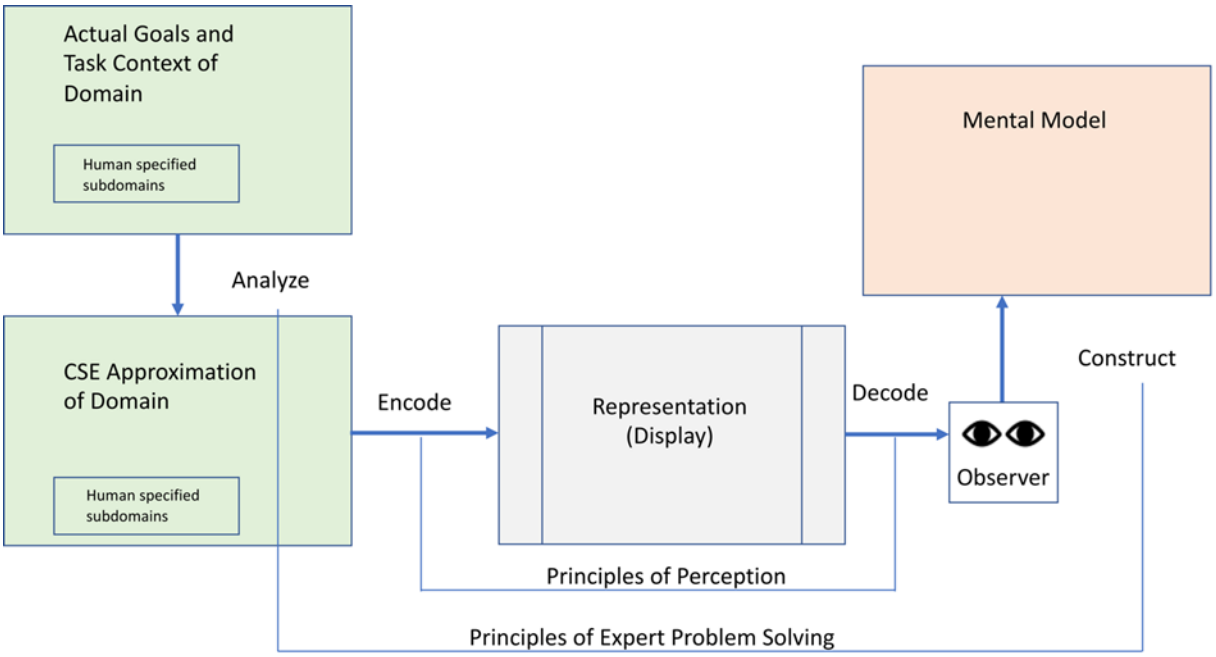

Figure 5. The Mapping Principle. (Adapted from Elm et al. [28]; originally in Woods [29]).

IV.B. Problem 2: Obtain Tacit Knowledge from Experts (Knowledge Elicitation)

The issue of tacit (undocumented) knowledge of the personnel within any complex sociotechnical work system presents many problems. The very complexity of the systems implies that it difficult if not impossible to document completely the details of every procedure.

Should any of these personnel leave without their knowledge being documented, critical gaps in organizational performance are likely to occur. In the Deep Water Horizon disaster, for example, only one senior employee had accurate (tacit) knowledge of how a critical test should be interpreted and he was away on training the day of the explosion. [30]. Understanding the tacit components of current processes would be particularly important in NPP modernization.

IV.B.1. Solution 1 to Problem 2. Using the EPRI Knowledge Elicitation Methods (Knowledge Elicitation)

EPRI performed a project to capture undocumented (tacit) task knowledge (EPRI 2004) [31]. The process began by asking several levels of management at a facility which worker had the most valuable tacit knowledge. Next, a similar question would be asked of peers in an organization, and finally, when an individual had been identified, he or she was asked what tacit knowledge they held that was believed by them as most valuable. For these knowledge elicitation exercises, a list of questions was developed for each expert. The knowledge elicitation team discussed the questions with the expert and followed up on answers that provided valuable information.

Interestingly, several times the experts said did not believe they had valuable tacit knowledge, but came to realize after the knowledge elicitation process that they did. For example, at an old fossil plant, two tacit knowledge experts were identified. One knew where buried pipes were located on the plant site, and no map of such pipe locations could be found. The second expert knew where all of the equipment drawings were located because they were more or less randomly stored. This was a very old plant and when equipment needed to be replaced, the plant would need to provide the drawings for the part to be custom built by an outside vendor because replacement parts or the entire unit were no longer available. Similarly, at a fuel fabrication plant, the identified expert was the only one who could quickly calculate

future radiation levels. Others were able to perform calculations that would provide similar results, but the difference was he could provide the results in 2 hours and others might require at least a day.

IV.B.2. Solution 2 to Problem 2. Using the EPRI Knowledge Elicitation Methods (Knowledge Representation)

Typically, the interviewer would meet for 2 days with each expert. Between days, he would prepare a document that outlined the expertise provided. This was modified by the expert, and follow-up questions were discussed. Finally, the team would finalize an outline of the tacit knowledge that was elicited. This constituted the knowledge representation component of the solution and typically included the use of concept maps.

IV.C. Comment on Problems and Solutions

The tools and methods presented in this report are not meant to be used rigidly; they are a means to practical solutions. In many circumstances, a "mix and match" among parts of different tools and methods may be appropriate given the circumstances. In any case, the application of any of the approaches described herein should be subject to the following usability criteria [32]. Usability is defined as a combination of usefulness and feasibility. Usefulness, in turn, is a combination of impact (the effect on the outcome) and uniqueness (compared with alternative available methods). Feasibility relates to available time and resources. It can be argued that the above solutions are both useful and feasible.

The interaction of the PTPG components in the work system must be attended to in the application of this approach. In each of the above examples, it is possible to parse out the relative contribution of people, technology, process, and governance to the overall function of the system. In the case of Problem 2, Tacit Knowledge, an individual *person* was the only one who had knowledge of where equipment drawings were located (*technology*). According to the

current *governance*, if equipment needed to be repaired, the *process* was to contact this individual. However, this revealed an in-balance in the relationship between the criteria: effectiveness, efficiency, and safety. The current system was efficient (quite cost effective) but only if the key employee was available. If he or she were absent, or had left the company, the outcome would likely result in serious consequences for effectiveness (accomplishment of mission) and possibly safety. As mentioned above, this is exactly what happened at Deep Water Horizon [30].

However, there were particular challenges in the solution to the Tacit Knowledge Problem. Some expert respondents did not want to provide their expertise because they wanted to come back as consultants following retirement. Others were afraid of being forced to retire after their knowledge was elicited; they were viewed as the expert on a topic by peers and management and they did not want to lose that status, or they were mad at the organization because they did not receive a promotion or the raise they thought they deserved.

Nevertheless, the organizational consequences of this kind of tacit knowledge being lost are so great that this effort is well worth the cost. This is particularly the case for plant modernization.

IV.D. Extended Application

An extended application of the socio-technical approach described above is presented in Kovesdi, et al. [33]. These were conducted in partnership with a utility concerned about modernization. This approach was applied to the analysis and design of two separate modernization use cases within the utility partner's operations.

The first, the Radiation Protection use case, was focused on identifying potential design approaches for improving efficiency and performance of maintenance-related RP tasks without loss of safety. The second, the Information Support use case focused on analysis and design of

methods and tools to enhance efficiencies in managerial decision making and issue resolution, specifically regarding support of forcing function meetings such as management review meetings. While each case used different analytic and design tools to accomplish its objectives, they both shared a fundamental emphasis on the core socio-technical principles presented above.

V. SUMMARY, CONCLUSIONS, AND RECOMENDATIONS

V.A. Summary

It is assumed that the modernization of nuclear power plants will require an advanced concept of operations, involving an integrated set of tightly coupled systems in which all stakeholders act in a coordinated manner. For this modernization effort to be enabled, we developed a human and organizational factors approach, based on a broad sociotechnical framework. Starting from core human factors principles, we conducted a literature review of the methods and approaches relevant to the modernization problem. These included core disciplines such as cognitive systems engineering, systems theoretic accident modeling and processes (STAMP), human systems integration, resilience engineering, and macroergonomics but also related topics of safety culture and organizational change. From this literature, we developed a conceptual framework centered around the work system with its four interacting components: people, technology, process, and governance. In an effective work system, these four components are jointly optimized according to three systems criteria: efficiency, effectiveness, and safety. System failure may result from excessive emphasis on any one criterion. The actual work of attaining joint optimization in a given work system can be accomplished by utilizing three high-level functions: knowledge elicitation, knowledge representation, and cross-functional integration. We illustrated the utility of this approach by applying it to practical problems and case studies.

V.B. Conclusions

Utilities are and will be modernizing their nuclear power plants. Many are pursuing a digital transformation instead of doing like-for-like replacements. A digital transformation process includes developing an advanced concept of operations applicable to plant design and operations, and the process needs to involve technology considerations, systems engineering, and human and organizational expertise.

In particular, the set of capabilities required for integrated operations, as seen in Figure 3, necessarily involves the combined operation of four components: (1) people, (2) technology, (3) process, and (4) governance. We have developed a human and organizational factors approach based on sociotechnical systems theory (see Figure 4) in which these four components are conceptualized as the elements of a work system; such elements are jointly optimized with respect to maintaining a balance among effectiveness, efficiency, and safety. Operationally, joint-optimization can be accomplished by applying three high-level human and organizational functions-- knowledge acquisition, knowledge representation, and cross-functional integration—and their associated tools. (See Figure 4.) Examples of the successful application of this approach have been presented. (See above and Kovesdi, et al. [33]).

V.C. Recommendations

It is recommended that the human and organizational strategic framework described above be considered in developing a Human Factors Engineering Plan at nuclear power plants that are planning a technology-centric modernization effort. This application could serve as a test case for the human and organizational strategic framework and will provide results that can be used to update and validate the framework.

It is further recommended that the human and organizational strategic framework should be integrated into the Plant Modernization Pathway from the Department of Energy Light Water

Reactor Sustainability Program Strategic Action Plan and Technology Centric Plant Operations Model.

ACKNOWLEDGMENTS

This manuscript has been authored by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Idaho National Laboratory issued document number for this paper is: INL/JOU-22-57908.

REFERENCES

[1] M. J. DAINOFF, L. HETTINGER, L. HANES, and J. C. JOE, "Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology," INL/EXT-20-57908, Idaho National Laboratory (2020).

[2] K. D. THOMAS and P. J. HUNTON, "Light Water Reactor Sustainability Program Nuclear Power Plant Modernization Strategy and Action Plan," INL/EXT-19-55852, Idaho National Laboratory (2019).

[3] P. J. HUNTON and R. T. ENGLAND, "Vendor-Independent Design Requirements for a Boiling Water Reactor Safety System Upgrade," INL/EXT-20-61079, Idaho National Laboratory (2020).

[4] J. C. JOE, T. MIYAKE, and A. HALL, "Guidance on Transforming Existing Light Water Reactors into Fully Modernized Nuclear Power Plants: The Role of Plant Modernization R&D," INL/LTD-21-64369, Idaho National Laboratory (2021).

[5] K. THOMAS et al., "Analysis and Planning Framework for Nuclear Plant Transformation," INL/EXT-20-59537, Idaho National Laboratory (2019).

[6] EPRI, "Digital Engineering Guide: Decision Making Using Systems Engineering," Technical Report 3002011816, Electric Power Research Institute (2021).

[7] EPRI, "Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification, " Technical Report 3002004310, Electric Power Research Institute (2015).

[8] U.S. NRC, "Human Factors Engineering Program Review Model," NUREG-0711 (Revision 3), U.S. Nuclear Regulatory Commission (2012).

[9] IEEE, "Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities," IEEE Std 1023™, Institute of Electrical and Electronics Engineers (2020).

[10] G. ROPOHL, "Philosophy of Socio-Technical Systems," *Society for Philosophy and Technology Quarterly Electronic Journal*, **4**, 3, 186–194 (1999).

[11] E. HOLLNAGEL, "Resilience – The Challenge of the Unstable," in *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. Wood, N. Leveson (Eds.), Ashgate Publishing Ltd., Farmham, UK (2006).

[12] E. HOLLNAGEL and D. D. WOODS, *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*, CRC Press, Boca Raton, FL (2005).

[13] M. J. DAINOFF, "Can't We All Just Get Along? Some Alternative Views of the Knowledge Worker in Complex HCI Systems," *International Journal of Human–Computer Interaction*, **25**, 5, 328-347 (2009); doi: 10.1080/10447310902864944.

[14] B. M. KLEINER, L. J. HETTINGER, D. M. DeJOY, Y. H. HUANG, and P. E. D. LOVE, "Sociotechnical Attributes of Safe and Unsafe Work Systems," *Ergonomics*, **58**, 4, 635-649 (2015); doi: 10.1080/00140139.2015.1009175.

[15] J. RASMUSSEN, A. M. PEJTERSEN, and L. P. GOODSTEIN, *Cognitive Systems Engineering*, Wiley, New York (1994).

[16] N. LEVESON, *Engineering a Safer World*, MIT Press, Cambridge, MA (2016).

[17] B. CRANDALL, G. KLEIN, and R. HOFFMAN, *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*, MIT Press, Cambridge, MA (2006).

[18] J. M. SCHRAAGEN, L. MILITELLO, T. ORMEROD, and R. LIPSHITZ, *Naturalistic*

Decision Making and Macrocognition, Ashgate, Burlington, VT (2008).
[19] G. KLEIN, J. ORASANU, R. CALDERWOOD, and C. ZSAMBOK, *Decision Making in Action: Models and Methods*, Ablex Publishing, Norwood, NJ (1993).
[20] H. BOOHER, *Handbook of Human Systems Integration*, John Wiley & Sons, New York, NY (2003).
[21] U.S. NRC, "NRC Safety Culture Policy Statement," 76 FR 34773, U.S. Nuclear Regulatory Commission (2011).
[22] IAEA, "Key Practical Issues in Strengthening Safety Culture" INSAG-15, International Atomic Energy Agency International Nuclear Safety Advisory Group, Vienna (2002).
[23] A. P. GONCALVES FILHO and P. WATERSON, "Maturity Models and Safety Culture: A Critical Review," *Safety Science*, **105**, 192–211 (2018); doi: 10.1016/j.ssci.2018.02.017.
[24] M. M. ROBERTSON and D. TUBBS, "Organizational Readiness for Change: A Systematic Literature Review and Field Experience as Related to Safety and Wellness Improvements at Work," presented at the *European Academy of Management Annual Meeting*, 2016.
[25] M. ROBERTSON et al., "The Intervention Design and Analysis Scorecard: A Planning Tool for Participatory Design of Integrated Health and Safety Interventions in the Workplace," *Journal of Occupational and Environmental Medicine*, **55**, 12, 86–88 (2013); doi: 10.1097/JOM.0000000000000036.
[26] A. L. DELBECQ, A. H. VAN DE VEN, and D. H. GUSTAFSON, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*, Green Briar Press, Middleton, WI (1986).
[27] K. J. VICENTE, *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*, Lawrence Erlbaum Associates, Mahwah, NJ (1999).
[28] W. ELM et al., "Pragmatic Use of Cognitive Work Analysis in System Design Extending Current Thinking by Adapting the Mapping Principle," in *Applications of Cognitive Work Analysis*, A. M. Bisantz and C. M. Burns (Eds.), CRC Press, Boca Raton, FL (2009).
[29] D. D. WOODS, "The Cognitive Engineering of Problem Tepresentation," in *Human-Computer Interaction and Complex Systems*, G. Weir and J. Alty (Eds.), Academic Press, London, UK (1991).
[30] E. BOEBERT and J. M. BLOSSOM, *Deepwater Horizon, A Systems Analysis of the Macondo Disaster*, Harvard University Press, Cambridge, MA (2016).
[31] EPRI, "Real Time Expert Knowledge Acquisition and Transfer: Needs and Technology Assessment," Technical Report 1009581, Electric Power Research Institute (2004).
[32] N. NAIKAR, "Beyond the Design of Ecological Interfaces: Applications of Work Domain Analysis and Control Task Analysis to the Evaluation of Design Proposals, Team Design, and Training," in *Applications of Cognitive Work Analysis*, A. M. Bisantz and C. M. Burns, (Eds.) CRC Press, Boca Raton, FL (2008).
[33] C. KOVESDI, J. MOHON, K. THOMAS, J. REMER, J. C. JOE, L. HANES M. J. DAINOFF, and L. HETTINGER, "Nuclear Work Function Innovation Tool Set Development for Performance Improvement and Human Systems Integration," INL/EXT-21-64428, Idaho National Laboratory (2021)