

Light Water Reactor Sustainability Program

Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology



April 2020

U.S. Department of Energy

Office of Nuclear Energy

DISCLAIMER

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

Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology

Marvin Dainoff, Larry Hettinger, Lew Hanes, and Jeffrey C. Joe

April 2020

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

ABSTRACT

Utility owners and operators of commercial nuclear power plants in the United States (U.S.) are and will be modernizing their nuclear power plants by performing a digital transformation involving design of an integrated set of systems that together enable a technology centric operating plant. The Plant Modernization Pathway of the U.S. Department of Energy Light Water Reactor Sustainability Program has a strategic action plan that lays the groundwork for a digital transformation of the nuclear industry. The model for this transformation is an advanced concept of operations, with an end point vision, “To achieve the maximum aggregate benefit enabled by this digital transformation.” To achieve this, the digital infrastructure for a nuclear plant must be designed as an integrated set of systems that together enable a technology centric operating model.

The digital transformation process obviously needs to involve technology considerations and systems engineering, but it also needs to include human and organizational expertise. Thus, human and organizational factors, including sociotechnical systems methods and techniques (e.g., Cognitive Systems Engineering, Systems Theoretic Accident Modeling and Processes, human systems integration, and Macroergonomics) need to be considered for digital transformation projects in order to effectively integrate human and organizational expertise efforts into the new work system that results from nuclear power plant digital modernization. That is, the work system is the basic unit of sociotechnical systems analysis and contains three components: personnel, technical, and organization and management. These components should be jointly optimized with respect to the interdependence of systems performance criteria of effectiveness, efficiency and safety. Joint optimization can be achieved through the application of three human and organization functions: knowledge representation, knowledge elicitation, and cross-functional integration. This report provides a strategic framework for effective integration of human and organizational expertise within nuclear power plant digital modernization efforts.

CONTENTS

ABSTRACT.....	iii
ACRONYMS.....	x
1. Introduction	1
1.1 Objectives.....	3
1.1.1 Objective 1. Description of the Core Model and Supporting Standards and Guidelines	3
1.1.2 Objective 2. Review of Human and Organizational Factors.....	4
1.1.3 Objective 3. Methodological Integration	4
1.1.4 Objective 4. Case Studies.....	5
2. NPP Modernization Strategy Action Plan	6
2.1 Plant Modernization Pathway	6
3. Relevant Standards and Guidelines	7
3.1 National and International Standards and Guidelines	7
3.1.1 EPRI Digital Engineering Guide.....	7
3.1.2 EPRI 3002004310 Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification (EPRI 2004a).....	8
3.1.3 NUREG-0711 Rev 3 HFE Program Review Model	8
3.1.4 IEEE 1023-2004.....	8
3.2 International Sources.....	9
3.2.1 IAEA HFE and Organizational Factors	9
3.2.2 NEA/OECD Overview.....	9
4. Review of Literature on Human and Organizational Factors	10
4.1.1 Sociotechnical Systems Theory	10
4.1.2 Macroergonomics.....	10
4.1.3 Cognitive Systems Engineering	10
4.1.4 Resilience Engineering	13
4.1.5 STAMP/Systems Theoretical Process Analysis.....	13
4.1.6 Macro cognition/Naturalistic Decision-Making	15
4.1.7 Human-Systems Integration.....	15
4.1.8 Safety Culture/Climate.....	15
4.2 Organizational Change.....	18
4.2.1 Organizational Readiness for Change	18
4.2.2 Determining the Best Pathway for Implementing Change.....	20
4.2.3 Illustrative example: Transforming the DOD with Human-Centered Artificial Intelligence	21
4.2.4 Change Agents: A Pragmatic Approach	23
5. Conceptual and Methodological Framework	24
5.1 Introduction: The Translation Problem.....	24
5.2 Selecting Solutions with Field Based Utility	24

5.2.1	Cognitive Work Analysis.....	24
5.2.2	Safety Climate.....	24
5.2.3	STAMP Mental Model Extension.....	25
5.2.4	Resilience Engineering: Learning from Incidents.....	26
5.3	Methodological Integration.....	26
5.3.1	Conceptual Overview.....	26
5.3.2	Basic Unit of Analysis: Capability Development and the Work System.....	26
5.3.3	Fundamental Problems in Achieving Joint Optimization	28
5.3.4	Knowledge Representation	28
5.3.5	Knowledge Elicitation.....	39
5.3.6	Cross-Functional Integration.....	41
5.3.7	Literature Review Summary as Example of Concept Map.....	41
5.4	A Problem-Solving Approach to Methodological Integration	42
5.4.1	Problem 1 Management Consensus and Problem 2 Consensus on Core Values	43
5.4.2	Problem 3: Source for Core Values.....	46
5.4.3	Problem 4: Develop HFE Program Management Plan	48
5.4.4	Problem 5: Obtain Tacit Knowledge from Experts.....	54
5.4.5	Problem 6: Alignment/Misalignment of Existing Skills to New Technology	56
5.4.6	Problem 7: Integration of PTPG and Governance at all Levels of the System.....	58
5.4.7	Problem 8: The Silo Problem.....	60
6.	Summary, Conclusions, and Recommendations	61
6.1	Summary	61
6.2	Conclusions.....	65
6.3	Recommendations	65
7.	References	66
	Appendix A.....	1
	Exemplary Case Studies	1
	A.1 Zumwalt Class of U.S. Navy Destroyers.....	1
	A.2 Boeing 737 MAX	4
	A.3 Deepwater Horizon.....	6
	A.4 USS John S. McCain Accident.....	8
	A.5 Westinghouse Commercial NFD TQ Program.....	10
	Appendix B	15
	The Translation Problem.....	15

FIGURES

Figure 1. Technology Centric Plant Operations Model (Thomas and Hunton 2019).	2
Figure 2. A Model of Integrated Operations Merging Capability Development and Work Reduction Strategies (Thomas 2019).	7
Figure 3. Generic safety control structure (After Levenson 2011).	14
Figure 4. General form of a model of sociotechnical control (Levenson 2011, p 82).	14
Figure 5. Traits which define a positive safety culture, according to NRC.	16
Figure 6. Predictors of Organizational Readiness to Change (Robertson and Tubbs 2016).	19
Figure 7. Intervention Design and Analysis Scorecard (IDEAS) (Robertson et. al 2013).	20
Figure 8. Revised Project/Product Management Model (Trent 2019).	22
Figure 9. Human-Centered AI (Trent 2019).	22
Figure 10. Mapping capability development components PTPG onto Macroergonomic work system (Thomas 2019, Hendrick and Kleiner 2001)	27
Figure 11. The Mapping Principle (Adapted from Elm et al. 2009; Original in Woods, 1991).	30
Figure 12. Above and below the line of representation (Cook 2019). Copyright 2016–18 by R.I. Cook for ACL, all rights reserved.	32
Figure 13. SCS of generic maintenance process example: Work as envisioned. Modified from Levenson (2011).	35
Figure 14. SCS of generic maintenance process example: Work as practiced. Modified from Levenson (2011).	35
Figure 15. Generic SCS Modified from Levenson (2011).	36
Figure 16. Human controller mental model. (Adapted from France 2017, Figure 18).	37
Figure 17. Example of MEAH. (Lintern 2009, Figure 4).	38
Figure 18. MEAH for Work Domain: Generic Commercial Processing Facility. (Modified from Naikar 2013)	38
Figure 19. Concept Map Representation of Literature Review	42
Figure 20. INCOSE Data on Project Failure (Dainoff 2006).	44
Figure 21. Conceptualized depiction of WDA of core values.	48
Figure 22. Intervention Design and Analysis Scorecard. Modified from Robertson, et al. (2013) [http://links.lww.com/JOM/A134]	49
Figure 23. WDA Example Illustrating Automation of Turbine Control (After Vicente 1999).	52
Figure 24. Control structure of negative pressure test on <i>Deepwater Horizon</i> (After Boebert and Blossom 2019).	53
Figure 25. Mapping PTPG into the work system.	59
Figure 26. Shared mental models (Cronin and Weingart 2007).	61
Figure 27. Strategic Integration Framework presented as a concept map.	64
Figure A-1. The <i>USS Zumwalt</i>	1

Figure A-2. The Boeing 737 MAX.	4
Figure A-3. The <i>Deepwater Horizon</i>	6
Figure A-4. Damage sustained by the <i>USS John S. McCain</i> in its collision with the tanker <i>Alnic MC</i>	8
Figure A-4. Triangle developed by NFD that identifies conditions of excellence to fulfill TQ requirements.	12
Figure A-5. Baldrige Excellence Framework with Table of Contents for document describing Framework shown at bottom.	13
Figure B-1. Stokes' Two Dimensional Classification of Research (https://en.wikipedia.org/wiki/Pasteur%27s_quadrant#cite_note-2).	16

TABLES

Table 1. Matrix of problems and solutions.	43
Table 2. Fitness function criteria.....	45
Table 3. Resilience Engineering criteria.	47
Table 4. Baldrich award criteria.....	47
Table 5. NRC safety culture traits.....	47

ACRONYMS

BCPE	Board of Certification in Professional Ergonomics
BOP	Blowout Preventer
CSE	Cognitive Systems Engineering
CWA	Cognitive Work Analysis
DEG	Digital Engineering Guide
DOD	Department of Defense
DOE	U.S. Department of Energy
DSS	Decision Support System
EFC	enzymatic floor cleaning agent
EFM	Ergonomist Formation Model
EPRI	Electric Power Research Institute
FAA	Federal Aviation Administration
HFE	Human Factors Engineering
HSI	Human-System Interface
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IDEAS	Intervention Design and Analysis Scorecard
INSAG	International Nuclear Safety Group
IEEE	Institute of Electrical and Electronics Engineers
IRS	Internal Revenue Service
JAIC	Joint Artificial Intelligence Center
JCS	Joint Cognitive Systems
LWR	Light Water Reactor
LWRS	Light Water Reactor Sustainability
MCAS	Maneuvering Characteristics Augmentation System
MEAH	Means-End Abstraction Hierarchy
NASA	National Aviation and Space Administration
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NFD	Westinghouse Commercial Nuclear Fuel Division
NIOSH	National Institute of Occupational Safety and Health
NIST	National Institute of Standards and Technology
NGT	Nominal Group Technique

NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Commission Regulations
OECD	European Organisation for Economic Cooperation and Development
PTPG	people, technology, process, and governance
R&D	Research and Development
RCS	Risk Control Services
SCS	Safety Control Structure
STAMP	Systems Theoretic Accident Modeling and Processes
STPA	Systems Theoretic Process Analysis
TCS	Turbine Control System
TQ	Total Quality
USS	United States Ship
WDA	Work Domain Analysis

Addressing Human and Organizational Factors in Nuclear Industry Modernization: An Operationally Focused Approach to Process and Methodology

1. Introduction

The United States (U.S.) Department of Energy (DOE) sponsors work to enhance the success of the U.S. nuclear industry under a program entitled Light Water Reactor Sustainability (LWRS). Under the LWRS Program, the Plant Modernization Pathway conducts targeted research and development (R&D) to address aging and reliability concerns with the legacy instrumentation and control (I&C) systems in operating U.S. commercial nuclear power plants (NPPs), or the light water reactor (LWR) fleet. This work involves two major goals: (1) ensuring that legacy analog I&C systems are not life-limiting issues for the LWR fleet, and (2) implementing digital I&C technology in a manner that enables broad innovation and business improvement in the NPP operating model.

Within the framework of the Plant Modernization Pathway, a Strategy and Action Plan, and a Technology Centric Plant Operations Model (K. D. Thomas and Hunton 2019) have been formulated to address the most pressing needs of the industry, in terms of needs for near-term performance improvement and cost reduction.

This Strategy and Action Plan...presents a digital strategy overview, describing a broad approach to plant modernization that ensures long-term technical and economic viability is achieved by defining the future concept of operations, and then basing all modernization activities on this end-state vision (Thomas and Hunton 2019).

In direct support of this plan, an R&D project in the Plant Modernization Pathway has been initiated, with the overall goal to develop a strategic framework for effective integration of human and organizational factors within NPP digital modernization efforts. This framework extends traditional human factors engineering (HFE) concepts to a sociotechnical perspective, which focuses on jointly optimizing elements of work systems containing both technical and social/organizational components. In achieving such optimization, three basic problems must be solved: knowledge acquisition, knowledge representation, and cross-functional integration. Practically, such concerns include organizational influences (e.g., communications, organizational decision-making, etc.), and synchrony of system mental models within and across organizational levels. While the major focus will be on supporting the end-state digital transformation process, it must be emphasized that the material in this report can be much more broadly applicable. This point will be elaborated below.

A major premise of the Strategy and Action Plan and Technology Centric Plant Operations Model is that digital technology is a cornerstone enabler of a sustainable nuclear power industry. Implementation of this technology requires a digital transformation. Figure 1 crystalizes the NPP Modernization Strategy in which the end point vision is an Advanced Concept of Operations, the strategic objectives of which are achieved via a digital transformation strategy (Thomas and Hunton 2019). This Advanced Concept of Operations drives transformative enterprise changes from the top down, as shown in Figure 1. A business-driven approach is used to reformulate the operating model of a commercial nuclear plant from one that is labor-centric to one that is technology centric, using a top-down/bottom-up process (Thomas and Hunton 2019).

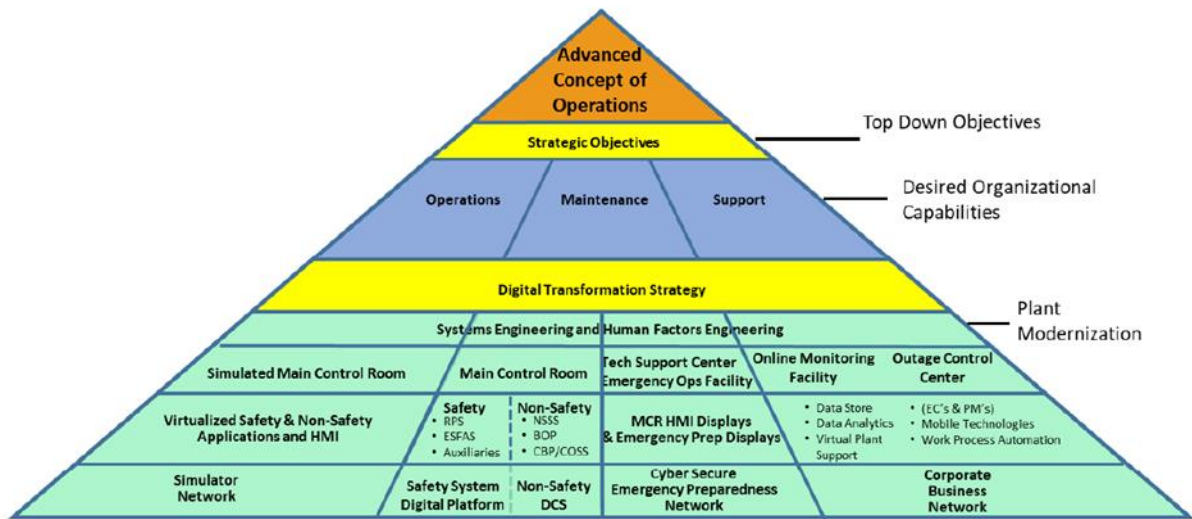


Figure 1. Technology Centric Plant Operations Model (Thomas and Hunton 2019).

However, the NPP Modernization Strategy reflected in Figure 1 also reflects the reality of a continuum from the base to the apex with respect to an individual utility company's perceptions of their own concepts of operations in the modernization process. At the apex is an advanced concept of operations philosophy, which assumes a simultaneous top-down and bottom-up process. Sets of strategic objectives lead to a fully integrated transformation strategy, with a simplification of individual work functions mapped onto higher-level objectives. In contrast, the base of the figure represents a primarily like-for-like bottom-up replacement philosophy, in which individual legacy components are replaced by digital variants. Some utility companies will have approaches to modernization located between these extremes.

It should be mentioned that concept of operations can have different meanings. According to the Glossary in NUREG-0711, Rev 3, from an HFE perspective, a concept of operations:

Defines the goals and expectations for the new system from the perspective of users and other stakeholders and defines the high-level considerations to address as the detailed design evolves. An HFE-focused ConOps addresses the following six dimensions:

- *Plant Goals (or Missions)*
- *Agents' Roles and Responsibilities*
- *Staffing, Qualifications, and Training*
- *Management of Normal Operations*
- *Management of Off-normal Conditions and Emergencies*
- *Management of Maintenance and Modifications*

Consequently, like many academic and professional areas of discourse, the definition of key terms depends on their context. In this case, the description of advanced concept of operations will be considered Meaning 1 and the NUREG-0711 definition will be Meaning 2 (NRC 2004).

Therefore, assuming an advanced concept of operations (Meaning 1), legacy components and processes need to be replaced with fully integrated digital systems. For this to occur, it is necessary to establish high-level strategic objectives focused on the achievement of designs and practices that effectively integrate and address human-system performance capabilities. From such objectives, concept

of operations (Meaning 2) and functional requirements based on identified technological, organizational, and other enablers of effective human-system performance will be derived. During the design process, it is critical that there is harmonization among these technological, organizational, and other enablers. This is most efficiently addressed by incorporating human and organizational factors expertise within the systems engineering processes and teams working on specific modernization efforts. This level of integration and collaboration also supports the identification and promulgation of human factors best practices for individual plant and fleet modernization programs.

Such optimization and integration require new tools and methods; the goal of this project is to provide these. Traditional HFE has a long and valued history in the nuclear industry as an enabler of effective and safe human operator performance. Human and organizational factors build on this history by extending its focus beyond the control room operator to all stakeholders in the design process. Thus, the goal is to enhance the performance, not only of stakeholders in the system engineering process, but also of stakeholders beyond (before and after) the systems engineering process. While the performance enhancement tools and methods which follow in this report are critical for success in advanced concept of operations (defined by closely integrated systems), these tools and methods are broadly applicable to many aspects of NPP modernization.

The starting point of this research project is a review of literature on sociotechnical systems analysis (see definition above). This will include approaches derived from the areas of Cognitive Systems Engineering (CSE), the Systems Theoretic Accident Modeling and Processes (STAMP) framework, Human-Systems Integration, Resilience Engineering, and Macroergonomics. In performing this work, two general principles have been considered. First, under the assumption that digital transformation will result in incorporating many previous human operations into digital form (i.e., automation), the operational capabilities given to the remaining human operators become just that more critical. This will be particularly the case for the inevitable unpredictable event, not covered in normal operating, abnormal, and emergency procedures. Second, inherent in the description of the systems engineering process in advanced concept of operations is the problem of organizational silos, which are defined as barriers (formal and informal) to communication and collaboration across organizational boundaries. A major challenge is the breaking down of existing organizational silos, preventing the development of future silos, and the facilitation of serious and active collaboration among all parties throughout all phases of system design, test and operation.

1.1 Objectives

In this report, we are focusing only on those human and organizational issues required to achieve the necessary integration across multiple levels of both system development and operation. More traditional HFE issues related to the process used and methods applied in the nuclear industry, although referenced and summarized below, will not be discussed in detail since these are more than adequately covered elsewhere.

1.1.1 Objective 1. Description of the Core Model and Supporting Standards and Guidelines

The research team has identified key components of the Technology Centric Plant Operations Model (Thomas and Hunton 2019) and the associated description of the Plant Modernization Pathway. We examined relevant portions of the Electric Power Research Institute (EPRI) Digital Engineering Guide (DEG), applicable U.S. Nuclear Regulatory Commission (NRC) guidance, and Institute of Electrical and Electronics Engineers (IEEE) standards. In these materials, we found a consistent emphasis on the need for integration and collaboration among stakeholders and the need for communication across all levels of the system. *However, and critically*, these documents were largely silent on describing procedures or processes for how these needs will be met. In particular, we found the integration requirements of the DEG particularly coherent with those contained in the Technology Centric Plant Operations Model,

described herein. The EPRI HFE Guide for Control Room Design (EPRI 2015) should also be referenced. It has, for example, some guidance regarding team member qualifications and methods. Also, this report is referenced extensively in the DEG (EPRI 2018a).

The team also reviewed materials from the International Atomic Energy Agency (IAEA) and the European Organisation for Economic Cooperation and Development (OECD). In both sources, we found clear indications that a strong safety culture needed to be included in any organizational consideration. Though Figure 1 does not explicitly include safety culture as an analytic focus area, given this evidence, we have included it in our discussion. At the same time, the IAEA document identifies resilience as an essential component of modern NPPs. This supported our decision to give resilience engineering a prominent place in our discussion.

1.1.2 Objective 2. Review of Human and Organizational Factors

Given the gaps between integration requirements and integration process already identified in Objective 1, Objective 2 will constitute a review of the literature in the area of human and organizational factors relevant to the achievement of our broader, organizational integration goals. Given the discussion above, we have divided this review into two portions: literature based on sociotechnical systems theory and a review of safety culture and the related concept of safety climate.

The team turned first to the sociotechnical system theory section. We identify sociotechnical systems theory as fundamental to all of the major conceptual areas we have reviewed, including Macroergonomics, CSE, and human-system integration. Within CSE, we further discuss cognitive work analysis (CWA), Resilience Engineering, STAMP, and Macrocognition/naturalistic decision-making. In each case, we identify potential attributes of the approach which might aid our third objective—methodological integration.

The initial strategy for this project was to review and summarize a large range of possible, sociotechnically-based methodologies. However, it was decided that this would not be an effective use of resources. First, a recent and thorough review of 52 methods relevant to sociotechnical system theory already exists (Waterson et al. 2015). Second, the large number of such methods gave pause as to the underlying context in which individual methods are developed. Specifically, it was questioned whether the large number of academically based methods was the result of academic pressure to work independently and create something novel, rather than build on an existing framework. Additionally, there was concern that same pressure would generate methods which, while methodologically sophisticated enough to pass scrutiny of journal editors, might be less likely to be sensitive to demands of field work utility. Accordingly, it was decided to focus on those methods where there was evidence of existing communities of practice; involving ongoing collaboration among multiple groups, continual modification and development, and where there is a history of successful use in practical application. Experience with the development of human-system integration methods in the construction of the United States Ship (USS) *Zumwalt* and Westinghouse Commercial Nuclear Fuel Division (NFD) Total Quality (TQ) program discussed in Appendix A supports this pragmatic strategy.

In the safety culture section, we identify some conceptual concerns with the core concept itself. At the present time, there is a lack of scientific consensus on either the basic definition or reliable and valid metrics of safety culture^a. As part of Objective 3, we present a prolonged discussion of the culture question which presents a potential solution.

1.1.3 Objective 3. Methodological Integration

Our objective is to provide a high-level description of a set of human and organizational methods that can support modernization strategies. At present, we can employ a core concept from Macroergonomics called the *work system* to represent the integration of people, technology, process, and governance

^a As we discuss, this lack of scientific consensus is not the case for safety *climate*.

(PTPG) needed to support effective, sustainable modernization. With this as a basis, we envision a combination of methodologies grounded in CSE, STAMP, and resilience engineering that can provide the means for embedding high-level organizational values directly into the systems engineering process, and, more importantly, provide a mechanism for visualizing how high-level values might influence potential tradeoffs at the work function and sub-capability level. We argue that incorporating basic organizational values within a systems engineering framework can also avoid the conceptual problems with safety culture. In addition, within the section on knowledge elicitation, we identify specific techniques, such as the Nominal Group Technique (NGT), for extracting information and establishing consensus among stakeholders.

There are two additional challenges, which we deal with in this report. The first is scalability. As discussed in the introduction, not all individual utility company modernization strategies will be at the apex of Figure 1. Our methodological recommendations will need to consider these intermediate and lower-level use cases. Second, we need to be concerned about the modernization process as well as the operational issues. We note that both CWA and STAMP address this second concern explicitly.

1.1.4 Objective 4. Case Studies

Our fourth objective is to present a series of case studies (Appendix A) illustrating key concepts raised throughout the body of the report. Our intention is that these serve as illustrative material for the technical discussions in the main body of the report, particularly regarding methodological integration and social/organizational factors impacting the design and/or use of safety-critical systems. The specific case studies include: The ‘sailor-centric’ design of the *Zumwalt* class of U.S. Navy destroyers, the Boeing 737 MAX accidents and associated development background, the 2017 USS *John S. McCain* accident, the *Deepwater Horizon*/Macondo spill, and the NFD TQ Program that resulted in the Malcolm Baldrige National Quality Award. These case studies represent a cross-section of situations in which significant organizational pressures have impacted the design and use of complex technical systems within a variety of safety-critical environments.

2. NPP Modernization Strategy Action Plan

To achieve the maximum aggregate benefit enabled by this digital transformation, the digital infrastructure for a nuclear plant must be designed as an integrated set of systems that together enable a technology centric^b operating model. The Technology Centric Plant Operations Model (Thomas and Hunton 2019) represents such an approach (Figure 1). The model can be interpreted as implying a continuum along the side with respect to the location of an individual utility company's perceptions of their concepts of operations of the modernization process. The advanced concept of operations philosophy at the top of Figure 1 assumes a simultaneous top-down and bottom-up process. A fully integrated transformation strategy is derived from sets of strategic objectives through the mapping of the strategic objectives onto individual work functions. In contrast, a primarily like-for-like, bottom-up replacement philosophy, in which individual legacy components are replaced by digital variants is represented at the base of the figure. Different utilities will have modernization strategies located between these extremes.

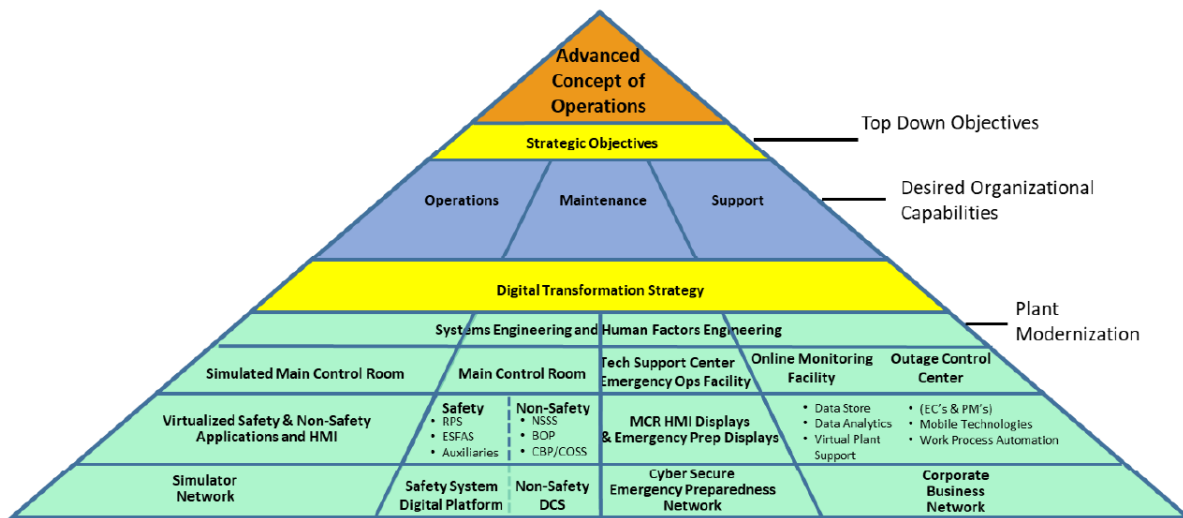


Figure 1. (repeated). Technology Centric Plant Operations Model (Thomas and Hunton 2019).

2.1 Plant Modernization Pathway

Figure 2 (Thomas and Hunton 2019) further refines various aspects of potential strategies for plant modernization. Two separate but related aspects of the strategy are indicated. Capability Development (top half of Figure 2) consists of a planning process that focuses transformation on those core capabilities that truly define value in the eyes of the ultimate customer. Capability is the synthesis of the PTPG dimensions. From an analytic perspective, capability starts at the individual function level, with functions becoming successively integrated at higher levels. From a concept of operations perspective, however, the starting point is the highest level one can achieve, applying a set of basic principles that reflect the end-state vision, and effectively propagate downward. The bottom of Figure 2 reflects the work reduction focus, which is to be systematically applied.

^b Technology centric in this context means that the operating model for commercial NPPs uses technology safely, but also to the greatest extent possible to realize workload efficiencies. In contrast to the current, heavily labor centric operating model used at virtually all commercial NPPs, a technology centric operating model allows NPPs to safely reduce Operation and Maintenance costs.

3.1.2 EPRI 3002004310 Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification (EPRI 2004a)

This technical report provides comprehensive HFE guidance for NPP control room Human System Interface (HSI) design and modification. The research team's review of this guide, however, focused primarily on investigating various qualitative approaches it suggests using to determine the impact of digital systems and infrastructure on overall plant safety and risk factors. While acknowledging that social and organizational factors play a significant role in determining levels of safety and risk, the report's level of analysis was strictly focused at the control room level and did not directly address organizational factors per se. Regardless, the investigators concluded that HFE must be an integral part of the systems engineering process. From the Report Summary (p. v):

This report provides guidance on planning, specifying, designing, implementing, operating, maintaining, and training for modifications to control rooms and related facilities, and making effective use of digital instrumentation and control (I&C) systems and human-system interfaces (HSIs). Guidance is also provided on planning for new build HSI design and licensing efforts.

Section 2.5.1.4 requires 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, Section 2.5.3.5 emphasizes that HFE should be involved in gathering user input to design, for performing required design verification, and providing a structured process for accomplishing these functions.

3.1.3 NUREG-0711 Rev 3 HFE Program Review Model

NUREG-0711 contains detailed review criteria that NRC staff should use to evaluate an applicant's submissions regarding its HFE program and is not a design guideline for utilities. The review criteria for the regulator consist of a model of the process divided into key elements (e.g., HSI design and integration, procedure development, training program development) and the indicators of the best practices for each. These indicators are used to assess an organization's HFE program.

The definition of HSIs in the glossary of NUREG 0711 notes that their effectiveness is impacted by numerous factors, including the influences of management/cultural factors and safety culture:

The use of HSIs also can be affected indirectly by other aspects of plant design and operation, such as personnel training, shift schedules, work practices, and management/organizational factors, such as the plant's safety culture. (p. 114)

The NRC has also documented the requirement for nuclear plant safety culture in its 2011 Safety Culture Policy Statement (76 FR 34773). This requirement is described in more detail in Section 4.1.8.

NUREG-0711 contains many specific guidelines for reviewing the integration and coordination of HFE functions and processes that are fully consistent with the integration requirements of the Technology Centric Plant Operations Model. However, the description of specific mechanisms for accomplishing these goals are not part of its scope. While over-specifying a desired approach may be undesirable for many reasons (e.g., restricting creative, adaptive responses to emergent system design issues), general guidance is clearly something that the regulator and industry require (Thomas and Hunton 2019).

3.1.4 IEEE 1023-2004

IEEE 1023-2004 provides recommended practices to engineering personnel for the development of integrated programs for applying HFE to the design, operation, and maintenance of nuclear power generating stations and other nuclear facilities (IEEE 2004). Among other things, it contains guidance for program organization, the design aspects to consider, the human factors methodologies and tools to apply, and for developing a human factors program plan (Desaulniers and Flegler 2019).

Clause 5.5.9 of IEEE 1023-2004 states that, “Organizations should strive to maintain a culture that values “safety first”. Training and appropriate reinforcement for desired (e.g., safety-promoting) behaviors should be considered, obstacles to desired behaviors (e.g., fear of reprisal) should be reduced, and undesirable (e.g., unsafe) behaviors should be prevented or discouraged.” Additionally, this document recommends integration of HFE with overall planning and systems engineering processes. However, it provides no specific guidance as to how such integration is to be carried out.

3.2 International Sources

3.2.1 IAEA HFE and Organizational Factors

Recent IAEA guidance has emphasized the notion of system resilience, including the notion that the more perfectly a system is developed for a specific situation, the more inflexible it becomes for situations that might occur outside the defined boundaries of that situation. Flexibility is essential to be able to adapt to the unexpected and guard against the belief that all situations have been anticipated. The resilient organization is one that quickly realizes deviation from normal operations and has the ability to make even the toughest and least popular decisions and to manage the margins in which it can maneuver. The resilient organization knows how far it can push its boundaries because it has learned from successful normal operations how flexible its systems are. This type of thinking and strategizing represents a paradigm shift away from the traditional way that organizations try to manage the unexpected to maintain safety.

IAEA guidance also states that safety culture should be a top priority for all organizations. Leadership and management for safety are critical in the development and maintenance of a strong safety culture. The International Nuclear Safety Group (INSAG) has emphasized the need to establish a safety culture in which safety is the highest priority and in which everyone involved in the nuclear enterprise accepts personal and individual responsibility for it. The interaction of human, organizational, and technical factors across all stakeholder organizations and between different levels inside each organization must be evaluated and understood for each phase of the nuclear facility life cycle. Those interactions will occur within the broader scope of the culture of the organization and, in this way, will reflect the organization’s safety culture. The safety culture exists within the context of the organizational culture and broader external factors that must be considered in any assessment. Risk management is an important element of safety culture. A false sense of security in measures such as defense in depth, redundant, and complex safety features and “managed” risk can all result in a sense of complacency. As stated in (INSAG 2002), “[T]he key [to improving safety] will always be constant vigilance, as there is no room for complacency or anything less than a total commitment to improving safety... The establishment of a robust and enduring safety culture” is crucial (p. 30).

3.2.2 NEA/OECD Overview

The Nuclear Energy Agency (NEA) is contained within the OECD. The NEA maintains a Committee on the Safety of Nuclear Installations (CSNI) comprising several working groups, including the Working Group on Human Organisational Factors. The working group’s intent is to provide a forum for the examination of issues of direct relevance to those identified in this report.

Two of the working group’s recent reports touched on issues central to effective integration of humans and technical systems (NEA/IAEA 2006) as well as the potential impact of social/organizational factors (NEA/IAEA 2012). With the development of new plants and upgrading of existing plants with new control station technologies, new concepts of operations will need to be developed. This will require a balance among technology, economics, and human performance.

As concepts of operation change, so will the associated nature of teamwork in operations. Other changes are likely to include integrated operations between local and remote sites, teams made up of humans and intelligent systems, and multi-unit control from a single control room, all of which imply

significant changes in the structure and functions of teams and organizations within a given nuclear utility.

4. Review of Literature on Human and Organizational Factors

This literature review is based on a combination of (M.J. Dainoff 2009) and (M.J. Dainoff 2017), as well as the Hopkinton Conference on Sociotechnical Systems and Safety (Carayon et al. 2015). Additional materials have been added on organizational change.

4.1.1 Sociotechnical Systems Theory

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 the social conditions of work, in such a way that efficiency and humanity would not contradict each other any longer (Ropohl 1999).

The goal of sociotechnical systems theory, as applied to systems design, is joint optimization of social-organizational and technical sub-systems. 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) (Grant et al. 2018).

Sociotechnical systems theory provides a pathway to these goals and is foundational for several core disciplines within the HFE community, including Macroergonomics, human systems integration, and CSE (Dainoff 2009).

4.1.2 Macroergonomics

Macroergonomics is a sociotechnically-based scientific and technical domain that has provided numerous useful methods for the design and analysis of work systems.

According to (Kleiner et al. 2015), viewed within the Macroergonomic approach, a work system involves two or more people interacting with some form of technology and/or work process within an internal environment (including physical, psychosocial, and cultural components) and surrounded by an external environment (including the financial, cultural, social, and political milieus). In this regard, it seems quite similar to the Capability Development approach (see Section 2.1) that emphasizes the importance of the effective integration of PTPG.

Work activities within the work system are constrained by the social and technical components and boundaries of that system. The higher-order goal of the system is joint optimization, in which there is a balance between social and technical components. As will be seen, failures of safety can usually be attributed to failures of joint optimization (e.g., relaxation of safety constraints in the service of increased productivity).

4.1.3 Cognitive Systems Engineering

CSE is a form of systems engineering and, as such, requires understanding and description at multiple levels of analysis. This perspective is effectively communicated through the interplay of the:

Sharp and blunt ends of a complex system. The sharp end is where practitioners use their expertise to directly interact with the system to achieve desired goals. The blunt end is where managers, regulators, and developers allocate resources, define constraints, and provide incentives. Mutual communication and adaptation occurs between sharp and blunt ends (Hollnagel and Woods 2005, p. 8).

An understanding of both pathways is necessary to understand successful or unsuccessful functioning.

This review will focus only a limit set of subspecialities within CSE; concentrating on those we believe will have direct relevance to our overall modernization strategy goals. We will not discuss important areas such as cognitive task analysis or Situation Awareness. A more complete description can be found in Dainoff (2009). An alternative perspective can be found in (Roth 2008). She applies the description “Cognitive Work” to a wide variety of techniques for accomplishing this work including cognitive task analysis (Militello and Hutton, 1998), CWA (Vicente, 1999), and applied cognitive systems engineering (Elm et al. 2009).

4.1.3.1 Cognitive Work Analysis

CWA provides a set of modeling tools and an overlying conceptual framework for their application. The outcome of the analysis provides a perspective that allows for the development of support tools (the ecological interface) that makes the underlying system structure and dynamics transparent and allows the operator to make rapid adaptations to unforeseen events.

A complete description of CWA is found in (Rasmussen et al. 1994), with a more pedagogical treatment by Vicente (1999). CWA explicitly takes as its point of reference the description and characterization of complex sociotechnical systems (Rasmussen, Pejtersen, and Goodstein, 1994; Vicente, 1999). The approach is formative in the sense that it provides a set of requirements that should be satisfied if work is to be supported effectively (Vicente, 1999, chap. 5). This can be contrasted with descriptive (what is) or normative methods (what should be). In ecological terms, these are collections of potential affordances, in which affordances are defined as attributes of the environment of an individual described with respect to the action capabilities of that individual (Gibson, 1979) (Dainoff and Mark 2001).

Two separate contributors to CWA are identified. The original Vicente/Rasmussen (Vicente, 1999; Rasmussen et al. 1994) approach, which we intend to generalize to higher-level top-down processes including fundamental values and goal of top management, and the modifications of Naikar (Naikar et al. 2003), which explicitly includes changes in staffing configurations. This should be particularly relevant to staffing issues in redesigned digital control rooms.

4.1.3.2 Basic Outline of CWA

CWA provides a set of modeling tools and an overlying conceptual framework for their application. The outcome of the analysis provides a perspective that allows for the development of support tools (the ‘ecological’ HSI) that makes the underlying system structure and dynamics transparent and allows the operator to make rapid adaptations to unforeseen events. The tools are applied in a systematic order so that each level reduces the available degrees of freedom of the level below.

The first stage is work domain analysis (WDA). This tool allows for characterization of the overall landscape of work, embodying all possibilities for action. A key step is the identification of intrinsic behavior-shaping constraints. These provide a boundary within which a variety of different actions are possible. This is central concept in CWA; the goal is to characterize this landscape at a level of abstraction which is independent of any particular technology.

The second stage is control task analysis. If the work domain is characterized by nouns, the control task analysis is characterized by verbs. For all action possibilities, a set of information queries and goals states are identified.

The third stage, strategies analysis, further reduces the available degrees of freedom by identifying strategies for deciding among alternative decision pathways.

The fourth stage is social organizational. It inherits the constraints of the previous stage but adds social-organizational components.

The fifth and last stage is where worker competencies are considered. It is of some interest that the point of entry of the main findings of cognitive psychology into the process is at the end. However, this is

quite deliberate. The requirements of the domain should determine the worker competencies needed, rather than assuming a set of pre-existing competencies and then designing the system around them (Vicente, 1999, p. 275).

4.1.3.3 *Application of CWA to Staffing Needs*

According to Naikar et al. (2003), an important dimension of the modernization process will be the need to reallocate job functions and staffing needs to a redesigned digital system. The following summary provides a framework as to how this might be accomplished.

1. Work Domain Analyses capture:
 - a. The functional purposes or high-level objectives of the proposed work systems
 - b. The priorities and values that must be preserved during system operation
 - c. The general functions that the system must coordinate and/or execute to fulfill its functional purposes
 - d. The physical functions or functionality afforded by the physical devices of the system
 - e. The physical form or physical devices of the proposed work system.
2. Activity analysis in work domain terms, to identify the set of work situations that workers will be required to participate in or the set of work problems that workers will be required to solve in order to fulfill work-domain constraints.
3. Table-top analysis (Kirwan and Ainsworth, 1992) that utilizes the WDA and the activity analysis to explore the feasibility of alternative team designs for a proposed work system (consistent with a formative approach to work analysis because it supports an examination of how work can be done rather than how work is currently done or how work should be done). The table-top analysis involves:
 - a. Specifying the team concepts to examine including team-design variables (e.g., team size, number of levels of hierarchy) and plausible values for each variable
 - b. Designing scenarios that are representative of the kinds of situations that the proposed system may encounter
 - c. Holding discussions with subject matter experts to explore how the work demands of the scenarios can be distributed across team members given different team concepts
 - d. Translating the distribution of scenario-specific work demands for each team concept into a distribution of work problems from the activity analysis
 - e. Using the WDA to evaluate the alternative team concepts in terms of how well the alternative distributions of work problems support the functions, priorities and values, and purposes of a work domain, given the set of physical resources.

The insights gained from this fifth step lead to requirements for a new team design.

The hierarchical structure of WDA, one of the components of CWA, provides an explicit method for incorporating the high-level management values and objectives and indicating how they map on the lower-level bottom-up processes which characterize the core modernization strategy.

4.1.3.4 *Ecological interface design*

A logical outgrowth of CWA is the design of ecological interfaces. That is, once the full set of behavior-shaping constraints have been mapped out, it is possible to design mediated environments (interfaces) that provide information in a form that minimizes memory and attention load to the operator and that simultaneously supports skill-based, rule-based, and knowledge-based behavior. The resulting interface will achieve this support by providing, respectively, direct manipulation, consistent mapping between work domain constraints and perceptual information in the interface, and an external mental model of the work domain constraints (Bennett and Flach 2011).

While the benefit of applying ecological interface design to the lower-level bottom-up processes described in the modernization strategy is clear, it is our intention to investigate the underlying logic of this approach to the higher-level top-down processes as well.

4.1.4 Resilience Engineering

Resilience Engineering is a field of practice that focuses specifically on safety and risk assessment in organizations, but within the broad CSE framework (Hollnagel et al. 2006). As such, it provides an alternative to the human-as-weakest-link approach seen in traditional models of safety and risk.

Within the resilience engineering framework, accidents are regarded as failures of adaptation to work pressures (reflected in the inevitable conflict between production demands and safe operating constraints) rather than specific component failures to be determined probabilistically. The focus, therefore, is less on system reliability, with its emphasis of lowering failure probability, and more on system resilience, which relates to the capability of adapting to, and recovering from, unexpected variations and degradations of operating conditions.

As mentioned previously, the IAEA HFE and Organizational Factors report explicitly calls out resilience as a necessary characteristic for modern nuclear plants. In addition, there is an active community of practice, to be described in more detail, applying resilience principles to analysis of near-miss incidents.

4.1.5 STAMP/Systems Theoretical Process Analysis

Leveson's STAMP approach could be considered part of resilience engineering, but here it will be considered separately (N. Leveson 2011). STAMP is a systems-theoretically based accident causation model. In STAMP, the emphasis is shifted from preventing failures to enforcing behavioral safety constraints. Safety is viewed as an emergent property of a complex system with multiple degrees of freedom. Safety is determined by sets of constraints which maintain control over the system. Therefore, control rather than reliability is the primary focus. The safety control structure (SCS) of the system maps out the interaction between controllers and controlled processes. The level of safety of a system depends on the extent to which safety constraints allow the system to avoid controlled processes which are hazardous. In this sense, the system can be said to be considered under control.

Within the overall conceptual framework of STAMP is a specific hazard analysis method called Systems Theoretic Process Analysis (STPA). STPA has four fundamental steps:

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

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

STPA is already part of the EPRI recommendations for hazard analysis (see Section 4.2.3 of the EPRI DEG and EPRI 2018b). However, the intention in this report is to apply the methodology more broadly, taking advantage of the fact that the same logical structure is used for human decision and machine action. See Figure 3 for a simplified generic SCS and Figure 4 for a more complex example, indicating control and feedback links involved in both system development and operation for the U.S. commercial air transportation system.

Operating Process

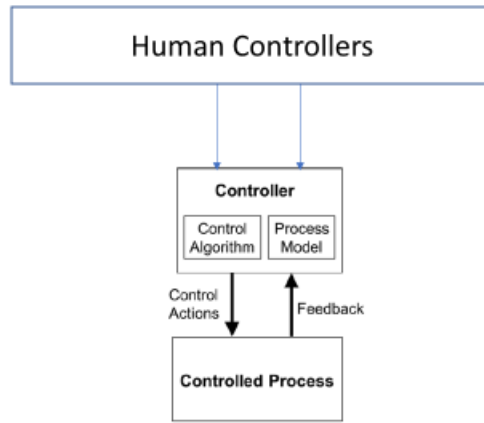


Figure 3. Generic safety control structure (After Levenson 2011).

Example Safety Control Structure

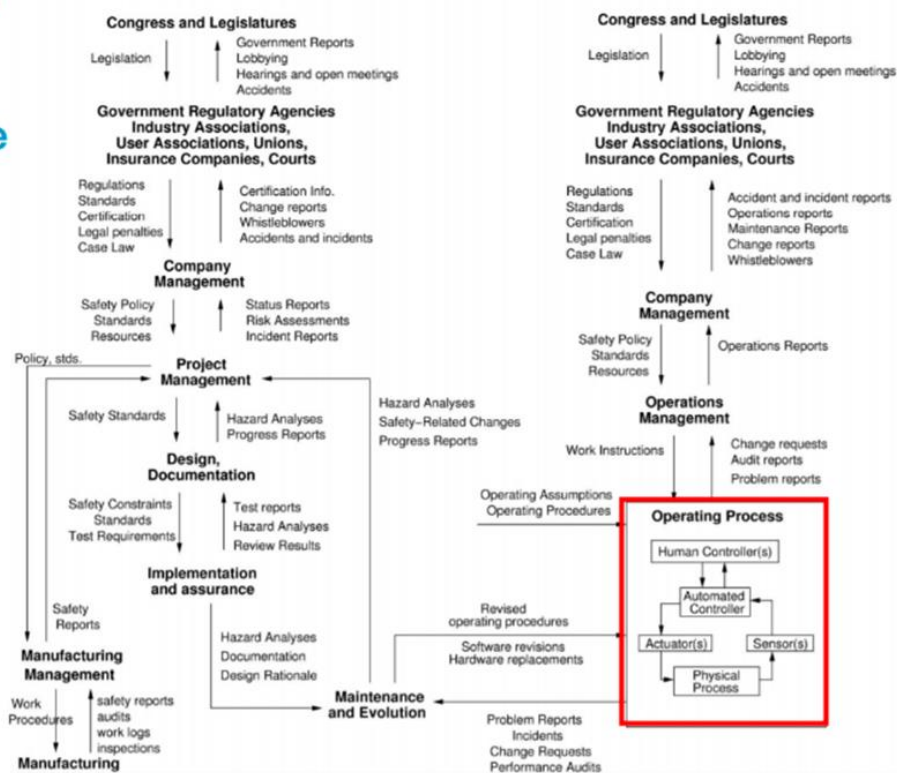


Figure 4. General form of a model of sociotechnical control (Levenson 2011, p 82).

4.1.6 Macro cognition/Naturalistic Decision-Making

Macro cognition is described as the collection of cognitive processes and functions that characterize how people think in natural settings (Crandall et al. 2006). It is derived from the seminal work of Gary Klein on naturalistic decision-making (Klein et al. 1993). 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. The inclusion of this body of work in our review relates to the portfolio of methodologies for knowledge elicitation from experts and stakeholders—a key challenge in complex systems.

4.1.7 Human-Systems Integration

Human systems integration emerged within the context of acquisition of large military/transportation systems and is simultaneously a high-level conceptual model for systems design and a formal U.S. Department of Defense requirement (DOD) (Booher 2003).

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/risk) can be achieved.

The conceptual model for human-systems integration, as described by Booher (2003, Fig. 1.2, p. 7), begins with standard practice for systems engineering and management and then superimposes additional human-centered elements. The inputs to the human systems integration process are standard systems engineering stages for acquisition: systems definition, systems development, and systems deployment. It should be noted that the third component requires focus not just on the design of the systems but on its operation through its life cycle.

The output of the process is a delivered system in which, even without the human systems integration approach, attempts will be made to integrate people, technology and organization. However, such integration will be much less likely to succeed without the two additional components of user focus on all aspects of each of the three stages of acquisition and the combined application of human-related technologies and human systems integration disciplines (Booher 2003, p. 5). The insights from practical application of human systems integration principles in the USS *Zumwalt* project will be brought to bear on solutions developed in Section 5.2.

4.1.8 Safety Culture/Climate

The issue of safety culture, and the parallel but methodologically quite different concept of safety climate, requires its own section in this literature review.

4.1.8.1 Safety Culture

The NRC Safety Culture Policy Statement (76 FR 34773; June 14 2011) includes the following language (NRC 2011), which is further elaborated on in Figure 5:

The Safety Culture Policy Statement includes a list of nine traits further defining a positive safety culture. These traits describe patterns of thinking, feeling, and behaving that emphasize safety, particularly in goal conflict situations, such as when safety goals conflict with production, schedule or cost goals. The traits listed below are not all-inclusive. Some organizations may find that one or more of the traits are particularly relevant to their activities. There may also be traits not included in the Safety Culture Policy Statement that are important in a positive safety culture.

Leadership Safety Values and Actions	Problem Identification and Resolution	Personal Accountability
Leaders demonstrate a commitment to safety in their decisions and behaviors.	Issues potentially impacting safety are promptly identified, fully evaluated, and promptly addressed and corrected commensurate with their significance.	All individuals take personal responsibility for safety.
Work Processes	Continuous Learning	Environment for Raising Concerns
The process of planning and controlling work activities is implemented so that safety is maintained.	Opportunities to learn about ways to ensure safety are sought out and implemented.	A safety conscious work environment is maintained where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment or discrimination.
Effective Safety Communications	Respectful Work Environment	Questioning Attitude
Communications maintain a focus on safety.	Trust and respect permeate the organization.	Individuals avoid complacency and continually challenge existing conditions and activities in order to identify discrepancies that might result in error or inappropriate action.

Figure 5. Traits which define a positive safety culture, according to NRC.

The policy statement also contains the following:

It is the Commission's expectation that all individuals and organizations, performing or overseeing regulated activities involving nuclear materials, should take the necessary steps to promote a positive safety culture by fostering these traits as they apply to their organizational environments.

Clause 5.5.9 of IEEE 1023-2004 states:

Organizations should strive to maintain a culture that values "safety first." Training and appropriate reinforcement for desired (e.g., safety-promoting) behaviors should be considered, obstacles to desired behaviors (e.g., fear of reprisal) should be reduced, and undesirable (e.g., unsafe) behaviors should be prevented or discouraged (IEEE 2004).

The definition of HSIs in the glossary of NUREG 0711 mentions safety culture as follows: "The use of HSIs also can be affected indirectly by other aspects of plant design and operation, such as personnel training, shift schedules, work practices, and management/organizational factors, such as the plant's safety culture." (NRC 2004, pg. 114)

The IAEA report on HFE and Organizational Factors states that: "Safety culture should remain the top priority for all organizations."

A summary of the findings of IAEA workshop on safety culture can be found in Section 3.2.1.

4.1.8.2 The Problematic Status of Safety Culture as a Scientific Concept

A number of safety researchers have, in recent years, expressed concern regarding the scientific status of safety climate. This concern goes beyond a purely academic issue of usage and definition to practical questions of misuse.

The following is an extended quotation from a recent review by (Goncalves, Filho and Waterson 2018)

Following the 1986 Chernobyl nuclear disaster the term ‘safety culture’ started to be regularly used amongst a broad community of safety scientists, psychologists and other groups (Silbey 2009). There are a number of different explanations for the rise in interest in the construct of safety culture including increasing recognition of the importance of cultural aspects of health and safety management (Cooper 2000; Cox and Cheyne 2000; Flin et al. 2000; Reason, 1998) and the shift in the last few decades toward a focus on organisational factors governing risk and safety (Borys et al. 2009; Waterson et al. 2015; Robertson et al. 2016). As a result, many contemporary organisations strive to understand and improve their safety culture in order to deliver effective health and safety management and enhance their safety performance (Antonsen 2009a; Reason, 1998, 2016).

At the same time, amongst researchers and academics, there have been a number of criticisms leveled at the construct of safety culture. Henriqson et al. (2014) for example, argue that the study of safety culture encourages the view that safety is a widely shared norm, value or set of beliefs within organisations which masks important conflicts and disagreements which may exist amongst employees and managers. Others (e.g., Reiman and Rollenhagen 2014; Dekker 2018) suggest that a preoccupation with safety culture has shifted the focus away from more systemic accounts of the causes of accidents and encouraged a rather more superficial account of how safety is related to system levels and other organisational dynamics (e.g., how safety culture changes over time). Finally, Antonsen (2009b) compared qualitative and quantitative descriptions of the safety culture in the same organisation (a Norwegian oil and gas platform) and found them to be dramatically different, leading him to cast doubt on the predictive validity of safety culture assessments.

In particular, it is argued: “the concept of safety culture sometimes tends to be used as an ‘excuse’ for not dealing with some more fundamental safety problems involving technological design.” (Reiman and Rollenhagen 2014)

4.1.8.3 Deepwater Horizon example—Beyond culture

One of our case studies in Appendix A is partially based on a discussion of official reports of the Deepwater Horizon/Macondo accident by two retired nuclear engineers from Sandia and Los Alamos (Boebert and Blossom 2016). The following quotation indicates the need to go beyond safety culture to what the authors call an “engineering culture.”

Promoting a “safety culture” of methodical wariness is insufficient unless that culture is backed up by an “engineering culture” that includes methodical decision-making, contextual review, and management of change. Just as important, a corporation must accept that an engineering culture imposes inefficiency in two ways: directly, because of the time employees must devote to those vital efforts, and indirectly, because ensuring that employees at every level take pains with safety-critical decisions slows down other activities. Macondo teaches that those in an oil company who are responsible for allocating resources might save thousands or even millions of dollars by forgoing such activities but spend multiple billions on the other side of The Edge.

4.1.8.4 Safety climate

The concept of safety climate is closely related to that of safety culture, but it is quite different methodologically. Safety climate is a measure of employees' perceptions of management commitment to safety and, as such, is measurable with instruments such as validated questionnaires (Huang et al. 2017).

As opposed to the concept of safety culture, there is much more professional consensus regarding safety climate, based largely on over 30 years of research and a broad community of practice (Zohar, 1980). Safety climate has been explicitly found to predict objective safety outcomes (such as crashes among truck drivers) and has high diagnostic value in terms of identifying underlying systemic issues such as training, management communications, sufficiency of equipment, etc.

In a sense, safety climate is safety culture, operationally defined. A variety of safety climate scales and tools are currently in use in industry, some of which are specialized to specific industries such as trucking, while others are broader and more generic. Scores on the underlying dimensions of safety climate, readily derived from the analysis process, can provide valuable insight into organizational, cultural, and technical factors underlying safety in complex sociotechnical systems.

4.2 Organizational Change

The following material is a brief overview of the issue of organizational change. A systematic review of the change management literature is beyond the scope of this project. However, existing research indicates a lack of consensus regarding how to conceptualize the problem. The material we present in Sections 4.2.1 and 4.2.2 is based on Dainoff (2009) and will be restricted to the domain of occupational health and safety. However, it is our argument that the findings below can be suggestive of the underlying constraints to be found in approaching change management in NPP modernization.

4.2.1 Organizational Readiness for Change

Within the context of the National Institute of Occupational Safety and Health (NIOSH) National Occupations Research Agenda, Goldenhar et al. 2001 present a model for health and safety interventions. They argue that such interventions need to go beyond concerns about effectiveness and consider development and implementation strategies. In this section, we offer some arguments as to how a sociotechnical framework might help achieve these objectives.

While rarely documented, the history of any safety intervention, whether part of a scientific investigation or simply carried out as a normal business activity, requires some consideration of organizational readiness. If the intervention is part of normal business practice, it will typically require a proposal from someone in the safety organization (perhaps as a part of a consulting relationship) to higher management where it will be accepted, modified, or rejected. We would expect that safety professionals and field consultants typically have, as part of their professional experience, some intuitive knowledge as to whether an organization is ready to implement a given intervention and how to assist the organization in laying the groundwork for implementation.

If the intervention is part of a scientific investigation—typically, proposed by an outside investigator—a different set of management considerations come in to play. In many cases, the organization may regard the proposal as free consulting and be willing to allocate a certain set of resources to conduct what amounts to a pilot project. Despite the requirements laid out by Goldenhar et al. (2001), it is rarely the case that consideration of the possibility of implementation throughout the organization is systematically evaluated at the time of the intervention proposals. Consequently, a systematic evidence-based method of assessing organizational readiness would be a valuable supplement to current experience-based intuitive knowledge.

It is recognized that addressing this question will stretch the boundaries of traditional occupational safety into the arena of organizational design and change management. A preliminary review of the literature indicates lack of agreement about how to conceptualize organizational readiness (M. M.

Robertson and Tubbs 2016). There is, however, some indication that readiness depends on the specific content of the proposed intervention as well as on the surrounding context (see Figure 6). In this case, context is defined as the organization's current functioning or how it works day to day. Content, however, reflects the particular change being targeted.

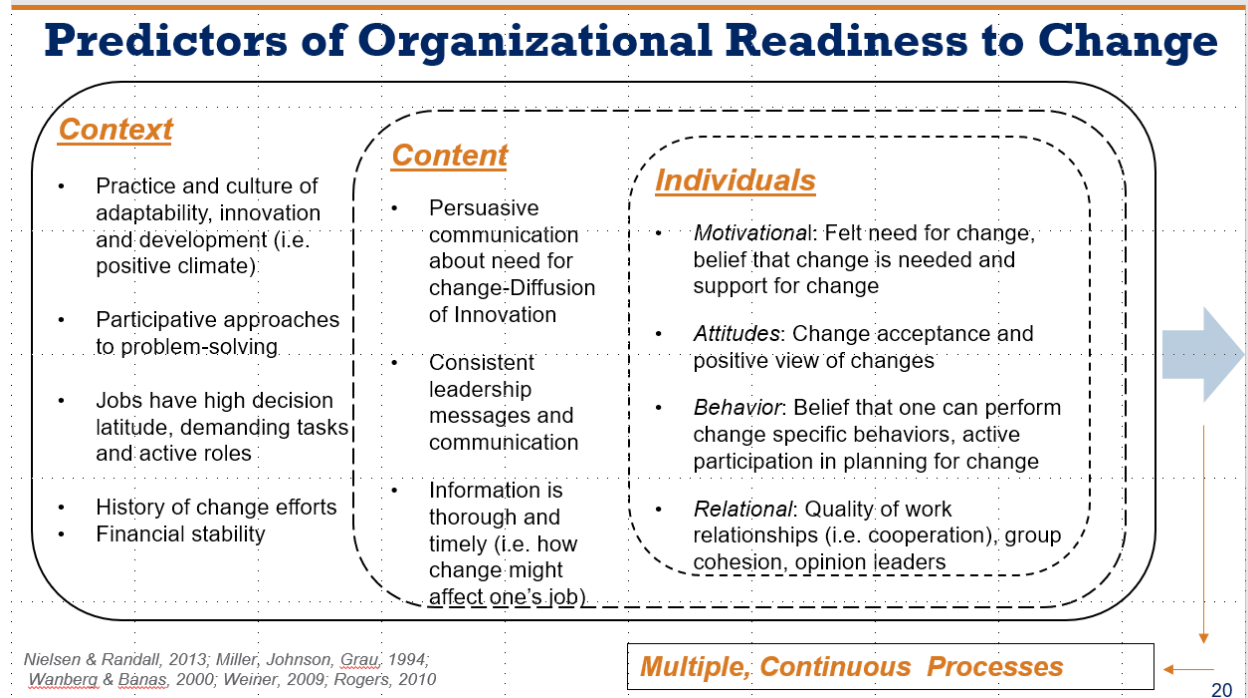


Figure 6. Predictors of Organizational Readiness to Change (Robertson and Tubbs 2016).

While there is little literature on organizational readiness in the specific area of occupational safety, a recent set of studies developed and utilized a psychometric scale assessing the readiness of organizations to allow employees to participate in the design of health and wellness interventions (M. Robertson et al. 2013). The scale included four key constructs (available resources and time, current policies toward participation, current programs in ergonomics, safety, wellness and quality, and ease of team building). The research team employed the scale as an organizational needs assessment tool at four field sites, and the results led to management negotiations prior to intervention, which helped resolve issues of time and resources.

This set of studies is particularly valuable since user/employee participation in design of tools, procedures, and environments is a fundamental principle of human factors/ergonomics, (see Czaja and Nair 2012) (Norman and Draper, 1986). However, allowing the participation of lower-level employees in decision-making has the potential to conflict with long established management practices and prerogatives. This could become particularly problematic when local knowledge, perhaps based on years of experience, conflicts with the expert knowledge of technical professionals. This point of discussion, which could also be framed in terms of shared/conflicting mental models, will be of relevance in considering various approaches in Section 5.

The focus here is on occupational safety and health *interventions*, which imply a specific change in some sort of work-related process or function. In the NPP modernization case, we are likewise looking to change processes/functions –typically via technology. The extent of that change is reflected by the vertical dimension of the Technology Centric Plant Operations Model (Figure 1). The question is: what are the determinants of where a given organization places itself on this dimension? Perhaps the constructs

in Figure 6 can be utilized for organizational self-reflection. In addition, the four factors derived from the psychometric scale of organizational readiness for participative health and safety programs (available resources and time, current policies toward participation, current programs, and ease of team building) could be generalized to the case of modernization of NPP.

4.2.2 Determining the Best Pathway for Implementing Change

As in the previous discussion, the question of effective implementation of safety interventions is one of considerable practical importance. An organization must be ready to implement the intervention, but, unless the conditions leading to sustainability of the intervention are considered, it is much less likely to succeed. Consequently, the pure technical components of a given safety intervention need to be considered with respect to the broader sociotechnical structure and function of the organization.

While there are likely many pathways toward effective implementation, the Intervention Design and Analysis Scorecard (IDEAS) tool (Robertson et al. 2013) (M. M. Robertson and Courtney 2004) is particularly aligned with the high-level goals articulated by (Dul et al. 2012) (Hendrick and Kleiner 2011) in the sense that it provides specific mechanisms for the articulation of a given intervention into the overall mission of the organization.

IDEAS, which is summarized in Figure 7, represents a systematic approach to intervention design. It has been successfully used in a field study (Robertson et al. 2013). It is described in some detail, on the argument that alternative approaches to implementation ought to, at least, include the same basic components.



Figure 7. Intervention Design and Analysis Scorecard (IDEAS) (Robertson et. al 2013).

The intention for IDEAS is to provide a framework for participation in the design by principal stakeholders from the organization and, as such, embed a process to link any resulting intervention to business objectives. Detailed checklists, scorecards and manuals are provided. Two working groups are defined: the Steering Committee and the Design Team. The Steering Committee provides oversight over the process; for it to be effective, it should contain individuals with decision-making authority in the organization. In a fully participative project, the Design Team would involve a combination of technical experts and non-management employees with subject matter expertise. Specific pathways for communication between the two teams are provided throughout the process.

Steps 1 and 2 provide a framework for intervention development. In step 1, under guidance from the Steering Committee, the Design Team identifies problems and contributing factors. In step 2, the Design

Team develops activities and objectives which can be grouped in a set of alternative solutions (potential interventions).

Steps 3–7 reflect the concern with implementation and sustainability. In step 3, selection criteria are developed. These include cost/benefit analyses related to the overall mission of the organization. Each of the proposed alternative interventions are described in terms of the selection criteria in step 4. Step 5 consists of a formal vote in which each alternative is rated in terms of each criterion. Step 6 consists of the logistics and planning of the intervention(s) which resulted from step 5. Step 7 consists of the evaluation of the effectiveness of the intervention.

IDEAS consists of a practical tool, with demonstrated effectiveness, which can enable the implementation of a successful and sustainable intervention. However, it is only a framework. How the various steps are actually accomplished requires a different level of analysis. A pathway to that kind of analysis is provided by (Nielsen and Randall 2013).

Reacting to a lack of clear evidence indicating the effectiveness of occupational health interventions, Nielsen and Randall (2013) argue that a more careful evaluation of the process of creating and implementing an intervention is required. They provide a framework for this evaluation which contains three components: (1) intervention design and implementation, (2) context, and (3) mental models. The first component requires design information related to: (a) initiation of the intervention (who and why), (b) asking whether the intervention activities actually target the appropriate group, and (c) implementation information related to the roles of key stakeholders, degree of participation, support of top and middle managers, and the role and qualification of consultants. Next, the context component is focused on readiness and, as such, addresses many of the same issues raised in the previous section. Finally, the authors are concerned with assessing the extent to which participants targeted by the intervention have shared mental models. The report contains a detailed process checklist in support of their approach.

This section presents a specific framework for implementing change that has been field validated. The framework explicitly provides for the participation of stakeholders across levels of the organization, while ensuring that the proposed changes reflect core values, goals, and objectives of the organization. In particular, this framework provides a mechanism for collaboration across organizational units. In practice, this has allowed for dialogue between professional subject matter experts and key operators, affording an integration between technical expertise and local implicit knowledge.

4.2.3 Illustrative example: Transforming the DOD with Human-Centered Artificial Intelligence

In this section, we present an apparently successful example of change management; one that has the potential for direct impact on NPP modernization, which will almost certainly involve some degree of artificial intelligence (AI). This material is based on a presentation at the 2019 Human Factors and Ergonomic Society meeting by Colonel Stoney Trent, Chief of Missions of the DOD Joint Artificial Intelligence Center (JAIC) (Trent 2019). Here are the salient arguments:

- The DOD has mandated that all DOD AI projects must be coordinated by the JAIC.
- Significant barriers exist to the wide-spread DOD utilization of AI. For example, the military has the largest collection of medical records in the world, but they are inaccessible to AI types of analysis since there is a lack of consistency in diagnostic language.
- Therefore, radical departures from the traditional DOD approach to requirements generation are required.

As shown in Figure 8, requirements development will now start with multidisciplinary teams (including CSE) conducting field studies to develop a portfolio of artifacts, including use cases and user models. These will serve as a basis for generating requirements. Cognitive engineering will be involved at all stages of the process.

From Concept to Transition: Sustaining contact with users and program offices

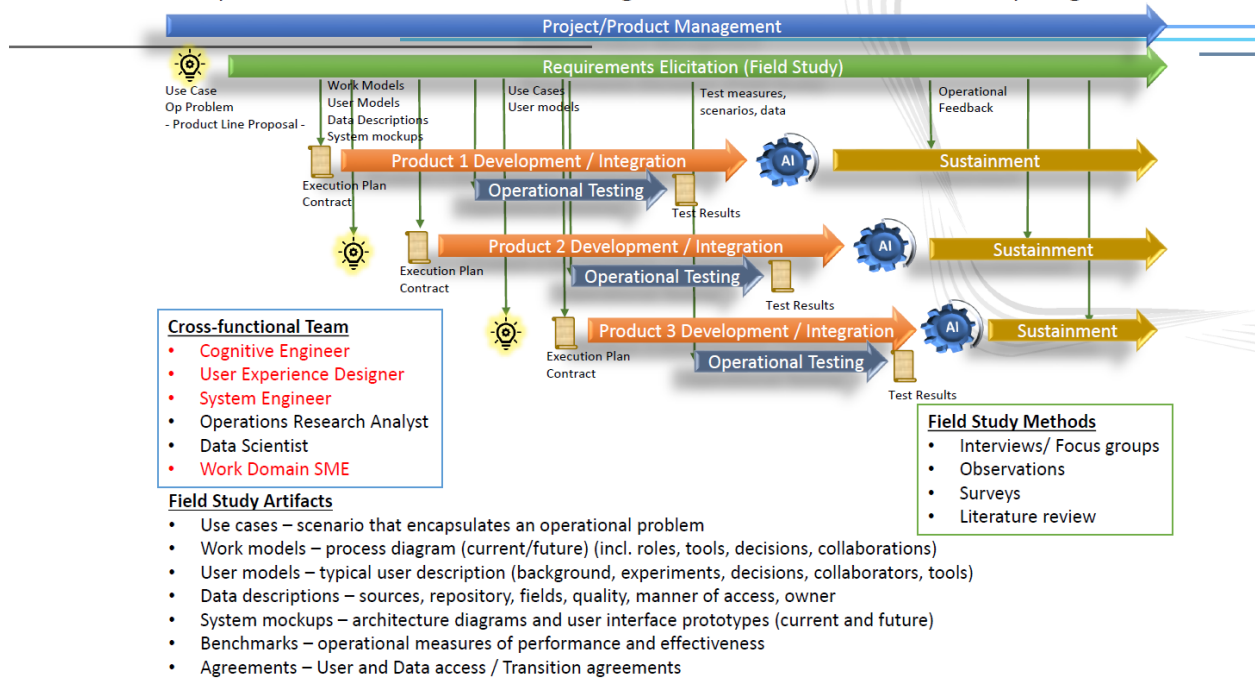


Figure 8. Revised Project/Product Management Model (Trent 2019).

As seen in Figure 9, user-centered AI is seen as a core value in the revised DOD AI project/product management model. Moreover, conceptually, human-centered is identified with resilience engineering. The book “Joint Cognitive Systems” (Hollnagel and Woods 2005) is cited for the quote: “humans are the source of resilience in the system.”

HUMAN-CENTERED = RESILIENT SYSTEMS ENGINEERING

- Terminology and promises of AI are misleading
 - “Learning” vs. Tuning coefficients
 - “Perceiving” vs. Classifying data
 - “Predicting” vs. Calculating probabilities
 - “Paying Attention” vs. Collecting sensor data
- Many AI evangelists are overlooking past failures of “intelligent” systems
 - Poor abstractions of desired logic
 - Poor explanations of rule-based and probabilistic logic
 - Solving for the wrong problem
- Substitution myth
 - Technology never replaces humans
 - Technology always changes the nature of work
 - Good systems are designed to accommodate supervisory control
- AI must be*:
 - Learnable
 - Useable
 - Observable
 - Explainable/
 - Directable
 - Predictable
- Test tools and methods for AI are inadequate or non-existent
 - Need to determine performance envelope for AI implementations
 - Continual monitoring of system in production
 - Must test for human-machine performance



Humans are the source of resilience in systems

* Cf Woods, D., Hollnagel, E. (2006). *Joint Cognitive Systems, Patterns in Cognitive Systems Engineering*. Taylor and Francis

8

Figure 9. Human-Centered AI (Trent 2019).

The assumption, from this presentation, is that DOD possessed the organizational readiness to commit the resources necessary to carry out the extensive field work required as the first stage of this process. However, it is unclear that the goals of user-centered AI could be accomplished without this effort. The same kinds of question can be applied to NPP modernization. A second point is the emphasis on resilience engineering, which we have seen elsewhere in this report.

4.2.4 Change Agents: A Pragmatic Approach

The intention in this final portion of Section 4.2 is to provide some pragmatic advice for change agents based on a combination of methodology and pragmatic experience in the nuclear industry. The previous sections have been consistent in their recommendations of a user-centered focus in approaching management. In Section 4.2.1, members of an organization were more ready to accept change if (a) adequate resources were made available, (b) the organization viewed user participation favorably, (c) similar kinds of change had already taken place, and (d) team building was enabled. All of this would enhance the likelihood of the kind of shared mental models that would be necessary for change to be accepted. In Section 4.2.3, a human-centered approach to AI efforts in DOD is seen as critical for future success.

All of this is consistent with the proposition that human and organizational factors experts, as a member of the systems engineering team, can act as an enabler of change via the mechanisms to be presented in Section 5. Examples of such change management in the nuclear industry are already available in the NFD TQ program case study description in Appendix A, as well as in (Hanes et al. 2015), (Joe et al. 2018)), and (Forbes et al. 2012). The following examples are extracted from these references.

1. **Demonstration.** Demonstrate a new way to do some task or how new equipment will work. For example, demonstrate graphic displays containing integrated display information and touch control to workers who had only worked with analog displays and associated “hard” controls.
2. **NGT.** Establish a group of stakeholders to address a common issue and have them apply an NGT method to develop a consensus, which often will change the views of some stakeholders.
3. **Peer influence.** Identify a member of the group who has accepted and strongly endorsed the desired change and encourage him/her to be a champion of change with his/her peers in the organization that have not accepted the change.
4. **Provide facts and data.** Show the group in which change is desired facts and data that support the desired change. For example, use another similar organization that has increased its productivity X% by implementing the desired change.
5. **Reference and apply regulations.** A government, other agency, or employer may require a change and enforce that requirement through regulatory authority. For example, workers in a part of the facility must always wear respirators, whereas before it was optional. Workers should be notified of the change and the reasons for it.
6. **Make the formal case.** Most workers are inherently rational and will question to what extent change is needed and whether they want to commit personally to making change happen. They will look to the leadership for answers. The statement of a case for change and the creation of a clear vision statement are needed to effect change.
7. **Create ownership.** Ownership of change requires more than mere buy-in or passive agreement that the change is acceptable. Ownership is often best created by involving people in identifying problems and creating solutions. It is reinforced by incentives and rewards. These can be tangible or psychological.
8. **Communicate the change message.** Too often, a change agent may believe that members of the organization understand the issues, feel the need to change, and see the new direction as clearly as

the change agent. The best change programs reinforce core messages through regular, timely advice that is both clear and practicable. Communications are targeted to provide workers with the right information at the right time and to solicit their input and feedback.

5. Conceptual and Methodological Framework

5.1 Introduction: The Translation Problem

The purpose of this section is to convert the various sources of knowledge and expertise contained in Review of Literature on Human and Organizational Factors into usable methods which can provide solutions to specific problems associated with the modernization strategy discussed in Introduction. As such, this can be described as a translation problem. Translation issues are well-known in the health and safety arena. For example, the NIOSH has a Translation Research Program; the purpose of which is to: “... *more effectively transform science into useful actions and products*” (<https://www.cdc.gov/niosh/topics/translationresearch/default.html>). The translation issue, central to the approach described herein, is discussed in greater detail in Appendix B.

5.2 Selecting Solutions with Field Based Utility

One of the challenges being faced is the results from the sociotechnical constraints of the research enterprise. Even in the field of HFE, those methodologies available come, with some exceptions, from reports published in scientific journals. As such, the criteria for acceptance in these journals tend to stress novelty and methodological rigor, at the expense of demonstrated field utility. As discussed previously, the motivation for choosing content for this report is based on the capability for such field utility, including the presence of a community of practice. The experience of selecting specific human systems integration related methods from the USS *Zumwalt* project reflects exactly this kind of practicality. Also, the modernization efforts performed at Progress Energy and Duke Energy nuclear facilities involved the application of HFE methods, including some described in this report (Joe et al. 2018).

To establish some context, we will next present three examples in which academically based methods were translated to workplace-relevant applications. All three involved the establishment of communities of practice. Each of these examples will be further considered a potential methodological solution.

5.2.1 Cognitive Work Analysis

CWA (Rasmussen, et al. 1994; Vicente, 1999) now embodies a large and well-documented community of practice, as reflected by several practice-related publications (Burns and Hajdukiewicz 2004) (Bisantz and Burns 2009) (Jenkins et al. 2008) (Lintern 2009) but especially by the work of (Naikar 2009) (Naikar 2013). She has presented a set of criteria for assessing both the *usefulness* and *feasibility* of applying CWA methods. Usefulness can be assessed in terms of two subcategories: *impact* and *uniqueness*. Impact reflects the extent to which the method influenced practice, whereas uniqueness reflects the extent to which a unique contribution relative to standard techniques commonly in use. Feasibility is assessed relative to the capability of the method to be accomplished within existing project resources (schedule, staff, and financial budget). *These criteria should be considered as aspirational for the recommended methodologies presented later in this report.* The following descriptions of communities of practice each reflect successful meeting of these criteria.

5.2.2 Safety Climate

In 2008, the Liberty Mutual Research Institute of Safety began a major effort to establish a research program in safety climate. Initially developed by Prof. Dov Zohar at Technion University in Israel, researchers at Liberty were the beneficiaries of 30 years of research in the area (Zohar, 1980). They were

fortunate to be able to directly collaborate with Prof. Zohar and were successful in creating new instruments for assessing safety climate in lone workers (long haul truck drivers and utility workers).

However, Liberty Mutual also had a parallel organization named Risk Control Services (RCS). This organization consisted of a large group of customer-facing safety consultants who had, as part of their mission, translated the Institute's research findings into practice. RCS showed interest in safety climate as a customer service product. Accordingly, a collaborative team of researchers and risk control field operatives worked to convert the Institute's scientific findings into a practical customer-facing tool. In effect, we worked to create a community of practice within the RCS organization. The Institute's results were highly successful; safety climate scales were administered to over 37,000 employees at over 50 companies (Huang, Jeffries, Tolbert, and Dainoff 2017).

The collaboration did not end there. The RCS community utilized the results of the scale administration as a consulting opportunity for diagnostic follow-up conducted jointly by RCS field agents and company safety officers. The researchers at Liberty developed a project to track the progress of these adaptive interventions (Lee et al. 2019).

In 2015, Emily Huang was given a major award by the President of Liberty Mutual for her efforts in this translation activity. In 2016, top management at Liberty closed the Institute. However, the follow-up analysis of the adaptive intervention is still being continued, independent of Liberty Mutual.

5.2.3 STAMP Mental Model Extension

STAMP includes a group of system analytic tools originally developed by Nancy Leveson at MIT. The original STAMP model was a university-based research project developed by Prof. Leveson and her students. This program was documented in a book, *Engineering a Safer World* (Leveson 2011). However, Professor Leveson made the decision to offer a free online version of her book to the general public. In addition, in 2012, she initiated a series of yearly workshops at MIT. These steps resulted in a large and growing international community of practice with several subgroups.

In 2012, the Liberty Mutual Research Institute began a collaborative relationship with Prof. Leveson. One early outcome of that collaboration was a joint Liberty-MIT project with the Boeing Corporation. Larry Hettinger was the project lead for Liberty. STPA was initially applied to the lock out-tag-out issue at one of the aircraft assembly sites. This effort was later expanded by Boeing to four additional successful projects. At the 2019 STAMP workshop, a senior Boeing Director reported that his initial operating assumption going into the STAMP implementation was that *safety should not be compromised by production pressures*. However, he said they came to learn that a more accurate statement is *a focus on safety will result in enhanced quality*. (It is of some interest that this conference was held only two weeks after the second Boeing 737 MAX crash).

As a result of the engagement of these communities of practice, STAMP methodologies are continuously developing. The original hazard analysis method was named STPA and is currently being used in EPRI's Hazards and Consequences Analysis for Digital Systems (EPRI 2018b). Other models dealing with accident analysis, cybernetic incidents, and a framework for the coordination of multiple decision components have been developed. However, of particular interest to this discussion is an extension to STPA which includes a framework mental models (France 2017).

As discussed previously, the advantage of STAMP is that human and machine control actions are included within the same framework. The machine control component displayed in Figure 3 might just as well refer to a human controller. The process model for a machine would be some sort of control logic or algorithm. In humans, the corresponding term is mental model. France and her colleagues decided that the mental model aspect of the human controller needed to be further elaborated. There was a plethora of conceptual models available in the published literature, but these were rejected as being too complicated and not easily fitting into the control logic of STPA.

It should be emphasized that the STPA mental model was developed within the context of a subgroup of automotive engineers who were part of the STAMP community of practice. In fact, at a recent STAMP annual conference, a demonstration of its use in the development of the dashboard of a new vehicle was present. The author, a senior development engineer, indicated that this was the first time in his experience where there was effective communication between design engineers and human factors experts. Consequently, the automotive community of practice is currently working to embed STPA within Society of Automotive Engineers (SAE) standard J3187 (SAE 2019).

5.2.4 Resilience Engineering: Learning from Incidents

The resilience engineering movement had its origins in the (National Aviation and Space Administration) NASA *Columbia* shuttle disaster. Leading researchers (e.g., Woods, Levenson) were involved in post-accident analysis and received a commitment from NASA that the next shuttle program would be resilience-based. However, this effort was sidetracked by the Bush Administration's emphasis on a Mars program. The result was the emergence of the resilience movement. The resilience movement is a rather loose, informal collection of researchers linked by common principles and an organization—the Resilience Engineering Association. Hollnagel's book on Safety II (Hollnagel 2014) created an alternative label for the resilience movement. For the purpose of this report, however, the focus should be on a small community of practice within the resilience movement we call, for convenience, the Learning from Incidents group. This is an active group of practitioners, not academics, who are applying the resilience principles to the area of software engineering. The core of their approach, which has obvious application to NPP modernization, is the need to pay close attention to the analysis of near miss incidents. They examine the cognitive work (aka mental models) employed by operators dealing with the incident and, in particular, ask what kept the problem from getting worse. This effort is within the resilience tradition of asking what went right, rather than what went wrong. As the contributors to this movement are not academics, their efforts tend to be documented in webinars and blogs. (<https://www.infoq.com/presentations/resilience-thinking-paradigm/>; <https://www.learningfromincidents.io/blog/learning-from-incidents-in-software>)

5.3 Methodological Integration

5.3.1 Conceptual Overview

The discussion in Section 3.1 reflects the reality that the various methods and approaches reviewed in Section 2 are not independent isolated elements, but reflect a dynamic interaction among multiple researchers and associated communities of practice. The perspective to be taken in this report is, as discussed previously, pragmatic, with a basis in field utility—definable by the criteria of usefulness and feasibility (Naikar 2009).

However, this pragmatic approach has a firm basis in theory. Mitchell presents a non-technical description of an approach to using genetic algorithms to solve software problems in which successively improved solutions were attained by combining elements of previous solutions (Mitchell 2009, Mitchell 2019). Section 5.4.1.1 describes how a genetic algorithm approach to user interface design (McGrew 2016) was utilized by the Board of Certification in Professional Ergonomics (BCPE) to modernize their fundamental conceptual model, the Ergonomist Formation Model (EFM). This is presented not only as an example of a particular recommended methodology, but as a general principle; namely, that combining components of existing successful methodologies might yield a more successful outcome.

5.3.2 Basic Unit of Analysis: Capability Development and the Work System

In Section 2.1, a central issue for NPP modernization is the problem of capability development (Thomas 2019). As seen in Figure 2, capability is the synthesis of the PTPG dimensions. The Macroergonomic concept of the work system (see Section 4.1.2) can be useful in providing a theoretical

framework for capability development. As seen in Figure 10, the four dimensions of capability development can be mapped onto the three components of the work system:

People → Personnel Subsystem

Technology and Process → Technological Subsystem

Governance → Organization and Management Subsystem.

For completeness, both internal and external environments are considered. Internal environments are the physical and psychosocial context within the work system, and external environments are physical and psychosocial contexts external to the work system. For example, in the Fukushima Daiichi accident, the risk of a tsunami was a physical context external to the work system.

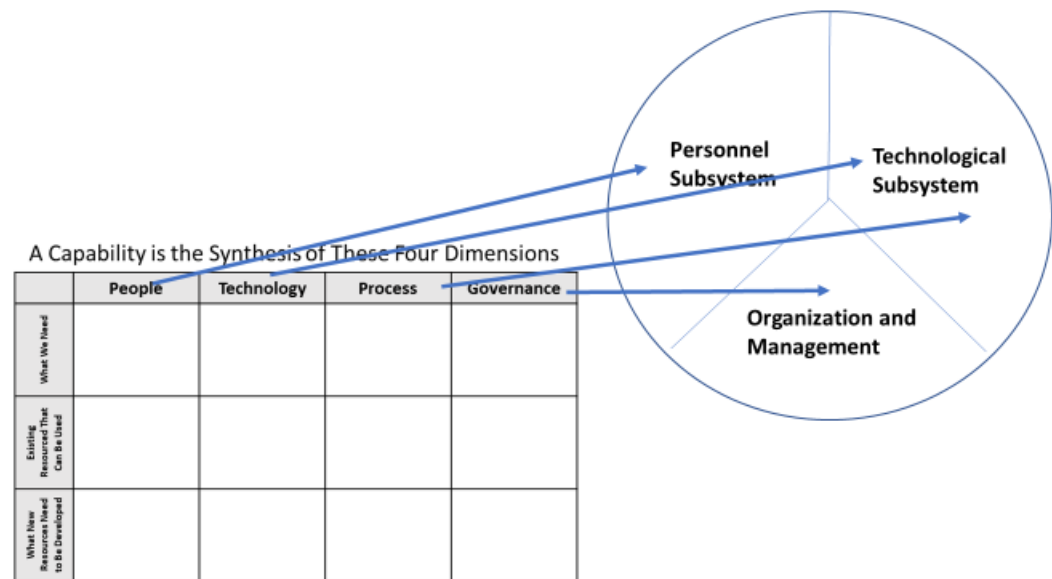


Figure 10. Mapping capability development components PTPG onto Macroergonomic work system (Thomas 2019, Hendrick and Kleiner 2001)

Central to the definition of work system is the concept of *joint optimization* (Hendrick and Kleiner 2001, pp. 24–25). To achieve maximum effectiveness, it is necessary to avoid maximizing any single subsystem at the expense of the others. Consequently, the practical goals of integrating the PTPG dimensions of capability development can be restated in terms of the Macroergonomic concept of joint optimization of work system components. However, the practical *solutions* of how this is to be accomplished have yet to be defined. This is the purpose of this report.

A conceptual parallel concept from resilience engineering is that of *joint cognitive systems (JCS)*. A JCS is a combination of human problem solvers and technology acting in a coordinated fashion to achieve some common goal (Hollnagel and Woods 2005). In fact, the resilience engineering approach to definition of system performance is framed as a balance among three interdependent components: effectiveness, efficiency, and safety (Hollnagel 2006).

In this report, the basic unit of analysis will be considered the work system. Joint optimization will be considered the goal. Resilience engineering concepts will be one of several potential approaches to achieve joint optimization.

5.3.3 Fundamental Problems in Achieving Joint Optimization

In Section 1.1, we stated that the overall goal of this report is the development of a strategic framework for effective integration of human and organizational expertise within NPP digital modernization efforts. This goal can be refined in terms of using methods for such integration in service of joint optimization of work systems within NPPs. To further refine this goal, the following three problems are identified as fundamental in applying human and organizational expertise in achieving joint optimization.

1. **The Knowledge Representation Problem:** How information about the work system is presented to those who need to operate on it. One view is that task analysis, which defines operator actions, identifies the information requirements that must be provided by HSIs. There are HFE guidelines on layout of the displays and controls. HSI designers prepare conceptual controls and display designs and users (operators and others) review and critique iteratively until the HSI design is accepted. Tests and evaluations are performed during the HSI design process, and after final design is completed, an Integrated System Validation is performed to determine if the design is acceptable. The results of the task analysis are also used to provide information for revising existing or preparing new procedures and training.
2. **The Knowledge Elicitation Problem:** How represented information is obtained from those who have the required expertise. In many cases, the end users of technology do not have experience with new technologies. Digital and systems engineers, representatives from vendors supplying the digital equipment, the system requirements documents, etc., are sources for this kind of information.
3. **The Cross-Functional Integration Problem:** How information will be enabled to flow freely between groups, and help support collaboration and prevent silos. The formation of groups involving all stakeholders affected by the issue and application of various problem-solving methods were applied at Progress Energy, Duke Energy (Forbes et al. 2012; Joe et al. 2018) and the Westinghouse Commercial NFD case study (Appendix A).

These three problems are separated for analytic purposes, but they are clearly interrelated. The following sections will identify examples of methodological approaches to solving each of these problems. In a subsequent section, these approaches will be utilized, among others, to present a matrix of specific NPP modernization problems and proposed solutions.

5.3.4 Knowledge Representation

Knowledge representation is critical for any problem-solving activity; it is well-known that the way in which a problem is represented influences the cognitive work needed to solve the problem (Norman 1988, Flach and Verhoorst 2020). Moreover, given the complexity inherent in the problem of NPP modernization, alternative forms of representation would add valuable redundancy. Hence, alternates are presented below.

In general, in the application of knowledge representation to the analysis of work, there are three approaches (Vicente, 1999):

1. Normative: how things **should** be done
2. Descriptive: how things **actually** are done
3. Formative: how things **might** be done.

The analyst will need to decide which approach is to be utilized. The approach taken in this report will largely be formative.

5.3.4.1 Knowledge Mapping

It is important to emphasize that the body of literature described in Section 2 is not static but represents conceptual and methodological developments over a number of years. Moreover, these developments are not independent of one another. For example:

CWA is useful for the design and testing of effective JCS only when understood within the larger context of a CSE approach that integrates that analysis with a representational approach to interface design. (Elm et al. 2009)

Elm et al. (2009) go on to propose the use of (Woods 1991) knowledge-mapping principle as a contextual framework to characterize the JCS, within which results from CWA are integrated into the overall systems engineering process. Their process, which will be described below and is taken from their chapter, is aimed at the production of a Decision Support System (DSS) with an associated HSI. However, it should be emphasized that the knowledge-mapping principle can be generalized beyond this specific goal. For example, the Technology Centric Plant Operations Model (Figure 1) discussed in Section 1.1 is a case of knowledge mapping. Communication of additional details of specific concepts of operations would benefit from application of these principles.

The starting point is the JCS, which as stated above, can also be conceptualized as a work system or collection of work systems. According to Elm et al. (2009), the system designer needs to understand:

- The goals of the JCS
- The relevant cognitive work that needs to be accomplished
- The information needed to accomplish that behavior
- The larger functional context within which work is completed.

From this understanding, some sort of user interface (which could be a document rather than a computer display) is created. This user interface reflects the expertise of the system designer in a way that allows the user to construct an accurate and efficient mental model of the system. The mapping principles are illustrated in Figure 11. It should be noted that this representation could be applied to any of the three approaches to analysis: normative, descriptive, or formative.

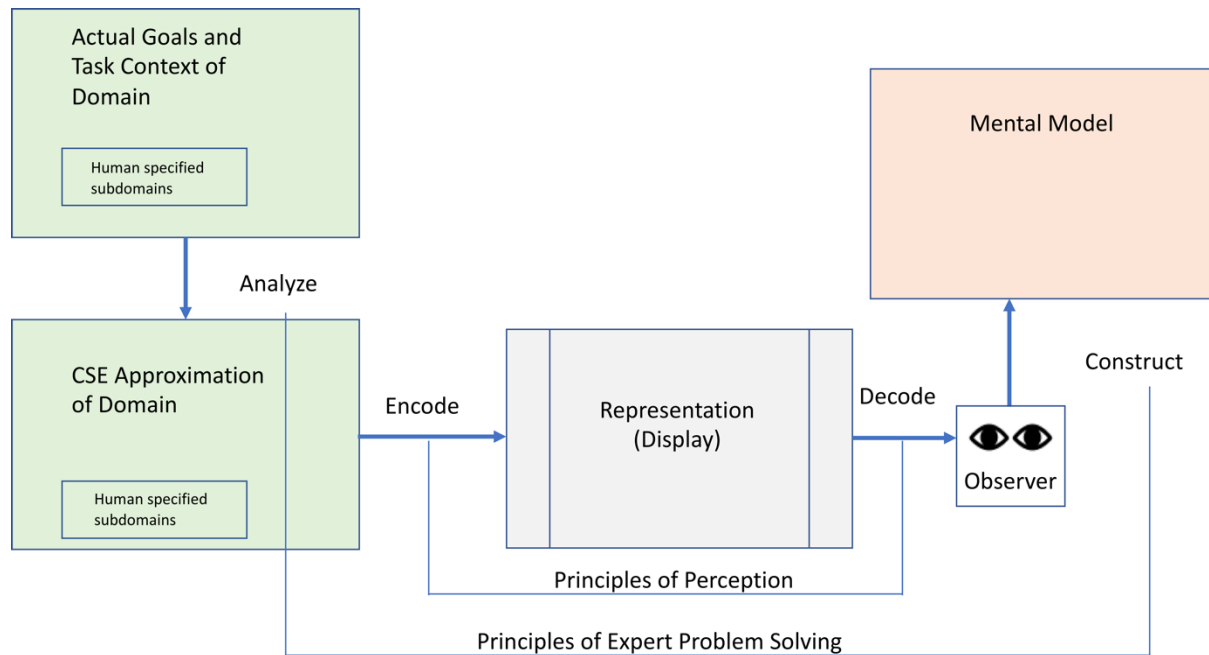


Figure 11. The Mapping Principle (Adapted from Elm et al. 2009; Original in Woods, 1991).

At the far left is represented the actual work domain to be characterized. This consists of actual goals and task content, with human imposed subdomains, reflecting the human participation within JCS/work system. The cognitive system engineer performs analyses on this material and generates an approximation of the work domain and subdomains. This would typically be the output of WDA within the context of CWA. The next step is encoding. This is the process of converting salient aspects of the work domain into a user representation/interface which is consistent with the mental model of an expert user. This allows the actual user to effectively decode the information in the representation use it to construct his or her mental model. The user can then, in turn, act on the work domain to perform desired activities to achieve the goals of JCS/work system.

The relationships between the inner processes *encode* and *decode* involve principles of perception. That is, the design decisions used in constructing the HSI reflect organizing those elements of information in the work domain characterizing the knowledge of an expert user into a form which, taking advantage of known principles of human perception and attention, allow the general user to construct an accurate mental model. This process is sometimes called *ecological interface design* (Bennett and Flach 2011).

The relationships between the outer processes *analyze* and *construct* involve principles of expert problem solving. Within the typical domains of cognitive engineering, CWA, or similar methods, would be used to create a DSS. However, there are invariant principles in the mapping strategy described herein which can be generalizable beyond a formal DSS.

The above approach has been expanded by EPRI's Decision-Centered Guidelines for the Design of HSI (2012) to be applied specifically to the problem of NPP modernization (EPRI technical report 10890926). They argue that digitalization of NPP processes generate HSIs in which higher levels of cognitive processing are required. Accordingly, a new approach to support decision-making beyond traditional HFE guidelines is necessary. The authors present a set of decision support guidelines. The following decision support requirements form the basis for these guidelines (see Section 3 of EPRI technical report 10890926):

1. Determining decision-making and information needs
2. Making processes observable

3. Controlling actions to achieve goals
4. Focusing attention
5. Making systems failure-tolerant
6. Teaming with automation.

In addition, the following background information related to procedures, which may be considered a DSS that facilitates knowledge mapping, is provided:

Current nuclear plant operators follow procedures. Current control panels were designed and built with analog technology requires extensive training of operators in order for them to develop robust and accurate maintenance mental models of the plant's state. Most analog indicators present one or a very few data points. Typically, an operator must obtain information from multiple displays and mentally integrate this information to develop a mental model of plant state. It is useful to understand plant state when diagnosing a plant problem. Because of this difficulty with emergency and abnormal problems, symptom-based procedures are in use. Event-based procedures have been used in the past that encourage operators to identify the event causing the problem, then apply event-based procedures to address the problem. Today the operator follows symptom-based procedures. The operator identifies symptoms that something is not correct from displays and then selects the procedure to handle the symptoms. If the operator encounters a problem he/she cannot handle, the last resort is to apply a procedure that shuts down the reactor completely. The use of graphical displays and trending information better supports the development of mental models (as used in military and commercial aircraft). An accurate mental model can help an operator more quickly identify a developing problem and possibly take corrective actions to prevent the problem from developing, or actions to minimize the impact of the problem.

Each owners group provides standard guidance for the use of emergency and abnormal operating procedures. INPO provides guidance for other types of procedures (INPO 2009). Procedures are classified as continuous use, reference use, information use, or multiple use. As per the Nuclear Energy Institute (NEI) document AP-907-005, Procedure Writers Manual, the cover page (or first page) of the procedure designates the level of use. For procedures designated as multiple use, a specific level of use designation is provided on the first page of each section (PPA 2011)

5.3.4.2 *Extension of Knowledge Mapping to Software Systems*

A recent extension of Woods' knowledge-mapping concept to software incident response is presented by (Cook 2019). He argues that keeping a web-based enterprise up and running requires constant attention and monitoring—similar to an intensive care unit. Figure 12 depicts such a system in which the horizontal line of representation identifies the location of display units and the input devices used to interact with them.

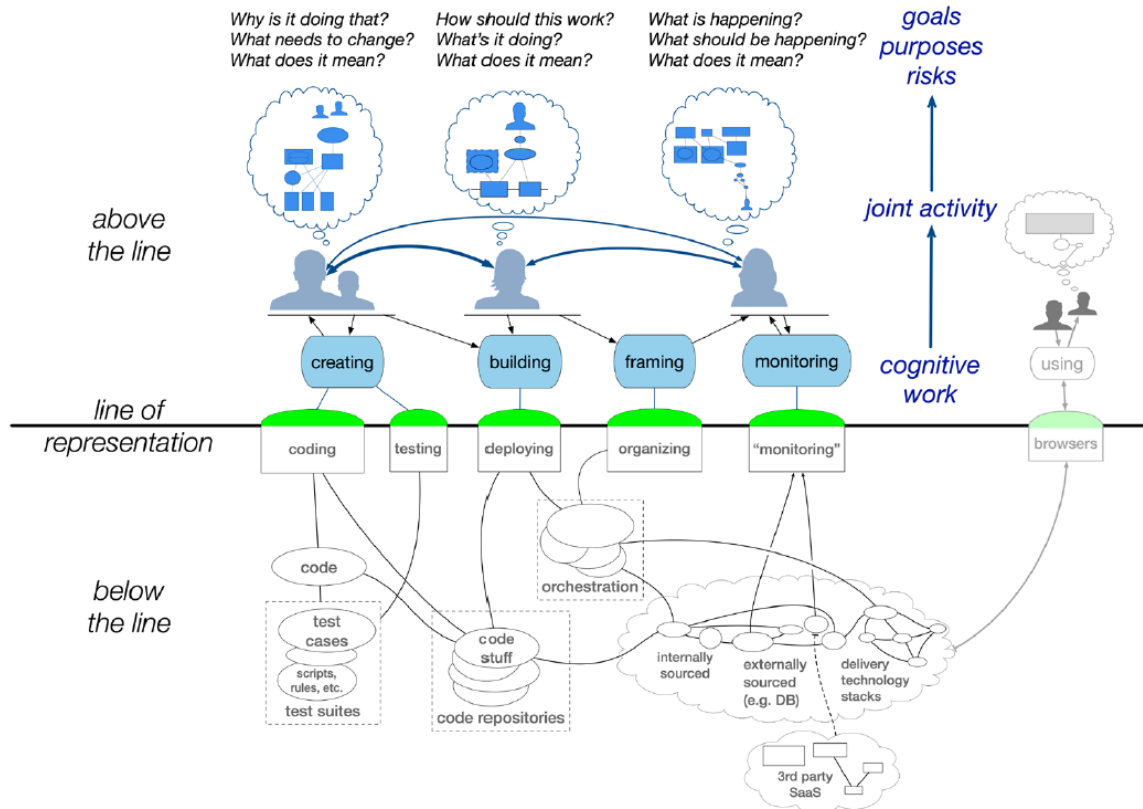


Figure 12. Above and below the line of representation (Cook 2019). Copyright 2016–18 by R.I. Cook for ACL, all rights reserved.

Below the line are the technical components/artifacts of the system. In terms of Woods' knowledge representation, this would be the work domain. Above the line are the people, organization, and processes that maintain the system. On the far right is depicted the end user of the system, whereas the team members coordinating the response to system incidents are located across the rest of the diagram. Note that team members have individual mental models of the system, but they must also be engaged in coordinated action. Current complex web-based enterprises may be continually in flux; therefore, these mental models must be frequently updated. It is emphasized that all of the cognitive activity that occurs above the line is derived from the representation on the line. That is, individual actors do not have direct access to the components below the line but must interact through displays and input/output devices.

This form of knowledge representation, clearly derived from Woods' knowledge-mapping concept discussed above, is current being actively used in the software community as a framework for incident analysis and may be useful for understanding digital control rooms in NPP.

5.3.4.3 Simplified Example STAMP/STPA

To illustrate the use of SCSs as the STAMP/STPA approach to knowledge representation, a relatively simple but real-world example is presented. This example is transformed into generic form from a case presented in (J.M. Flach et al. 2015). The problem is that of managing slips, trips, and falls in a generic commercial processing facility. While there is obviously a large gap between the complexity of this generic example and NPP, this example is of a ubiquitous maintenance activity and there are some important advantages to its use as an illustrative example.

The work processes in this facility generate grease which presents a safety hazard for falls. The problem is to control the grease by efficient floor cleaning. First, this is an important and expensive problem. According to the Liberty Mutual Workplace Safety Index (Liberty Mutual 2016) slips, trips, and falls resulted in direct worker compensation costs to U.S. industry of over \$17 billion. Indirect costs were several times higher, depending on circumstances.

Second, this example documents the failure of a purely technical solution to a sociotechnical problem. As such, it illustrates the utility of STPA in the knowledge representation of organizationally based issues, in addition to its current NPP application to mechanical problems. That is, STPA use can be used to understand an array of situations in NPPs where the knowledge representation, or mental model of the operator, is suboptimal for the state that the plant is in. Some investigations of minor incidents at nuclear facilities have identified that the actions the operator took made sense to that person at the time, but turn out to be less than ideal for the actual conditions or plant state.

Third, the simplicity of the example is an advantage in improved knowledge representation; however, at the same time there are elements in this problem which can generalize direct to NPP situations.

Fourth, the example is utilized not only in this section, but in Sections 5.3.4.4 and 5.3.4.5.

It has been clearly established (e.g., Verma et al. 2011) that a clear relationship exists between likelihood of falling and slipperiness of certain work areas, measured by coefficient of friction. Consequently, in this example, top management required the use of high-performance enzyme-based floor cleaners as a technical solution to managing grease spills and thereby reducing slipping hazards. In the preparation of such cleaners, cold water must be used. However, in practice, it appeared that at a majority (62%) of sites observed, employees actually used hot water. This defeated the purpose and actually made the floors more slippery. Thus, a *technical* solution was defeated by a *social* (organizational) failure of supervision/training. STAMP/STPA will be used to elucidate this problem.

An overview of STAMP as a general model of accident causality based on system theory is contained in Section 4.1.5. STPA is a specific proactive analysis methodology within the STAMP framework. STPA is also a four-step process (N. G. Leveson and Thomas 2018)

1. Define the purpose of the analysis: What are losses within the defined system? What are hazards which might cause such losses? What are safety constraints which address the hazards?
2. Model the SCS: A hierarchy of control and feedback links between controllers and controlled processes.
3. Identify unsafe control actions.
4. Identify loss scenarios.

For the purposes of this report, constructing the SCS will serve as a form of knowledge representation. This analytic framework is called the SCS and represents a series of interactions between controllers and controlled processes.

Figure 13 and Figure 14 represent the application of an SCS analysis to the floor cleaning example. This particular analysis represents a variant of typical STPA presentations in that two versions of the SCS are depicted: work as envisioned and work as actually performed. Thus, both normative and descriptive models are utilized. However, it is important to emphasize that STPA is meant to be proactive; therefore, it could be utilized in a formative mode.

Figure 13 depicts the control and feedback relationships as envisioned by the system designers. This simple example reflects the fact that very often the operational safety constraints in the system represent tight couplings between the social (personnel) and technical components of the work system.

These components could be considered to have been extracted from a more complicated SCS, similar to that depicted in Figure 4 in Section 4.1.5. This might involve control and feedback relationships related to higher management at the franchise holder level as well those from the Federal Government (e.g., Occupational Health and Safety Administration) and worker compensation insurance carriers. These relationships constitute constraints on the system which result in a management directive to utilize enzymatic floor cleaner (EFC) to improve the safety by increasing the coefficient of friction on the floors of work areas.

Figure 13 depicts the control relationship between a supervisor and the employee who is assigned to clean the floor. The input to the supervisor, in his/her role of controller, is management input to utilize EFC. This input contacts a process model (supervisor mental model) which contains the information that the agent must be mixed with cold water, as well as the supervisor's knowledge that informational posters conveying this information are posted in the workplace. The supervisor/controller transmits a control command to the floor cleaning employee as controller.

Insofar as Figure 13 represents work as envisioned, the floor cleaning employee process model is identical to that of the supervisor. The controller sends a control signal to the actuator which, in this case, represents the mixture of cold water with an EFC agent. The controlled process represents the actions of the enzymes in dissolving grease efficiently. (This diagram does not include the additional control links involved in actually mopping the floor. These are not relevant to the problem and can be safely excluded from the analysis.) Finally, the sensor represents the visual appearance of the floor to the human controller.

Figure 14 shows the actual control structure, which reflects the reality that 62% of persons cleaning the floors with EFC used hot water. That is, the controller component identifies a failed safety constraint in the sense that an inappropriate control algorithm was used (hot vs. cold water). Moreover, the sensor component was inadequate (i.e., floor looks mopped despite use of hot water). In the language of STPA, an unsafe control action has been identified. In the language of cognitive psychology, the person cleaning the floor had an inappropriate mental model for this particular situation. However, for most floor cleaning situations, in which typical cleaning agents were employed, the mental model to use hot water would have been correct. Figure 14 also reflects, in a simplified form, the hierarchical nature of the problem in that the supervisor, by failing to ensure correct usage of the technology, can be identified as a controller with an incorrect algorithm/inadequate mental model. In one sense, the concept of safety constraints represents a pragmatic approach to joint optimization insofar as both social and technical safety constraints are considered within the same analytic framework.

Work as Envisioned

Representation of control structure for floor cleaning to avoid slips, trips, and falls.

Upper management requires Enzymatic Floor Cleaner (EFC) for more efficient cleaning effect increasing coefficient of friction (COF) but requires cold water

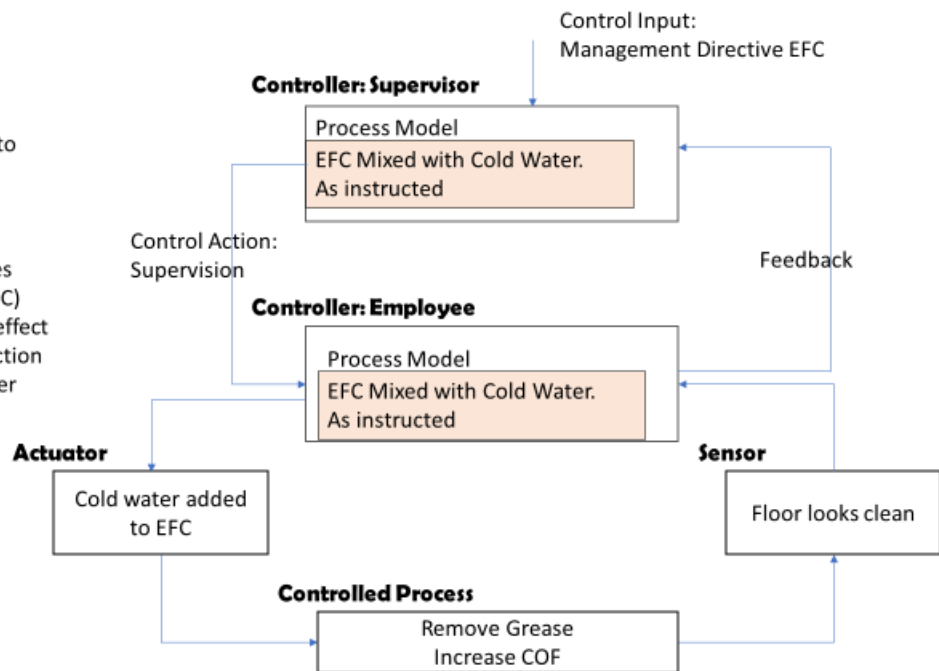


Figure 13. SCS of generic maintenance process example: Work as envisioned. Modified from Levenson (2011).

Work as Practiced

Supervisor Conflicting Mental

Model: Assume training (posters) adequate; direct supervision not necessary.

Employee Conflicting Mental

Model: Population stereotype "use warm water to clean" overrides minimal training.

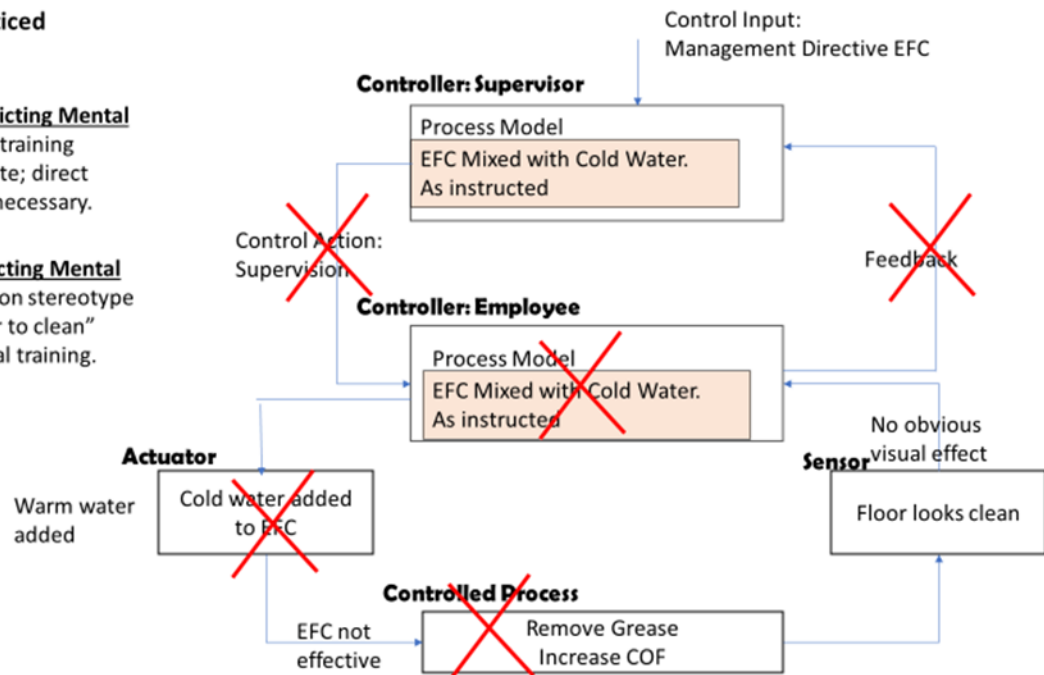


Figure 14. SCS of generic maintenance process example: Work as practiced. Modified from Levenson (2011).

Figure 15 represents a more general example of a SCS depicting control (downward) and feedback (upward) linkages to illustrate organizational decision-making processes related to safety. In the generic commercial processing facility example, high-level corporate policy resulted in decisions to employ EFC which, while more effective, was also more expensive. However, appropriate resources for training and supervision were apparently not provided, and feedback regarding lack of proper use was also missing. Therefore, SCSs represent organizational safety constraints in the form of policies, procedures, and processes/mechanisms to guard against hazards. The extent to which such structures contain inadequate control algorithms, missing links, or other deficiencies provides an indication of the overall level of safety in the system, as well as a measure of joint optimization.

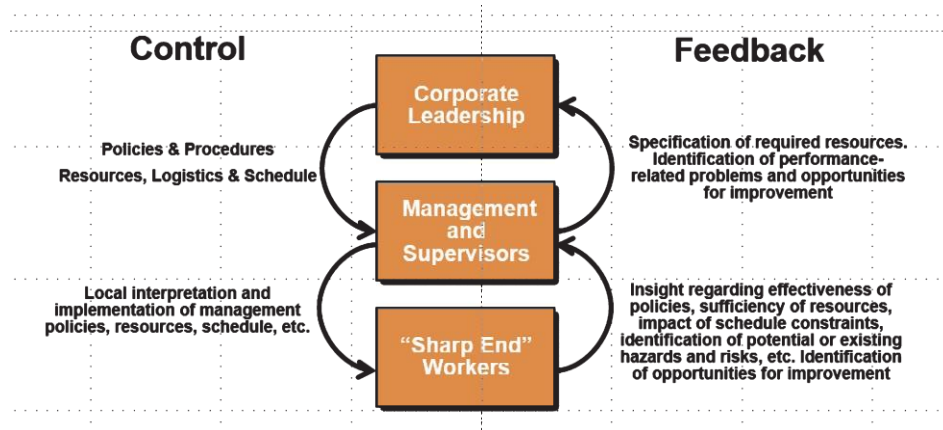


Figure 15. Generic SCS Modified from Levenson (2011).

5.3.4.4 STPA Extension – Mental Model Representation

In the previous section, the fact that both human and machine controllers are modeled within the same framework is a positive benefit with respect to assessing joint optimization of a work system. In Figure 14, the process model within the (human) controller component is described as containing a faulty algorithm. However, the STAMP community of practice decided that this language might be inadequate for human controllers and moved to develop a mental model replacement (France 2017). See discussion in Section 5.2.3.

As seen in Figure 16, the three components are described as follows:

1. How did the operator choose which control action to perform?
2. What does the operator know or believe about the system?
3. How did the operator come to have their current knowledge or beliefs?

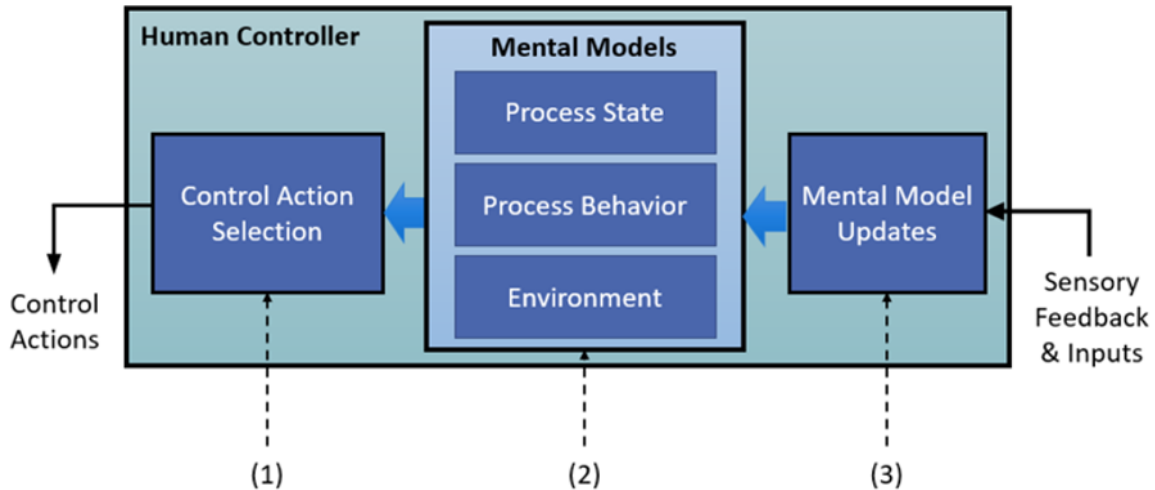


Figure 16. Human controller mental model. (Adapted from France 2017, Figure 18).

In Figure 16, the mental model corresponding to the grease cleaning employee has three subcomponents. The Process State subcomponent refers to the employee/controller's beliefs about the current state of the system. For the majority of employees surveyed, it is inferred that this belief is that warm water is the appropriate additive for the EFC. 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 is that the mixture of EFC and hot water will effectively remove the grease from the floor. For this example, the environment subcomponent refers to the situation that despite the presence of a poster in the work area reminding employees to use cold water with EFC, and a warning on the container itself, this information is either not processed by the employee or the population stereotype that warm water must be used in cleaning activities has overpowered the memory of this information.

Hence, when the employee receives an input signal from the supervisor saying it is time to mop the floor, he/she uses the contents of the mental model and selects the control action: mix EFC with hot water. The visual appearance of the floor after mopped does not appear different after either hot or cold water is used. However, the effect of the hot water is to kill the enzymes, disabling the grease removal properties of the EFC. It should be noted that, if the supervisor was actively observing the employee and noted the error, the result might be an update of the mental model (component 3 in Figure 16.) According to Flach et al. (2015), however, supervisory oversight and mental model correction were not a frequent occurrence.

5.3.4.5 Cognitive Work Analysis/Work Domain Analysis

The use of the generic commercial process facility example will be continued to illustrate the use of WDA as an alternative form of knowledge representation. WDA, a component of CWA (Rasmussen et al. 1994; Vicente 1999) provides a means of characterizing the structure of the user's problem space. See Sections 4.1.3.1 and 4.1.3.2 for additional discussion. A specific tool for accomplishing this analysis is Means-End Abstraction Hierarchy (MEAH).

Figure 17, from Lintern (2009), indicates a very simple example of the core structural relationships comprising a MEAH: Why, How, What. The overall goal (the Why) of this work-domain example is comfort. This is, in effect, a value statement: comfort is valued. One way that comfort can be achieved, assuming that it is cold outside, is by heating. This is a generalized affordance for comfort; that is, a means for accomplishing an end (the How). Moving down the hierarchy is a specific affordance for heating, namely a furnace (the What).

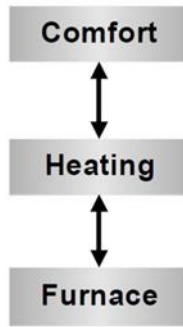


Figure 17. Example of MEAH. (Lintern 2009, Figure 4).

Figure 18 depicts a hypothetical WDA of the generic process establishment as a MEAH. The five levels are typical of most MEAH analyses; the three Why-How-What relationships discussed above would slide up and down the levels. This hypothetical analysis focuses only the components relevant to the current discussion. The actual analysis would be much more complex.

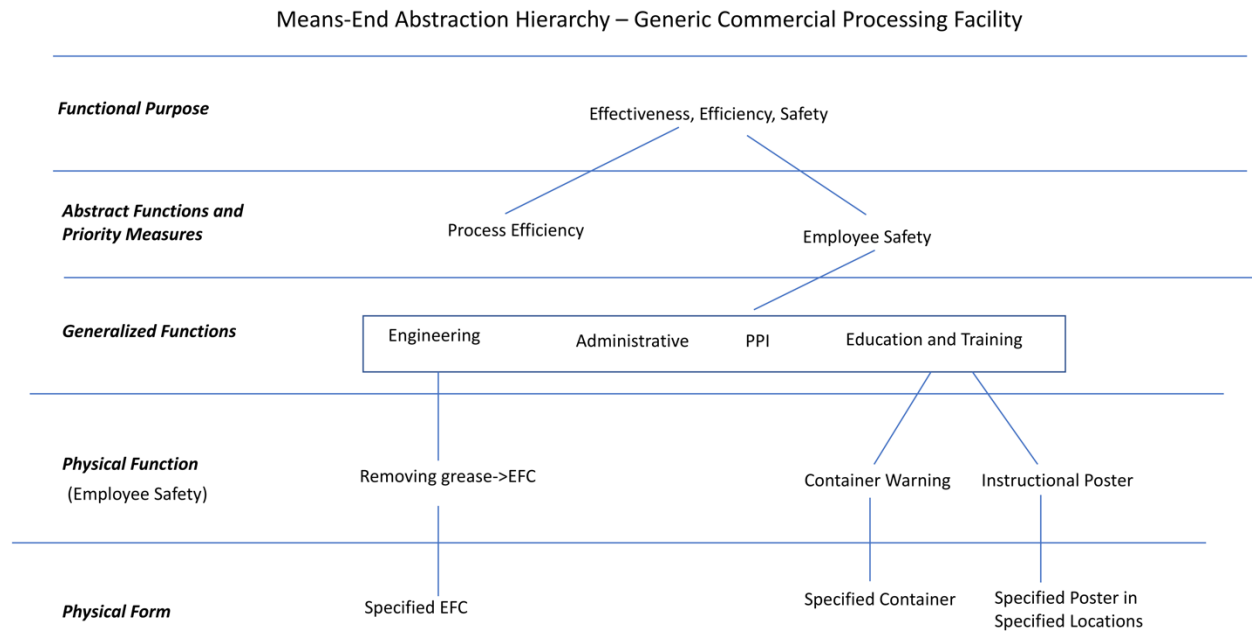


Figure 18. MEAH for Work Domain: Generic Commercial Processing Facility. (Modified from Naikar 2013)

At the upper end of the MEAH is the functional purpose level. This is where the overall goals (ends) of the system being analyzed is defined. In this case, the functional purpose will be taken from resilience engineering in that it is desired that the generic establishment overall work processes be effective (i.e., the product is produced quickly and with high quality), efficient (i.e., the facility is able to make a profit by using resources efficiently), and safe (i.e., injury to employees and unnecessary damage to equipment is avoided).

The next level down is abstract functions and priority measures. This is where the higher-level values which are the means of achieving the ends at the functional purpose level are located. In this case, these priorities are, among many others, process efficiency and employee safety. In a more detailed analysis,

these might be stated in specific quantitative terms (i.e., keep employee injury rate below a certain threshold level).

The third level is that of generalized function. This diagram depicts the means of achieving one of the desired abstract function ends, which in this case is that of employee safety. At this level are listed the traditional components of an occupational safety and health program: engineering solutions, administrative solutions (processes), personal protective equipment, and education and training.

The fourth level is that of physical function. This level is where specific classes of solutions are defined as means to accomplish the functional ends of level three. That is, removing grease by the use of EFC would make floors less slippery and decrease the risk of slips, trips, and falls. It is also recognized that this cleaning agent requires special handling, so a specification for warning level on the solution container as well as the placement of informational posters is required. This level, therefore, is where component specifications are located.

Finally, the fifth level is that of physical form. This is where the actual physical components which meet the specifications in level four are defined. In this case, a particular brand of EFC is identified, it is determined that a warning to use cold water is visible on the container, and that posters requiring the use of cold water are available at specific locations in the workplace.

It should be noted that the same safety constraints identified in the STPA analysis (see Section 5.3.4.3) are present in this analysis as well. However, no actual human actors are part of the analysis; WDA is formative in that it identifies possibilities for action (affordances). Within these possibilities for action, however, are built in some subtle constraints based on information contained in the data collected from the actual case upon which this example is built (Flach et al. 2015). Specifically, the education and training function is satisfied only by warning labels and posters. In the overall training budget, the priority for safety training was relatively low compared with process efficiency training.

5.3.5 Knowledge Elicitation

Knowledge elicitation refers to the process of identifying the **content** upon which the various knowledge structures just described are constructed. Fundamentally, this process can be considered the inverse of the knowledge-mapping problem (see Section 5.3.4.1, Figure 11) in that the starting point is the expert's mental model. Needless to say, the usefulness and feasibility (Naikar 2009) of the knowledge representation employed depends critically on the (a) comprehensiveness (completeness) and (b) the elicited information upon which it is based. Much information for the constructed knowledge representation can be obtained from available documentation, but many more critical pieces of information are based on undocumented practice and or tacit knowledge of users. Useful insights come from Naturalistic Decision-Making in Action (Klein et al. 1993) and human system integration (Booher 2003). The type of knowledge representation, normative, descriptive, or formative, will influence the kind of information to be elicited. Thus, if the analysis has a formative intention, knowledge elicitation will need to be focused on **why** questions, as well as **what** and **how** (see Section 5.3.4.4).

However, the conditions under which analysts seek to collect such information are not always benign. (Zuboff 1988) reports a case study of a paper mill in which previous manually operated processes were brought under digital control. Front line operators, whose previous daily work was described as an industrial version of cooking, were now working in a computerized control room. Those operators who managed the transition became adept with their new equipment and discovered they had the capabilities for simulation of potentially more efficient processes. They started asking questions of their supervisors, who were chemical engineers, and productivity began to quickly rise. However, at some point, the supervisors began to feel that their jobs might be in jeopardy if they transferred their knowledge to the technicians. They stopped answering questions and the rising productivity ceased. Therefore, careful attention to psychosocial dynamics of information collecting is required. Might the source of the

information perceive that the material he/she is providing will result in the loss of their job due to automation?

There are additional reasons that experts with valuable tacit knowledge may not provide knowledge: the knowledge provides status as the expert within the organization, they may plan to retire soon and want to be hired back as a consultant, they may be upset with the organization that did not give them a raise or promotion when they felt it justified, they were so busy they felt it more important to do their job than describe tacit knowledge, etc. EPRI conducted a major project to develop guidelines for eliciting valuable tacit knowledge, and tested the guidelines at nuclear and fossil plants, and a transmission and distribution center (where concept mapping was used to represent the results). The project was performed because nuclear management was concerned about loss of expertise with the expected major increase in retirements (EPRI 2004) (Hoffman and Moon 2010).

5.3.5.1 *Methods of Knowledge Elicitation*

There are many documented methods of knowledge elicitation available to the analyst (Durso, 1999; see particularly chapter by N. Cooke). Naikar (2013, p. 172) provides a survey which includes documents, field observations, and interviews. Specific variants of these include use of concept maps as triggers to informants Hoffman and Moon 2010; critical incident technique (Crandell et al 2006); walkthrough (demonstration at worksite), talkthrough (explanations away from the worksite) (Kirwan and Ainsworth 1992). Two specific method not in the above source which have potential utility for this research project are described below.

5.3.5.2 *Nominal Group Technique*

NGT (Delbecq et al. 1986) is a method which allows each member of the group to contribute equally. The general procedure is that the group is introduced to the method, a problem is stated, and members asked to individually write down their ideas relative to the problem. A series of round robin session follow in which all members present all ideas, each of which is written on a chart. Each member then discusses his or her idea, but the ideas are now considered property of the group as a whole. This process continues until discussion is concluded. The group then votes to prioritize the ideas.

The use of NGT as a knowledge elicitation technique is described in the NDS TQ study (see Appendix A). In this case, teams of stake holders used NGT to identify quality problems and potentials solutions. The process was successful in that most of recommendations were adopted by management. Westinghouse Commercial NFD later was awarded the Malcolm Baldrich National Quality Award.

In addition, the NGT was used successfully to help identify high priority HFE efforts that the nuclear industry should adopt following the Three Mile nuclear plant accident in 1979. One example was the recommendation to establish an IEEE standards group to develop HFE standards, emphasize development of human reliability analysis methods (IEEE, 1979).

5.3.5.3 *Work Domain Analysis Oriented Interview*

Additionally, a semistructured interview protocol specifically oriented for creation of a work-domain knowledge structure was utilized to examine the work processes of professional university research librarians (Simons et al. 2006). The participants were asked to describe the typical process he or she would use to address a typically research task. Why and How follow-up questions were used to elicit additional information. It was a straightforward procedure to map the results to a combined MEAH for all the respondents. As a validation step, the MEAH was discussed with each respondent and corrections/modifications made as appropriate.

5.3.6 Cross-Functional Integration

It is useful to differentiate between the knowledge elicitation problem and the cross-functional integration problem since they have certain similarities and may use the same methods. However, the goals are slightly different. Knowledge elicitation's purpose is primary to construct knowledge representations. Cross-functional integration's purpose is to coordinate design and/or decision-making. This distinction may be helpful for analytic purposes, but also in many situations, particularly involving design iteration, these goals may overlap and use similar methods. The focus in knowledge elicitation is on ensuring that individuals in a team with relevant knowledge and information will not be excluded from participating in collective decision-making. The focus in cross-functional integration is slightly different. Here the concern is ensuring that the structure of organization is not a barrier to collective decision-making.

In fact, the NGT approach described previously can, as described, be useful for decision-making and collaboration. An unpublished consulting project involving the first author of this report also successfully used NGT. The author and his wife were hired as ergonomic consultants to the Internal Revenue Service (IRS) and tasked with establishing ergonomic problem-solving teams at a major service center. Using a group of employees they had previously trained in basic ergonomics, a series of NGT sessions were used to (a) define the team's core mission, (b) establish the team's organizational structure, and (c) select the team's leaders. It is of note that while the team participants included representatives of both management and labor, the team elected a non-management employee as their leader. Corporate management accepted this decision, which was surprising in an organization as highly structured as IRS.

The IDEAS tool described in Section 4.2.2 also provides a field-validated method for collaboration/coordination. While initially focused on health and safety interventions, the method could be easily modified for NPP modernization. The process includes a bi-level approach, in which a steering committee provides an advisory role to collections of stakeholders who conduct the bulk of the analysis. Moreover, the structural framework in this template could easily be adapted to include NGT.

5.3.7 Literature Review Summary as Example of Concept Map

A final example of knowledge representation is the concept map. See for example, (Hoffman & Moon, 2010). Figure 19 consists of a concept map which summarizes the literature review of this report. This report is produced using cmap tools (cmap.ihmc.us.) The logic of the concept map is that concepts are connected by linking propositions. For example: the central concept "Sociotechnical Systems Theory" is linked to and underlies "Macroergonomics." This concept, in turn, is linked to and includes "Work System."

In addition, concept maps can be used for Knowledge Elicitation if the resources to familiarize the respondents with the technique are available.

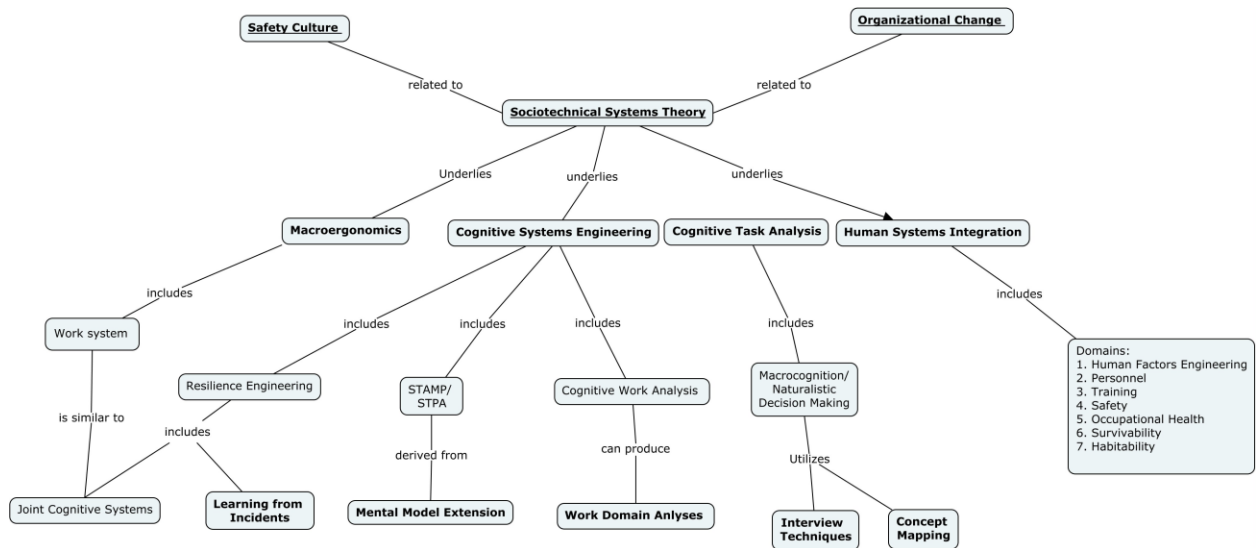


Figure 19. Concept Map Representation of Literature Review

5.4 A Problem-Solving Approach to Methodological Integration

The framework for the remainder of this section will be organized in terms of specific identified problems associated with the NPP modernization strategy and proposed solutions. Table 1 in the current section contains a matrix of problems and possible solutions. Links to subsequent sections will contain detailed descriptions of problems and solutions. These descriptions will refer to materials presented in previously in Sections 5.2 and 5.3, as well as relevant examples from the case studies contained in the Appendices.

To reiterate, the goals for this report in general and this section in particular, are to develop a strategic framework for effective integration of human and organizational expertise within NPP digital modernization efforts. The solutions proposed below involve the use of methods which have been successful in previous practical applications. However, it is also the case that the complexity of NPP systems necessarily dictates a certain amount of flexibility and pragmatism in such application. In particular, as discussed in Section 5.3.1, combinations of methods from different sources may sometimes be required. Alternatively, the level of complexity may dictate the necessity of more than one perspective. In this regard, guidance may be taken from the USS *Zumwalt* case study (Appendix A) in which method selection was always based on pragmatic consideration of utility, as opposed to conceptual unity.

For many of the problems addressed below, considerable amounts of published technical requirements and regulations are already available. The materials added in the current report are meant to supplement and enable NPP modernization design and analysis activities currently well-established. In particular, the solutions discussed below can be framed in terms of three high-level issues: (1) Knowledge representation; (2) Knowledge elicitation; (3) Cross-functional integration (see Section 5.4). Moreover, criteria for solution effectiveness are available: Usefulness and Feasibility (Naikar 2009). Usefulness can be assessed in terms of two subcategories: impact and uniqueness. Impact reflects the extent to which the method actually influenced practice, whereas uniqueness reflects the extent to which a novel contribution is made relative to standard techniques commonly in use. Feasibility is assessed relative to the capability of the method to be accomplished within existing project resources (e.g., schedule, staff, and financial budget).

It should also become clear that the listed problems and their solutions have dependencies. In many cases, solutions to one problem can be referred to a different problem.

Table 1. Matrix of problems and solutions.

	Problem	Solution	Section
1	Top management consensus on need for modernization	<ol style="list-style-type: none"> 1. High-level Strategic plan using facilitated genetic algorithm 2. Past Experience and comparing the nuclear industry with other industries (e.g., commercial airlines) 	5.4.1
2	Consensus on strong adoption/support for core values essential for successful transformation	Same as above	5.4.1
3	Source for core values	Using Baldrich award quality framework as core, combine resilience and safety culture	5.4.2
4	Develop HFE Program Management Plan?	<ol style="list-style-type: none"> 1. IDEAS framework combined with NGT 2. Representing the HFE Program Management Problem Space through WDA 	5.4.3
5	Obtain valuable tacit (undocumented) knowledge from experts	<ol style="list-style-type: none"> 1. Use knowledge elicitation methods as document in EPRI sources and 5.4.5 2. Apply STPA 	5.4.4
6	Determine if new skills are required to control new technology, and if current operators have the ability to learn the new skills	<ol style="list-style-type: none"> 1. Use Naikar's adaptation of CWA to training needs. 2. Use Resilience Engineering Learning from Incidents 	5.4.5
7	How to achieve the integration of PTPG at all levels of the system	<ol style="list-style-type: none"> 1. Components can be mapped into work system framework 2. Use Work Domain and Control Structure Analysis to focus on joint optimization of work system components 	5.4.6
8	The silo problem: how to bring the different stakeholder groups into agreement on communicating, sharing information and getting agreement on decisions on common priorities that cut across groups	Modified version IDEAS Use of NGT in step 1 to ensure all concerns are verbalized.	5.4.7

5.4.1 Problem 1 Management Consensus and Problem 2 Consensus on Core Values

Problems 1 and 2 are both consensus problems, but differ on the topic upon which consensus is needed. Problem 1 is achieving top management consensus on the need for modernization and Problem 2 is achieving consensus on the core values needed for transformation. There are ample sources of

documentation on economic and structural reasons why the nuclear power industry needs to embark on a modernization plan (Thomas and Hunton 2019) (Hunton and England 2019). However, deciding to commit to modernization is not the same as creating a modernization plan that succeeds. Figure 20, below, depicts data from the International Committee on Systems Engineering (INCOSE) on the high failure rate of major systems engineering projects. The two top causes of failure, incomplete requirements and lack of user involvement, are both directly relevant to the organizational goals of this project. The crux of the problem center on the utility's need for consensus. These issues might be considered beyond the scope of this review, but it is important to acknowledge without strong consensus and support from top management, the required transformation is likely to fail.

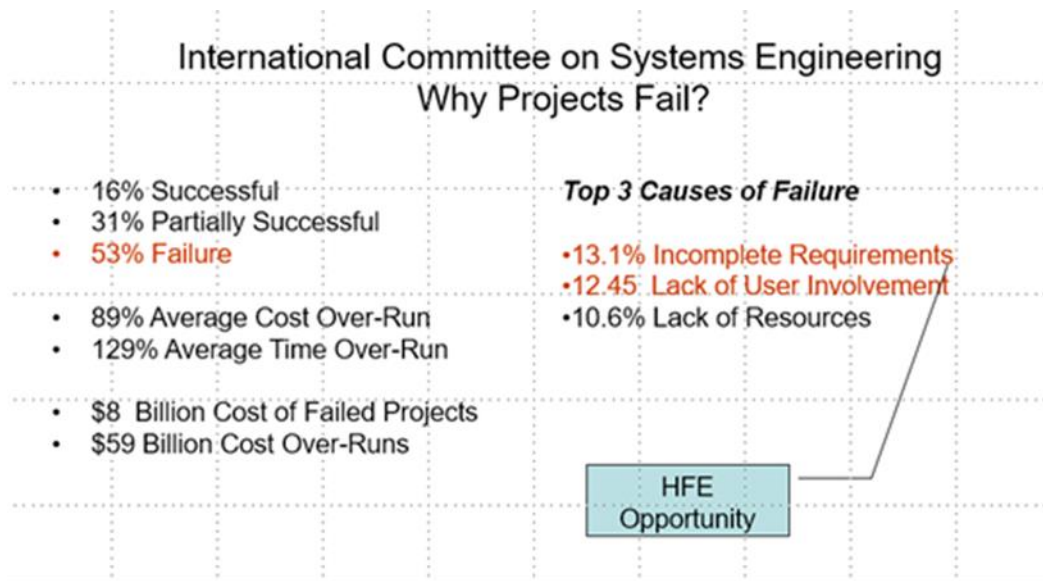


Figure 20. INCOSE Data on Project Failure (Dainoff 2006).

While the solution to this problem necessarily must emerge from top management, and it would be presumptuous to dictate to these leaders how to manage their businesses, the contribution of this report would be the following two proposals in support of this necessary action of such leaders.

5.4.1.1 *Solution 1 to Problems 1 and 2: Consensus Building Through Facilitated Genetic Algorithm*

The first proposed solution to Problems 1 and 2 involves consensus building through facilitation based on a genetic algorithm. Specifically, this solution encourages the development of a position paper summarizing high level strategic objectives and documenting the necessity of a long- term plan. While, in the past, the NEI has prepared such position papers and represented the industry to the NRC, the process of generating such objectives could utilize a version of consensus building through facilitated genetic algorithm (McGrew 2002). See details in Section 5.3.1. In this process, an initial high-level set of objectives would be presented to an upper management team. Team members would agree on a Fitness Function (set of criteria and constraints which the final product should satisfy), and then proceed to systematically revise and assess their position using the Fitness Function until they achieved consensus (see Table 2). This process mimics the genetic principle of natural selection in that each round of revision involves both modifying another participants' previous work product (genetic crossover) and creating something completely new (mutation). As such, knowledge elicitation from all stakeholders is accomplished in a collaborative and coordinated fashion. In addition, the knowledge representation problem is solved in the sense that each round of revision the group consensus is identified by the ratings of each set of strategic goals scaled against each of the criteria in the Fitness Function.

It is expected that the details of the concept of operations could result from this effort (Meaning 1, see Section 1). As discussed in Section 5.3.1 the BCPE utilized a method originally used for software development (McGrew 2006) to carry out required revision of the key document defining the structure and scope of the profession: the EFM. This method will be described in sufficient detail that it could be applied in NPP modernization practice.

The starting place for the process was the assembly of a group of stakeholders. In the present case, the stakeholders were nine current and past directors of BCPE. The stakeholders agreed on the overall goal, which was to produce a revised EFM. They also agreed to utilize the following Fitness Function to assess work products. The Fitness Function embodies the criteria and constraints which the Directors agree the revised EFM must possess.

Table 2. Fitness function criteria.

Fitness Function					
		-3		0	+3
1.	Inclusive				
2.	Breadth				
3.	Depth				
4.	Parsimony				
5.	Representative				
6	Practical/Usable				
7	Credible (Face Validity)				

The first round required that each stakeholder submitted a revision to the current EFM to the coordinator by a deadline. The coordinator removed any personal identifiers. It was agreed that all submitted work products became the “property” of the group.

When all submissions were received, the coordinator collated them and returned them to the group. Each group member rated each submission according to the Fitness Function, and returned the ratings to the coordinator.

For the next round, each member developed two revised EFMs. These revisions should: (a) include something from a previous version (crossover), and (b) something complete new (mutation). Since the goal was consensus, each member was asked to be guided in their work by the results of the fitness rankings of the previous contributions. These contributions were, in turn, submitted and rated, and the process continued until consensus was reached.

In this case, seven rounds were sufficient. The final version was accepted by BCPE as the revised EFM. This is an example of how a management team can come to consensus concerning the structure of a major organizational change. A similar example, using a different method, is the Westinghouse Commercial NFD approach. The approach used and the results are provided in the Case Study in Appendix A. The organization involved a couple of thousand workers, and the organization has similarities to a nuclear plant.

5.4.1.2 Solution 2 to Problems 1 and 2: Conduct an Operational Experience Review.

The second solution to Problems 1 and 2 is to perform an operational experience review. In this case, the recommendation is to conduct a historic review of way in which consensus towards improving safety among developed industry and government leaders in the airline industry during the mid 1930s compared with the nuclear industry. This solution presumes a traditional research paper that explores the similarities and differences between the nuclear and airline industries. This comparative historic review should provide useful information in negotiating current relationships (within industry and industry

regulator). Even here, however, the interaction of collaboration, knowledge elicitation, and knowledge representation functions should be explicitly considered by the research team.

5.4.2 Problem 3. Source for Core Values

The recommendation from the case study on *Deepwater Horizon* that an engineering culture in addition to a safety culture is needed is the motivation for this section. A potential framework for values will be developed by using a modification of Means-End Hierarchy in which the basis are the resilience engineering goals of efficiency, effectiveness, and safety. These are mapped onto the criteria for the Baldrich award which are in turn mapped on the components of the NRC Safety Culture structure.

Problem 2 in Section 5.4.1.1 states that there is a need for a sustained top management commitment to a set of core high level values in order to maintain the required long-term (10–20 years) focus on the desired concept of operations. The essential logic here is that such values will serve as guidance for making lower-level operational and trade-off decisions. In the military, such a philosophy is labeled “command intent.” The danger is that if sustained management commitment falters or varies, key mission critical-components are at risk. Evidence of such failure can be seen in the Boeing 737 Max, USS *McCain*, and *Deepwater Horizon* case studies in Appendix A. Problem 3, in turn, asks what the source and nature of those values should be. This section provides a solution.

While a number of organizations, including the NRC, specify the inclusion of safety culture as a high level value, we have argued (see Section 4.1.8), that the concept of safety culture is scientifically problematic and, in any sense, is not adequate by itself for making operational decisions. On the other hand, IAEA has explicitly argued that resilient organizations are essential to a well-functioning modern NPP, which implies that having a common set of core values and management commitment are essential to addressing this problem. These solutions are elaborated on in the following sections.

5.4.2.1 Solution to Problem 3. Generate Core Value Statement

Our proposed solution to problem 3 is to generate a core value statement by combination of Baldrich award criteria, NRC Safety culture traits, and resilience engineering goals. The following solution is suggested for problem 3. As a conceptual framework, the abstraction hierarchy in WDA explicitly includes specifications of values and priorities at the top of the hierarchy. Therefore, within these values and priorities levels, three sublevels of values are defined. As seen in Table 3 below, the first and most general sublevel of the three is: Interdependence of systems performance criteria as defined by resilience engineering (Hollnagel 2006). The next sublevel are the 10 core values and concepts (Table 4) which form the basis for performance excellence as defined by the Malcolm Baldrich National Quality Award (Calingo 2002). At the third sublevel may be found the nine traits (Table 5) described by NRC as comprising a positive safety culture (NRC 76 FR 34773; 2011). A suggestion as to how the relationships among these levels might appear when mapped out is shown in Figure 21.

As was the case in Problems 1 and 2, it is not the role of the authors of this report to carry out the actual mapping. Rather, this would be role of higher management. Conceptually, what is offered is a mechanism for integrating three sets of values; each of which presumably might have some degree of resonance with top management.

Philosophically, the resilience criteria are a high-level commitment to keep three major systems performance criteria in balance. At the same time, the Baldrich Award criteria should have a sufficient combination of generality and specificity to serve as a reference point for multiple aspects of organizational function. At the same time, the individual components comprising Safety Culture ought to translate into elements of the organization’s quality program, rather than be conceptualized as a separate silo. This would result in coherence in terms of the relationship between of organizational values and the processes of systems engineering.

Table 3. Resilience Engineering criteria.

Resilience Engineering: Interdependence of systems performance criteria
Effectiveness: Accomplishment of mission
Efficiency: optimization of resources
Safety: avoidance of injury, damage

Table 4. Baldrich award criteria.

Malcolm Baldrich National Quality Award: Core values and concepts which form the basis for performance excellence
Visionary Leadership: Senior leaders' capacity for setting directions for the organization by action and by example
Customer-Driven Excellence: The organization's focus on the customer and the ability to ensure that its operations meet their needs and expectations
Organizational and Personal Learning: The ability of the organization to acquire, share, and use information to improve
Valuing Employees and Partners: Commitment to employees and partners (such as suppliers and subcontractors) in order to optimize the opportunities for success in their work environment and contributions to the organization
Agility: Ensuring flexibility and the ability to act speedily
Focus on the Future: Operating strategically and ensuring a long-range orientation
Managing for Innovation: The capacity to develop creative and effective products, services, and processes
Management by Fact: Reliance on data and analysis in decision-making
Public Responsibility and Citizenship: Proactive and responsive commitment to the needs and concerns of the community and larger public
Focus on Results and Creating Value: The orientation to managing key outcomes for accomplishing the mission, meeting customer and market requirements, and creating value for key stakeholders

Table 5. NRC safety culture traits.

NRC Safety Culture Policy Statement (76 FR 34773; June 14 2011)
Leadership Safety Values and Actions: Leaders demonstrate a commitment to safety in their decisions and behaviors
Work Processes: The process of planning and controlling work activities is implemented so that safety is maintained
Effective Safety Communications: Communications maintain a focus on safety
Problem Identification and Resolution: Issues potentially impacting safety are promptly identified, fully evaluated, and promptly addressed and corrected commensurate with their significance
Continuous Learning: Opportunities to learn about ways to ensure safety are sought out and implemented
Respectful Work Environment: Trust and respect permeate the organization
Personal Accountability: All individuals take personal responsibility for safety

Environment for Raising Concerns: A safety conscious work environment is maintained where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment or discrimination

Questioning Attitude: Individuals avoid complacency and continually challenge existing conditions and activities in order to identify discrepancies that might result in error or inappropriate action

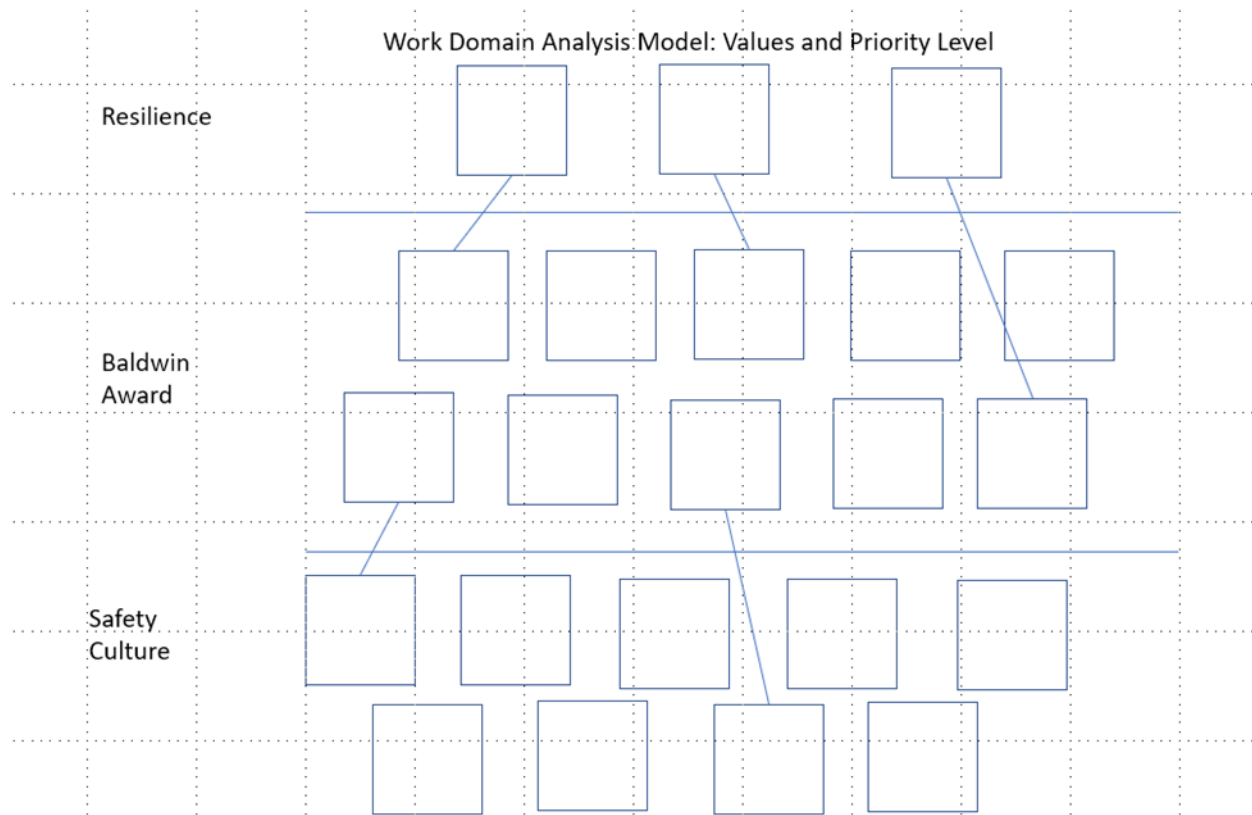


Figure 21. Conceptualized depiction of WDA of core values.

5.4.3 Problem 4: Develop HFE Program Management Plan

The centrality of the cross-functional integration issue for HFE within the systems engineering process has been clearly stated. Section 4 of the EPRI DEG emphasizes that systems engineering is a collaborative enterprise in which no single perspective or discipline may be allowed to dominate. Section 2.5.1.4 of EPRI's HFE guide (EPRI technical report 2003004310) requires 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, Section 2.5.3.5 of the HFE guide emphasizes that 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.

The two solutions identified in this section are actually meant to be considered in combination. Solution 1 primarily addresses the cross-functional integration and knowledge elicitation issue, whereas Solution 2 primarily addresses the knowledge representation issue.

5.4.3.1 Solution 1 to Problem 4. Modification of the IDEAS Tool Utilizing NGT.

Section 3.2.1 of EPRI technical report 3002004310 discusses the requirements for developing a HFE Project Plan for a Modification. Additionally, EPRI's DEG Section 6.1.1 has the following requirement as a starting point: 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.

Section 4.2.2 of this report described a methodology originally created for the development of occupational health and safety intervention. This IDEAS tool, as modified below, is proposed as a framework developing an overall end point vision, concept of operations, and migration plan while considering HFE impacts and stakeholder needs.

Figure 22, below, is a slight modification of Robertson et al. (2013) in which the language is more appropriate to the NPP domain. However, the logic is similar to the original. As can be seen in Figure 22, the method 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.

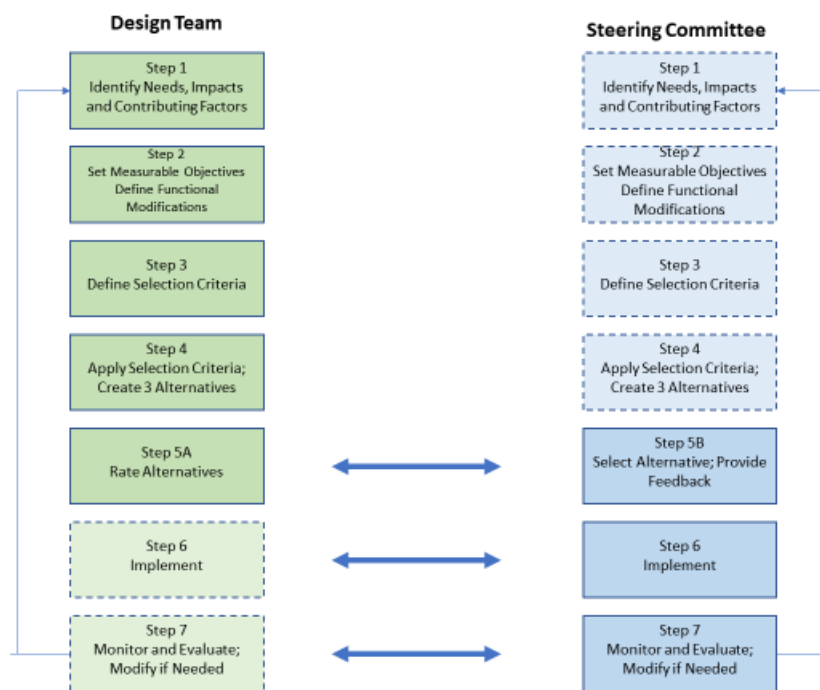


Figure 22. Intervention Design and Analysis Scorecard. Modified from Robertson, et al. (2013)
[<http://links.lww.com/JOM/A134>]

Steps 1 to 5A (solid boxes) illustrate the steps by which the design team develops and then prioritizes potential alternative actionable outcomes. Steps 5B to 7 (solid boxes) indicate the activities of the independent steering committee, which receives, reviews, and either accepts or rejects the recommendations of the Design Team.

Steps 1–4 (dashed boxes) illustrate monitoring/feedback and support roles played by the steering committee during these steps. Steps 6 to 7 (dashed boxes) illustrate a supporting, informational role played by the design team during these steps.

Step 1. The design team defines the problem space and conducts a systems analysis. Possible contributing factors are identified.

Step 2. The design team develops a set of functional objectives/modifications which address the needs and impacts addressed in Step 1.

Step 3. The design teams develop a set of selection criteria to prioritize potential alternatives developed in Step 2. Suggested categories of criteria include scope, effectiveness, obstacles, and cost.

Step 4. The design team uses the selection criteria to assess and/or combine potential alternatives into three specific alternatives.

Step 5A. The design team rates each of three alternatives on each of the selection criteria. These ratings become the prioritized recommendation to the steering committee.

Step 5B. 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.

Step 6. The steering committee implements the decision.

Step 7. The steering committee monitors and evaluates the impact of the decision. Modifications are made if necessary.

The 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, NGT (see Section 5.3.5.2) should 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, step 4 might 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.

5.4.3.2 *Solution 2 to Problem 4 (Part A) Representing the HFE Program Management Problem Space*

There exists a plethora of HFE documentation concerning the design of effective HSIs for operators of NPP control rooms. As discussed in above, the same fundamental HFE principles which are applied to enabling enhanced performance of control room operators can also be utilized for the collaborative activities of stakeholders participating in the systems engineering process of migrating to more modern systems. For example Forbes, Gibson, Pritchett, and Hanes (2012) describe a case where an utility explored the modernization of multiple turbine control systems (TCS) across its fleet of NPPs, and used HFE principles.

The knowledge-mapping principle described in Section 5.3.4.1 and represented in Figure 11 (repeated below) will be applied to characterize the knowledge representation problem. 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 Step 1 of Figure 22 would be represented in the upper left box of Figure 22—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 22—CES Approximation of Domain. This would presumably be occurring during Step 2 of Figure 22. As alternative automation possibilities become conceptualized (Steps 3 and 4 of Figure 22), more formal representations, equivalent to the Display in Figure 11 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 in Steps 4 and 5A, and ultimately for the members of Steering Committee, in Steps 5B.

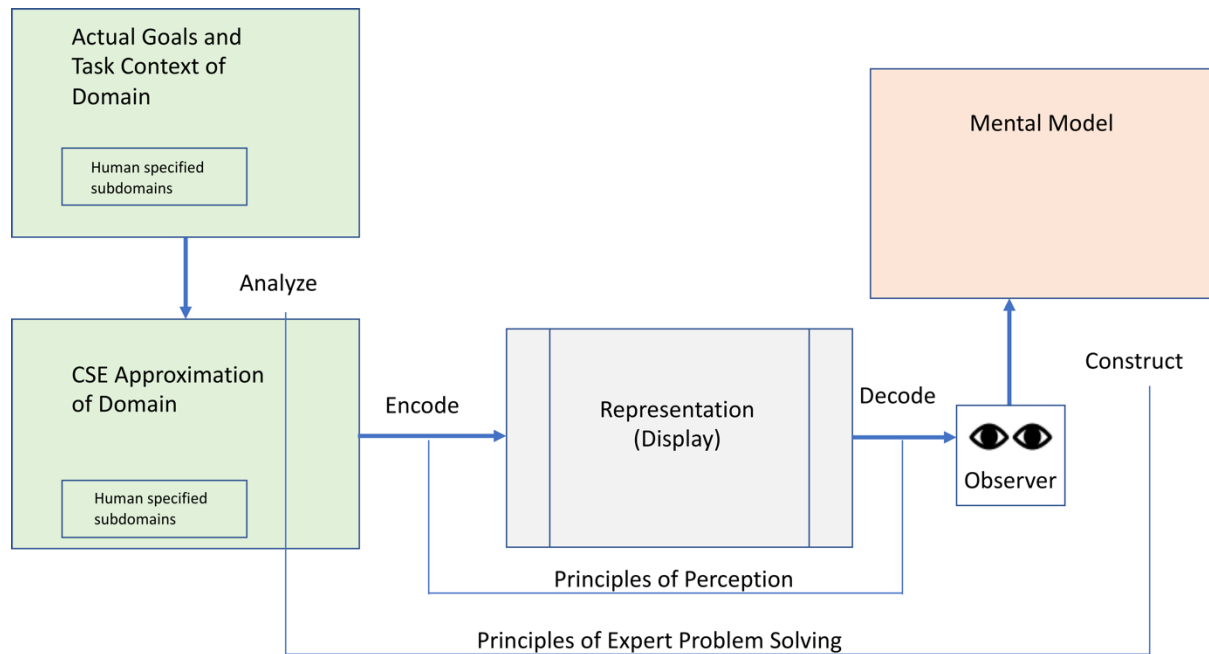


Figure 11. (repeated). The Mapping Principle (Adapted from Elm et al. 2009; Originally in Woods, 1991).

However, problems like TCS upgrades will always occur within an organization context. This context will necessarily inform both the knowledge elicitation and knowledge representation problem. Figure 2 (repeated) is an example of such content (see also above). It depicts a pathway to modernization of NPPs in which modernization of capabilities through integrated operations can be translated into costs savings through work reduction opportunities.

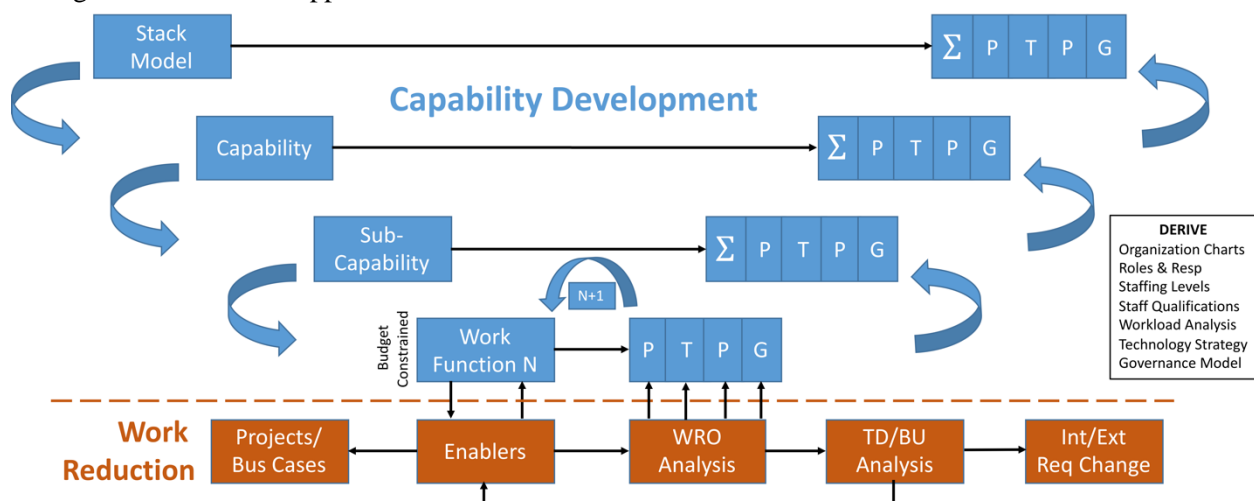


Figure 2. (repeated). A Model of Integrated Operations Merging Capability Development and Work Reduction Strategies (Thomas 2019).

We further assert that WDA (Vicente 1999) would provide an effective knowledge representation for this problem. Given its formative structure, it should be useful in allowing visualization of alternative automation possibilities. In addition, once created, a WDA has been shown to be valuable for tasks later

on in the systems engineering process, such as defining staffing structures and training requirements (Naikar 2013, chs. 10-11).

5.4.3.3 *Solution 2 to Problem 4 (Part B): WDA As Knowledge Representation*

A relatively simple example of the use of WDA is found in Section 5.3.4.4. That example illustrated one dimension of WDA, the MEAH. In more complex work domains, a second dimension is employed: a Part-Whole Decomposition.

In the current problem, the domain to be represented focuses on the possibilities for automation of one subsystem, the TCS, but must also include the organizational context. Consequently, as seen in Figure 23, the component on the far left contains entries at the top for the more abstract portion of the WDA. This is where the higher-level goals, values, and priorities of the organization would be located. Section 5.4.2 (Problem 3) addresses the issue of core values in terms of WDA as well. These goals, values, and priorities act downward in the means-end hierarchy and to the right along the part-whole decomposition, to effect decision-making at lower levels. In this case, an organizational priority is modernization in service of increased efficiency (reduced cost), and effectiveness of power generation, while maintaining safety. It must be emphasized that Figure 23 is only meant to illustrate principles and is considerably simplified.

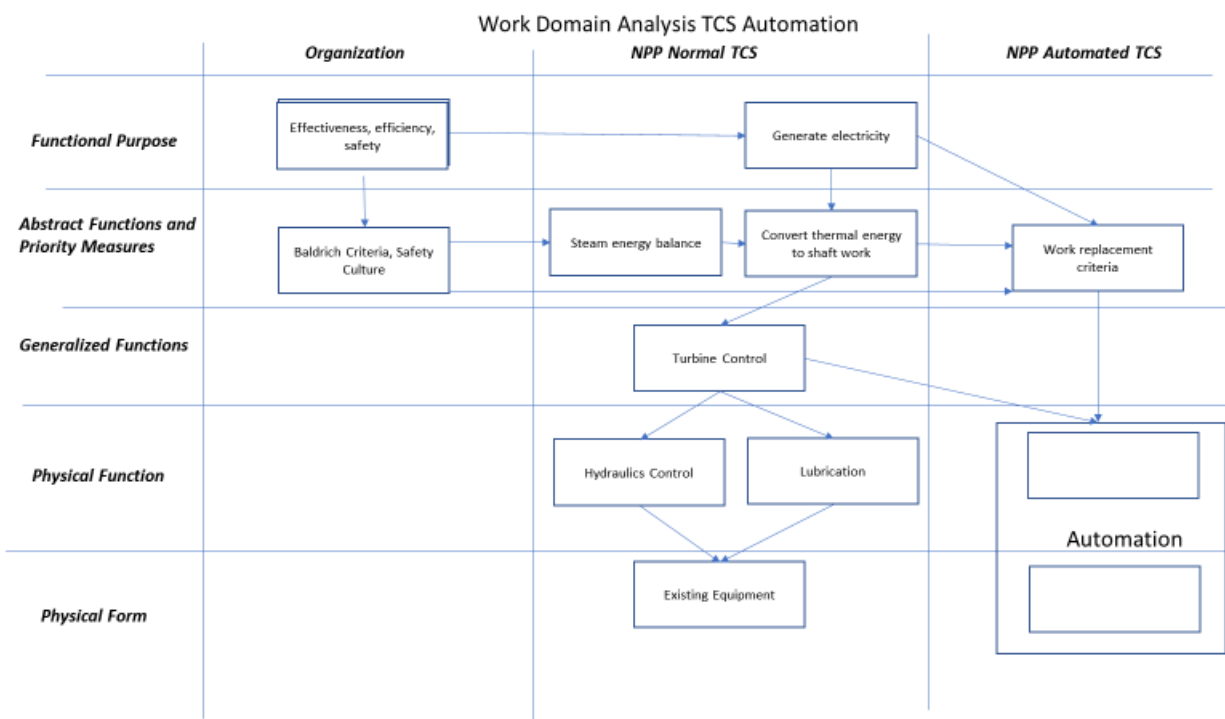


Figure 23. WDA Example Illustrating Automation of Turbine Control (After Vicente 1999).

The next section to the right contains attributes of the current NPP configuration relevant to the current discussion of TCS. Elements of this portion of Figure 23 are taken from (EPRI 2012, Figure 5.3).

The functional purpose is to generate electricity. At the abstract function level, the means of generating electricity is by converting shaft work to electric power. In addition, the values and priorities from the organizational level propagate across to this subcomponent. At the generalized function level, this abstract function is achieved by controlling a turbine to which steam energy is applied. At the level of physical function, two means of achieving controls are specified: hydraulics and lubrication. Finally, the lowest level contains a description of the actual physical mechanisms by which the turbines are controlled (e.g., valves controlling how much super-heated dry steam is applied to the turbine blades).

The right-most section of Figure 23 allows for the description of possible automation solutions. Alternative versions of this section could be presented. At the top two levels, functional purposes and abstract functions from the previous two sections are propagated. An additional priority specific to the modernization process is included. This is the Work Replacement priority. This priority acts as a constraint on automation solutions such that an expected benefit from any solution is the simplification of work such that staffing needs are reduced. The remainder of Figure 24 is left as a placeholder for specific automation alternatives.

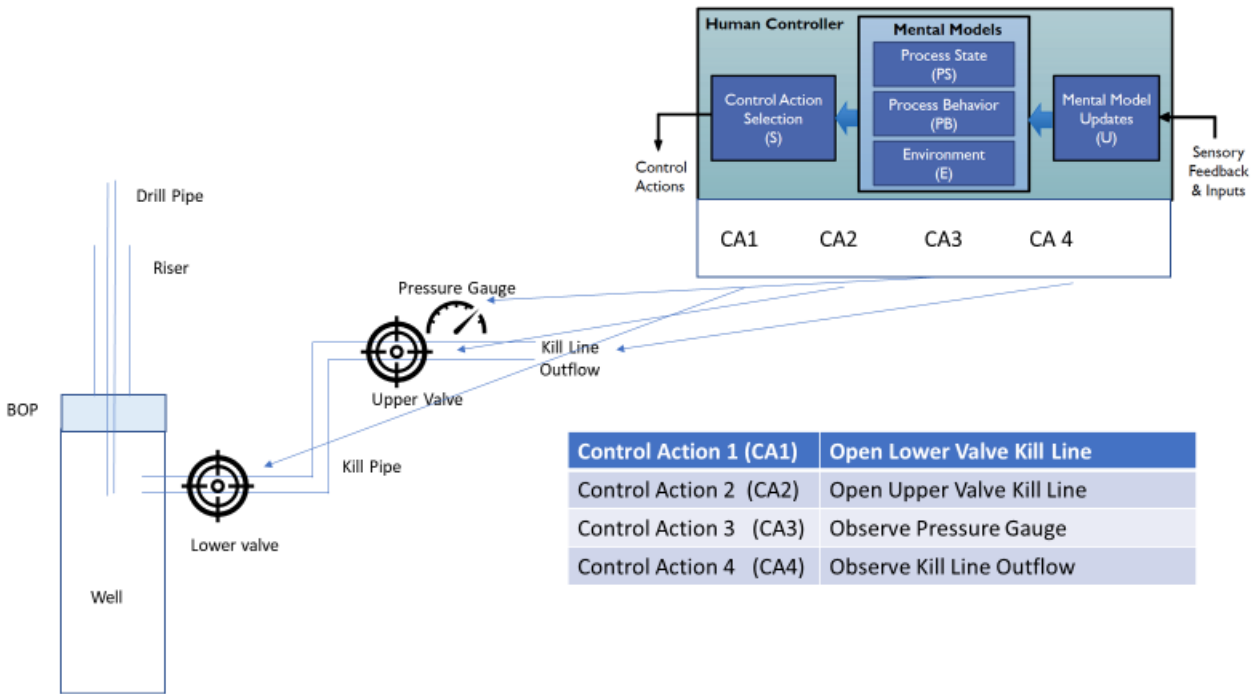


Figure 24. Control structure of negative pressure test on *Deepwater Horizon* (After Boebert and Blossom 2019).

The WDA presented here is a formative analysis (e.g., Naikar 2013, p. 14). As such, it reveals how work *can* be done in a system, as opposed to being prescriptive (how work *should* be done) or descriptive (how work *is* being done). The formative nature is what makes WDA so useful in considering alternative possible configurations.

However, as discussed earlier, WDA is only the first part of a broader approach called CWA. WDA is followed by Control Task Analysis, Strategies Analysis, Social-Organizational Analysis, and Worker Competencies Analysis. Logically, CWA takes an ecological approach in that the first step, WDA, characterizes the constraints or possibilities for action in the environment. As such, this description is independent of any particular actor or situation. Each successive analytic step reflects a reduction of degrees or freedom of possibilities for action. Control Task Analysis looks at possible control actions on the work domain. Strategies Analysis looks at the which control actions, of those possible, might be most effective. Once these constraints have been determined, Social-Organizational and Worker Competency Analyses look at how that work might best be allocated among different types of groups and/or individuals. Interestingly, it is only at this point that traditional human factors function allocation should take place.

The logic which stipulates that CWA begins with an ecological approach is not arbitrary. Particularly in a safety-critical domain such as NPPs, it is essential that key environmental constraints—which are driven by the laws of physics—are clearly reflected in the WDA and are available to be decoded and

constructed into a user mental model (Figure 11). As stated by Naikar (2013, p. 12): “An ecological approach to work analysis emphasizes that designs must be compatible with environmental constraints before it is worth considering that they are compatible with cognitive constraints.” Put simply, being concerned that the user’s mental model does not correspond with the design model in the case of a safety-critical system based on physical law, implies that it is the user mental model, not the design, which needs to change. Of course, just the opposite may be the case in a consumer domain such as marketing a new TV show. This distinction is reflected in Naikar’s discussion of causal vs. intentional systems (Naikar 2013, Fig 2.13). She defines a continuum with one end being from tightly-coupled causal constraints based on physical law, and the other end being user-driven intentional constraints. The examples just given, NPPs and TV shows, are at each extreme of the continuum.

5.4.4 Problem 5: Obtain Tacit Knowledge from Experts

The issue of tacit (undocumented) knowledge of the personnel within any complex sociotechnical work system is problematic. Should these personnel leave without their knowledge being documented, critical gaps in organizational performance are likely to occur. This section has two different solutions to this problem. The first is a report of a straightforward tacit knowledge elicitation project conducted by EPRI at a nuclear facility. The second applies STPA methods to the case study of *Deepwater Horizon* in Appendix A to reveal where, in a SCS, such critical gaps due to tacit knowledge might occur.

5.4.4.1 Solution 1 to Problem 5: Use EPRI Knowledge Elicitation Methods

EPRI performed a project to capture undocumented (tacit) task knowledge (EPRI 2004). 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. 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.

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. 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 was the knowledge representation. In several cases the expert wanted a few days to review and revise the knowledge representation. In the cases at the fossil plant, the expert on buried pipe location and the expert on part diagrams agreed to spend more time documenting their knowledge before retiring. As mentioned earlier, the interviewer had experts tell him, or he inferred, they did not want to provide their expertise because they wanted to come back as a consultant following retirement. They 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 raise they thought they deserved.

Others felt honored to be recognized as an expert, or felt it was their job to do what the organization wanted. Overall, most experts were cooperative. Only a few resisted cooperating.

5.4.4.2 *Solution 2 to Problem 5: Application of STPA: Negative Pressure Test During Deepwater Horizon.*

To illustrate the application of STPA, reference to the *Deepwater Horizon* case study will be utilized. In particular, the example of the negative pressure test, a critical element of the process, will be described.

The source for this example is Boebert and Blossom (2016). This source reflects a detailed examination, from a systems engineering perspective, of the volume of evidence including governmental hearings and legal proceedings. In those hearings, it became clear that, although the negative pressure test was a central component, it had never been formally documented as a written procedure. Primary evidence for how it was supposed to work was obtained by interviewing an experienced Well Site Leader (WSL) who had been responsible for the test in the past, but was unfortunately absent from the rig during the explosion. The present description will be somewhat simplified but will be based on information in Boebert and Blossom (2016; pp. 33, 68-77).

The context for this analysis is a deep undersea oil well, where hydrocarbons have been discovered. The exploratory phase is completed, and the drilling rig's task is to safely cap the well and remove its drilling equipment. The expectation is that a production rig will open the well at a later time and extract hydrocarbons.

The basic structure of the well from the rig downward includes a riser going from the rig to the head of the well. The well is capped by a Blowout Preventer (BOP). The drill pipe goes through the riser and BOP into the well. A second pathway, the Kill Line, goes from the rig to the well, entering just below the BOP. The well head and BOP are close to the seabed 5,000 feet from the surface. The majority of the well is below the seabed, ending at a depth of 18,200 feet.

From a STAMP perspective, the well is a controlled system. Pressure from the earth on the hydrocarbons at the bottom of well tends to force fluids upward, leading to a possible blowout. This pressure must be opposed by a heavier substance, drilling mud, during drilling operations, and by a combination of mud and cement barriers when the well is sealed. The negative pressure test is expected to be an indicator of the state of balance.

The point at which the analysis scenario begins is when the well is sealed at both ends. A so-called negative pressure test is performed in which a channel to the sealed well is opened, and observed for evidence of failure of the seal. This is labeled a negative pressure test since it is the absence of positive signs (either observed flow of fluid or increase in pressure readings) which leads to the conclusion that the well is intact.

In this case, the negative pressure test will be performed using the Kill Line. It is typical to use the Kill Line as an alternative source for pumping drilling mud in the well in the event of a potential blowout. The Kill Line has a lower valve operated by remote hydraulics, an upper valve which can be operated manually, and a pressure gauge. At this point, assume the Kill Line has been cleared of mud and the negative pressure test is ready.

Figure 24 depicts the SCS. The primary controller is the WSL. This depiction of the control structure includes the WSL mental model. Contents of the WSL mental model are inferred from presence/absence and/or sequence of selected control actions.

The mental model is updated by a direction, from higher authority, to commence the negative pressure test using the Kill Line. The Process State belief is that the Kill Line needs to open to the well. This triggers Control Action 1 – activating the hydraulics which open the lower valve. The Process Behavior belief is that the lower valve is now open. This triggers Control Action 2—opening the upper valve. The Process State Belief is that the Kill Line is now open to the well.

The Process Behavior belief is that it will take some estimated amount of time for the system to stabilize. After this time elapses, Control Action 3 – observe pressure gauge, and Control Action 4 – observe Kill Line outflow are triggered. If the pressure is zero and nothing is flowing out of the Kill Line, the test can be interpreted as indicating the well is under control.

However, there is one circumstance in which this negative pressure test cannot be trusted. If the hydraulic mechanism operating the lower valve is damaged, a spring-loaded mechanism will automatically close the valve. Unfortunately, no feedback signal indicating this has occurred is available by the operator. Therefore, if this knowledge is part of the Process Behavior of the operator, the operator's next control action would be to challenge the validity of the test, and suggest an alternative form of the negative pressure test, which is to use the drill pipe.

An additional set of problems is that of noise in the system. There are apparently marginal indications of pressure and/or flow which can be interpreted, within a given operator's set of process behaviors, as just anomalies. According to Bobert and Blossom (2019), this is what happened on *Deepwater Horizon*. A negative pressure test was employed using the Kill Line, but the possibility that the disruption which resulted in the blowout had also damaged the hydraulics to the lower valve, therefore resulting in a false negative pressure test, was never considered. There is also evidence that actual WSLs conducting the test were inexperienced, and did not possess the tacit knowledge regarding the details of the test as the experienced operator referred to above. There is evidence among staff sending emails just prior to the blowout expressing confusion regarding exact procedures for the negative pressure test. This example of *Deepwater Horizon* shows how STPA can be used to explain what went wrong, and explains the benefit of using STPA for NPP modernization.

5.4.5 Problem 6: Alignment/Misalignment of Existing Skills to New Technology

The advent of new technology will almost always imply critical issues in terms of how existing operators adapt to new demands. The extent to which this is an issue for any given case will, of course, be determined by where that on the Technology Centric Plant Operations Model (Figure 1) the organization falls. Presumably, a lower-level like-for-like replacement will have less impact than a complete transformation. Two alternative examples from past experience might be informative. The first is experience of commercial airlines moving from crews of three or four, to crews of two. This transition seemed to occur with very little problem; presumably because the crew members who were replaced were already licensed commercial pilots, and were able to move into flight crew positions. A second example, already referred to in Section 5.3.5, was the case of conversion automated paper production (Zuboff 1989). In this case, operators went from a very manual, noisy and dirty environment described as similar to large-scale cooking, to an office-like control room. The transformation in work demands was from direct manual manipulation of objects and processes, to abstract symbolic manipulation of these objects and process via computer input devices. For many of the workers, this was too extreme a transition. Others adapted to the technology and became so adept at understanding the possibilities of manipulation and simulation that they became threats to their supervisors, who were professional engineers.

Two rather different solutions to this problem will be proposed. The first could be considered as a programmatic top-down approach, while the second is very much bottom-up.

5.4.5.1 Solution 1 to Problem 6: Naikar's CWA to Training Needs

Naikar (2011, Ch.13) has described in detail work done for Australian Defense Organisation, which has similarities to cases of NPP modernization. This particular situation involved upgrading the capabilities of the F/A-18 multirole fighter aircraft. While this aircraft is flown by a single pilot, the change in functionality required the development of an enhanced instructional design system. The problem was approached by starting with the development of a WDA. As has been the case of previous discussion of WDA (see Sections 5.3.5.3 and 5.4.3.3), the system demands are characterized not in the form of tasks or procedures but of the functional structure of the work environments which places

constrains on the worker's (the pilot's) behavior. These constraints are event independent, such that the instructional design must reflect a capability of adapting to situations that are unanticipated.

Therefore, WDA resulted in a detailed functional model of the F/A 18 in its working environment. Each level of the means-end hierarchy generated constraints appropriate for that level. These constraints, in turn, generated potential training needs, and corresponding instructional system requirements. For example, the major constraints at the purpose-related function level were: (1) Flight, (2) Communication and Coordination, (3) Evaluation of Tactical Information, and (4) Weapons delivery to air and surface targets (Naikar 2011, Figure 11.3). Each of these constraints propagates into a training need, and an instructional system requirement. At the next level down (objective-related processes), the constraint, supersonic cruise, becomes a means of achieving the function purpose of flight. This generates its own set of training requirements.

This becomes a systematic way of insuring comprehensiveness of training needs. Embedded in this process includes the determination of knowledge, skills, and abilities (KSAs) required by analyzing task analysis of new systems against existing worker KSAs.

5.4.5.2 *Solution 2 to Problem 6: Learning from Incidents*

This solution reflects the contribution of resilience engineering (see also Sections 5.2.4 and 5.3.4.2). Resilience engineering is characterized less by specific methodologies than by a broad philosophy. Central among these is a critical view of traditional approaches toward human error (Woods et al. 2010) (Dekker 2011) (Hollnagel 2014). A common situation is the occurrence of an undesirable event considered serious enough that a root cause analysis is performed. Nuclear plants have or identify personnel who perform root cause analyses to identify the main or root cause of the event and contributing causes. For example, the root cause may be incorrect information in a procedure and a contributing factor may be the operator who did not detect the incorrect information. It is often the case that human error is identified as the root cause of the event. Corrective actions are identified and implemented to eliminate or reduce the probability of the same or a similar event occurring again. Resilience engineering has a deep skepticism toward this view. A close look finds that there is often a multifactorial network of circumstances which caused the negative outcome. In fact, the behavior—seen from the perspective of hindsight to be the cause of the incident—may well have been carried out successfully hundreds of times before by not only the individual, but his colleagues. One of the simplest but most effective methodologies of resilience engineering is the procedure of simply documenting the normal variability in processes which occur in daily work.

A classic study examined errors in air traffic controllers (Hollnagel and Altaberti 2001) (Dekker 2015, pp. 86-87). A team of behavioral psychologists worked with a team of air-traffic controllers who together developed a taxonomy of errors. However, when the air-traffic controllers who were observed creating the errors were interviewed, they strenuously objected to the classification. They effectively argued that what they were doing were not mistakes but deliberate attempts to manage an excessive workload, by, for example, delaying less critical decisions.

The 737 Max case study in Appendix A indicates a more nuanced approach is needed. In the 737 Max accidents, pilot error may have been a contributing factor, but other cockpit design and flight manual deficiencies contributed. Although Max pilots will be provided training, probably in flight simulators, changes will be made to software, instrumentation, and flight manuals.

In this context, the learning-from-incidents perspective has arisen from the demand of maintaining large internet-facing systems which are under constant pressure from not only deliberate threats (hackers), but also from the inherent complexity of the systems (Perrow 1984). Woods and Allspaw have summarized the human requirements and challenges necessary to keep these dynamic software networks robust and resilient despite their scale and complexity (Woods and Allspaw 2019). In this sense, Figure

12 is the knowledge representation of the cognitive work which needs to be done. Unlike traditional sociotechnical systems, the procedures are developed on the fly and rarely documented.

The learning-from-incidents approach is attempting to systematize the cognitive work. The approach proposes that actual incidents and, more importantly, near misses, be regarded as valuable opportunities for a learning organization. The philosophy of investigation can be summarized in a few principles. These principles, while developed in the context of high-pressure software maintenance, can be usefully applied to existing NPP practice (as in an operational experience review) but more importantly, during the emerging developing of increasingly automated processes. The following principles are taken from Allspaw 2019, but seem to reflect a general consensus within the community of practice:

- All incidents could have been worse: What are the things (people, actions, knowledge, etc.) that went into preventing them from being worse?
- Resilience: Proactive activities aimed at **preparing to be unprepared** – without an ability to justify it economically
- Sustaining the potential for future adaptive action when conditions change
- Something a system **does**, not what it **has**.

5.4.6 Problem 7: Integration of PTPG and Governance at all Levels of the System

This problem lies at the core of the Idaho National Laboratory approach to the Plant Modernization Pathway (Thomas 2019; Hunton and Thomas 2019), as discussed in Section 2.1. One solution to this problem has already been suggested in Section 5.3.2, which generalizes this problem to the basic unit of sociotechnical systems analysis (i.e., the work system). This solution is further amplified below. A second solution uses Work Domain and Control Structure Analysis to focus on joint optimization of work system components.

5.4.6.1 Solution 1 to Problem 7: Map Components into Work System Framework

As stated in Section 5.3.2, the PTPG components making up key dimensions of the Plant Modernization Pathway can be mapped into the more general Macroergonomics concept of work system. Work systems, in turn, can be viewed as the basic unit of sociotechnical systems. A fundamental principle of effective work systems is that of joint optimization. That is, no single component of the work system should be emphasized at the expense of the others. As such, as shown in Figure 25, joint optimization strives to achieve the goals of resilience engineering (Hollnagel 2006), which is a balance among the high level organization objectives of effectiveness (mission accomplishment), efficiency (optimum use of resources), and safety (avoidance of injury or damage).



Figure 25. Mapping PTPG into the work system.

The practical task of achieving joint optimization has been described in terms of three high level problems: knowledge representation, knowledge acquisition, and cross-functional integration (see Section 5.3.3). In terms of the Plant Modernization Pathway, these problems must be solved to answer the following three question which make up the vertical dimension of the Capability Development diagram in Figure 10, Section 5.3.2:

1. What do we need?
2. What existing resources can be used?
3. What new resources need to be developed?

The case studies in Appendix A provide examples of what can happen when joint optimization is **not** embedded in upper management higher-level goals and priorities. In the case of the USS *McCain*, new technology was rushed to implementation without adequate time or resources for formal training and/or familiarization. As a result, an advanced mechanism for engine control was implemented by the Captain in a mode for which there was not only no prior training, but the documentation needed for the system was not even available on the ship. It was the unfamiliarity with these controls that ultimately resulted in the collision.

In the case of *Deepwater Horizon*, the evidence is that a combination of factors contributed to the accident, each of which was an indication of lack of joint optimization. Extreme emphasis on speed and deadline pressure were combined with lack of technical supervision from the management level, which resulted in hastily drawn up plans involving combinations of unusual approaches. As indicated in Section 5.4.4.2, in one critical procedure, the test methodology was based on the tacit knowledge of a key employee who was missing at the time of well explosion.

The pilots of the Boeing 737 MAX who were involved in the two fatal crashes, like the crew of USS *McCain*, were untrained on a key control system and were unaware of what the automation was doing. Here again, high level time and cost-cutting pressures, led a documented shortcuts in traditional engineering practice.

A general observation across all three of these cases goes back to the issues discussed in Problems 1-3. The successful accomplishment of NPP modernization will require sustained management commitment over many years. Lapses in that commitment, as reflected in changes high level goals and priorities, percolate down to lack of operational discipline at lower levels, which can be catastrophic in safety-critical systems. Dekker (2011) has labeled this effect “Drift to Failure.”

5.4.6.2 *Solution 2 to Problem 7: Focus on Joint Optimization of Work System Components*

The formulation of a capability within the Modernization Pathway framework (see Section 5.3.2), requires synthesis of the four dimension of PTPG with the three questions: (1) What do we need? (2) What existing resources can be used? and (3) What new resources need to be developed? To address this synthesis within the joint optimization framework of work systems, three problems: Knowledge Acquisition, Knowledge Representation, and Cross-Functional Integration, need to be addressed. The knowledge representation problem can be approached through a combination of WDA, and the Control Structure component of STPA.

Specifically, for a given capability, WDA can provide a formative representation of the problem space that indicates what **should** be present for the capability to be realized. This allows for an answer to the “What do we need?” questions at various levels of abstraction (see Section 5.4.3.3 for a detailed example). The advantage of a WDA is it makes explicit the relationship between high level values and priorities as they percolate down to actual physical requirements. In general terms, these relationships are described as Why → What → How. It should be emphasized that applying this kind of hierarchical questioning does not require a formal WDA but can be usefully applied in many settings.

Once this representation is developed, the remaining questions—existing resources and new resources—need to be answered. In this case, a possible use of WDA would be to use WDA not in a formative, but in a descriptive, fashion to create a representation of existing resources. The difference between the two representations would be a map of what new resources would be required.

In Section 5.4.3.3, it was emphasized that the formative WDA was independent of specific events or actions but depicted a space of possibilities. As such, this is only a first step. In CWA (see Section 4.1.3.2) the next step is typically Control Task Analysis, which provides an assessment of actions on the work domain. However, STPA, which could logically be considered an outgrowth of CWA, provides an alternative analysis. Specifically, the control structure analysis of STPA provides a useful examination of control and feedback relationships among both humans and machines, viewed in the same framework. See Sections 5.3.4.3, 5.3.4.4, and 5.4.4.2 for detailed examples.

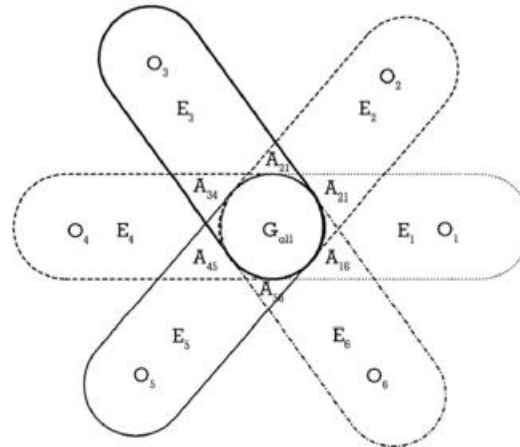
Finally, this discussion is focused in the Knowledge Representation problem. See Section 5.3.5 for examples of dealing with the Knowledge Elicitation and Cross-Functional Integration.

5.4.7 Problem 8: The Silo Problem

Problem 8 is essentially about how one can bring the different stakeholder groups into agreement on communicating, sharing information, and getting agreement on common priorities that cut across groups. A key theoretical concept in dealing the with practical questions of organizational silos is that of shared (or conflicting) mental models. This has been discussed at various points in previous sections, but the following knowledge representation of the problem, based on the work of (Cronin and Weingart 2007), might prove useful. Each oval represents an individual in a group. If the group is functioning as a team, overall goals (G) are shared by all members of the team. Some assumptions (A) are shared only by a subset of the team for whom they matter. Other components (O, E) are unique to each individual.

The problem of reducing silos in terms of shared mental models is to ensure that all participants at least have G components in common, and participants who share subinterests have A components in common.

Shared Mental Models



Note: Ovals represent each individual's representation. Operators (O) and elements (E) are unique to individuals, assumptions (A) are shared between those for whom they matter, and goal hierarchy (G) is shared by all.

Figure 26. Shared mental models (Cronin and Weingart 2007).

5.4.7.1 *Solution to Problem 8: Modified IDEAS with NGT*

This solution involves modifying IDEAS with NGT in step 1 to ensure all concerns are verbalized. There are two practical objectives in the process of creating consensus among members of cross-functional teams. The first is to ensure that every member has an equal opportunity of participation in discussion and group decision-making. The second is to structure the discussion in such a way that individual contributions to the discussion are perceived as property of the group. The purpose of this is for all members of the group to feel they have ownership of the group product. There is an obvious issue of rewarding specific individuals for their contributions, but this should be considered an individual interaction between employee and supervisor, independent of group process. That is, a given individual might have a well-conceptualized idea rejected by the group, but be rewarded by his/her supervisor.

A well-established mechanism for achieving these goals is NGT. This can be used alone (see Section 5.3.5.2, and Appendix A). It can also be combined with the modified IDEAS technique to provide a more formal structure to the process (see Section 5.4.3.1)

6. Summary, Conclusions, and Recommendations

6.1 Summary

The origins of this project, from which this report is a product, is the Plant Modernization Pathway of the DOE) LWR Strategic and Action Plan (Thomas and Hunton 2019). This plan lays the groundwork for a digital transformation of the nuclear industry. The model for this transformation is an advanced concept of operations, with an end point vision as follows:

To achieve the maximum aggregate benefit enabled by this digital transformation, the digital infrastructure for a nuclear plant must be designed as an integrated set of systems that together enable a technology centric operating model (p. 3).

Designing and operating such an 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 will be needed to percolate downward to the level of systems engineering in design and operations. For this effort to succeed a strict discipline is required for the coordination of multiple tightly coupled functions. This type of commitment has been described as Quality Management (see Section 5.4.2.1 and Appendix A) or alternatively, a combination of safety culture and engineering culture (see Section 4.1.8 and Appendix A). This discipline is required to ensure that all stakeholders in the systems engineering process are participating in a coordinated manner.

The goal of this report has been to facilitate and enable such coordination. Building on a traditional HFE foundation, this report employs a human and organizational factors approach to the broad area of sociotechnical systems. A literature review of the applicable sociotechnical systems literature focused on possible tools and methods which might be applicable to the NPP modernization problem. This search, which included the areas of CSE, STAMP, human systems integration, and Macroergonomics, 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.

The outcome of this effort is the development of a strategic framework for the effective integration of human and organizational expertise within NPP digital modernization efforts.

The basic unit of sociotechnical systems analysis is conceptualized as the concept of work system (Figure 25.) According to Macroergonomic theory, a work systems contains three components, Personnel, Technical, and Organization and Management. As discussed in Section 5.4.6.1, the four dimensions identified in the capability building framework of the Plant Modernization Pathway – PTPG (Thomas 2019) can be mapped into the three components of the work system. In an effective work system, these three components are jointly optimized. Per Hollnagel (2009), joint optimization can be operationally defined in the language of resilience engineering, in terms of an interdependence among the three major systems performance criteria: effectiveness (accomplishment of mission), efficiency (optimization of resources), and safety (avoidance of injury, damage). Excessive emphasis on any one criterion to the exclusion of others will, in all likelihood, over the long run to lead to system failure. The case studies in Appendix A relating to Boeing 737 MAX, *Deepwater Horizon*, and USS *McCain* present evidence of such examples where 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 information which is represented is obtained from those who have the required expertise), and Cross-Functional Integration (how information can be enabled to flow freely between groups and help support collaboration and prevent silos).

Knowledge Representation, Knowledge Elicitation, and Cross-Functional Integration, which are discussed in detail in Section 5.3, can be considered high level human and organizational factors functions. These functions are applied to a set of practical NPP problems in Section 5.4. The intention is for these functions to be used to enhance the practical work of stakeholders in NPP modernization design and operation in the same way that traditional HFE enhances the practical work of control room operators (see Section 3).

While the suggested solutions to problems posed in Section 5.4 will typically involve a combination of all three functions, for the purposes of elucidation, the dominant function will be identified in the following description:

- Problems 1 and 2. Top management consensus and the need for core values:
 - Solution 1. Cross-Functional Integration
 - Solution 2. Knowledge Representation and Knowledge Elicitation
- Problem 3. Top management core values:
 - Solution 1. Knowledge Representation and Cross-Functional Integration
- Problem 4. HFE program management:
 - Solution 1. Knowledge Elicitation and Cross-Functional Integration
 - Solution 2. Knowledge Representation
- Problem 5. Obtaining tacit (undocumented) knowledge:
 - Solution 1. Knowledge Elicitation
 - Solution 2. Knowledge Representation
- Problem 6. New skills and capabilities of current employees:
 - Solution 1. Knowledge Representation
 - Solution 2. All three functions
- Problem 7 involves PTPG integration:
 - Solution 1. Knowledge Representation
 - Solution 2. Knowledge Representation
- Problem 8. The silo problem:
 - Solution 1. Cross-Functional Integration.

The overall strategic integration framework is presented in Figure 27 as a concept map. This report is produced using cmap tools (cmap.ihmc.us). See Section 5.3.7.



Figure 27. Strategic Integration Framework presented as a concept map.

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 usability criteria (Naikar 2009) discussed in Section 5.4. 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.

Ultimately, NPP modernization is an activity carried out by human beings interacting with technology within an organization and its management. The intent of this report is to provide tools and methods to

optimize that interaction. These tools and methods are an extension of those already available to optimize the interaction of NPP control room operators.

6.2 Conclusions

- Utilities are and will be modernizing their NPPs. 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.
- Human and organizational expertise have been shown to be important contributors to successful transformation programs, such as the USS *Zumwalt* naval ship design (Appendix A), and the improvement in TQ at a nuclear fuel fabrication facility (Appendix A).
- Human and organizational factors that should be considered for digital transformation projects include sociotechnical systems (CSE, STAMP, human systems integration, and Macroergonomics) for effective integration of human and organizational expertise efforts within NPP digital modernization.
- The work system is the basic unit of sociotechnical systems analysis and contains three components: (a) personnel, (b) technical, and (c) organization and management. These components should be jointly optimized with respect to the interdependence of systems performance criteria of effectiveness, efficiency and safety.
- Joint optimization can be achieved through the application of three human and organization functions: knowledge representation, knowledge elicitation, and cross-functional integration.
- This report provides a strategic framework for effective integration of human and organizational expertise within NPP digital modernization efforts.

6.3 Recommendations

- The human and organizational strategic framework presented in this report should be applied at NPPs that are planning a technology centric modernization effort. This application will 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.
- The human and organizational strategic framework should be integrated into the Plant Modernization Pathway of the DOE LWRs Strategic Action Plan and Technology Centric Plant Operations Model.
- The human and organizational strategic framework should be considered a logical extension of traditional HFE, with application beyond control room operation to the design process itself.

7. References

- Allspaw, J. (2019). *Amplifying sources of resilience: what research says*. InfoQ Presentation. <https://www.infoq.com/presentations/resilience-thinking-paradigm/>
- Bennett, K. B., and Flach, J. M. (2011). *Display and Interface Design*. CRC Press. <https://doi.org/10.1201/b10774>
- Bisantz, A. M., and Burns, C. M. (2009). *Applications of cognitive work analysis*. CRC Press.
- Boebert, E., and Blossom, J. M. (2016). *Deepwater horizon*. Harvard University Press.
- Booher, H. (2003). *Handbook of human systems integration*. Wiley.
- Burns, C. M., and Hajdukiewicz R., J. (2004). *Ecological Interface Design*. CRC Press.
- Calingo, L. (2002). The U.S. Malcolm Baldrich National Quality Award: Recent Developments, Processes, and Applicability to the Asian Setting. In *The Quest for Global Competitiveness through national quality and business excellence awards*. Asian Productivity Organization.
- Carayon, P., Hancock, P., Leveson, N., Noy, I., Szelwar, L., and van Hootegeem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics*, 58(4), 548–564. <https://doi.org/10.1080/00140139.2015.1015623>
- Cook, R. (2019). Above the line, below the Line. *ACMQueue*, noember-december, 41–51. <https://doi.org/10.1215/9780822394136>
- Crandall, B., Klein, G., and Hoffman, R. (2006). *Working minds: A practitioner's guide to cognitive task analysis*. MIT Press.
- Cronin, M., and Weingart, L. (2007). Representational gaps, information processing, and conflict in functional diverse teams. *Academy of Management Review*, 32(3), 761–773.
- Czaja, S. J., and Nair, S. (2012). Human factors engineering and system design. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (4th ed., pp. 38–56). Wiley.
- Dainoff, M.J. (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). <https://doi.org/10.1080/10447310902864944>
- Dainoff, M.J. (2017). A sociotechnical approach to occupational safety. *Work*, 56(3). <https://doi.org/10.3233/WOR-172500>
- Dainoff, M J, and Mark, L. S. (2001). Affordances. In W. Karwowski (Ed.), *Encyclopedia of Ergonomics*. Taylor and Francis.
- Dainoff, Marvin J. (2006). HFES Past, Present, and Future: Presidential Address. *50th Annual Meeting of the Human Factors and Ergonomics Society*.
- Dekker, S. W. A. (2011). *Drift into failure: from hunting boken components to understanding complex systems*. Ashgate.
- Dekker, S. W. A. (2015). *Safety differently*. CRC Press.
- Delbecq, A. L., Van de Ven, A. H., and Gustafson, D. H. (1986). *Group techniques for program planning : a guide to nominal group and Delphi processes*. Green Briar Press.
- Desaulniers, D. R., and Fleger, S. (2019). IEEE Human Factors Standards for Nuclear Facilities: The Development Process, Available Standards, Current Activities, and the Future. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 63(1), 587–591. <https://doi.org/10.1177/1071181319631374>

- Dul, J., Bruder, R., Buckle, P., Carayon, P., Falzon, P., Marras, W. S., Wilson, J. R., and van der Doelen, B. (2012). A strategy for human factors/ergonomics: Developing the discipline and profession. *Ergonomics*. <https://doi.org/10.1080/00140139.2012.661087>
- Durso, F. (1999). *Handbook of applied cognition*. John Wiley and Sons Ltd.
- Elm, W., Gualtieri, J., Tittle, J., Potter, S., and Mckenna, B. (2009). Pragmatic Use of Cognitive Work Analysis in System Design Extending Current Thinking by Adapting the Mapping Principle. In A. M. Bisantz and C. M. Burns (Eds.), *Applications of Cognitive Work Analysis* (pp. 249–274). CRC Press.
- EPRI. (2015). *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification*. EPRI report 3002004310.
- EPRI. (2004). *Real Time Expert Knowledge Acquisition and Transfer* EPRI Report 1009581.
- EPRI. (2012). *Program on Technology Innovation : Decision-Centered Guidelines for the Design of Human System Interfaces for Electric Power Industry Applications: EPRI Report 10255791*.
- EPRI. (2018a). *Digital Engineering Guide: EPRI Report 3002011816*.
- EPRI. (2018b). *Hazards and Consequences Analysis for Digital Systems*. EPRI Report 3002012755.
- Flach, J.M., Carroll, J. S., Dainoff, M. J., and Hamilton, W. I. (2015). Striving for safety: communicating and deciding in sociotechnical systems. *Ergonomics*, 58(4). <https://doi.org/10.1080/00140139.2015.1015621>
- Flach, John M., and Verhoorst, F. A. (2020). *A Meaning Processing Approach to Cognition: What Matters?* Routledge.
- Forbes, J., Gibson, M., Pritchett, J., and Hanes, L. F. (2012). Application of HFE to support Turbine Control System (TCS) upgrade. *8th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies 2012, NPIC and HMIT 2012: Enabling the Future of Nuclear Energy, 1*, 464–475.
- France, M. E. (2017). *Engineering for Humans: A New Extension to STPA Signature of Author*. Massachusetts Institute of Technology.
- Gibson, J. J. (1979). *The Ecological Approach to Visual Perception*. Houghton Mifflin.
- Goldenhar, L. M., LaMontagne, A. D., Katz, T., Heaney, C., and Landsbergis, P. (2001). The Intervention Research Process in Occupational Safety and Health: An Overview From the National Occupational Research Agenda Intervention Effectiveness Research Team. *Journal of Occupational and Environmental Medicine*, 43(7), 616. <http://10.0.4.73/00043764-200107000-00008>
- Goncalves Filho, A. P., and Waterson, P. (2018). Maturity models and safety culture: A critical review. *Safety Science*, 105(March 2017), 192–211. <https://doi.org/10.1016/j.ssci.2018.02.017>
- Grant, E., Salmon, P. M., Stevens, N. J., Goode, N., and Read, G. J. (2018). Back to the future: What do accident causation models tell us about accident prediction? In *Safety Science* (Vol. 104). <https://doi.org/10.1016/j.ssci.2017.12.018>
- Hanes, L. F., Fink, R., and Naser, J. (2015). Human-automation function allocation. *9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2015*, 2, 1313–1325.
- Hendrick, H. W., and Kleiner, B. M. (2011). *Macroergonomics: an introduction to work system design*. Human Factors and Ergonomics Society.
- Hoffman, R., and Moon, B. (2010). Knowledge capture for the utilities. *Seventh Annual Nuclear Society*

International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technologies NPICandHMIT 2010.

- Hollnagel, E. (2006). Resilience – the challenge of the unstable. In *Resilience Engineering: Concepts and Precepts*.
- Hollnagel, E. (2014). *Safety-I and safety-II : the past and future of safety management*. CRC Press.
<https://www.taylorfrancis.com/books/e/9781315607511>
- Hollnagel, E., and Altaberti, R. (2001). The emperor's new clothes; Or whatever happened to "human error." *Fourth International Workshop on Human Error, Safety, and Systems Development*.
- Hollnagel, E., and Woods, D. D. (2005). Joint cognitive systems: Foundations of cognitive systems engineering. In *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*.
- Hollnagel, E., Woods, D. D., and Levenson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Ashgate.
- Huang, Y.-H., Jeffries, S., Tolbert, G. D., and Dainoff, M. J. (2017). Safety climate: What you can learn, what you can do--safety climate surveys for lone workers. *Professional Safety, January*, 28–35.
- Hunton, P. J., and England, R. T. (2019). *Addressing Nuclear I&C Modernization Through Application of Techniques Employed in Other Industries*. INL/EXT-19-55799, Idaho National Laboratory, Idaho Falls, ID.
- IEEE. (1979). *First IEEE Conference on Human Factors in Nuclear Power Plants*, Myrtle Beach, NC.
- IEEE. (2004). *IEEE Standard 1023-2004: Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities*.
- INPO. (2009). *INPO Good Practice INPO 09-004 February 2009 Procedure Use and Adherence*.
- INSAG. (2002). *Key Practical Issues in Strengthening Safety Culture INSAG-15, IAEA*.
- Jenkins, D. P., Stanton, N. A., Salmon, P. M., and Walker, G. (2008). *Cognitive work analysis: Coping with complexity*. Ashgate.
- Joe, J. C., Hanes, L., and Kovesdi, C. (2018). *Developing a Human Factors Engineering Program Plan and End State Vision to Support Full Nuclear Power Plant Modernization*. INL/EXT-18-51212, Idaho National Laboratory, Idaho Falls, ID.
- Kirwan, B., and Ainsworth, L. K. (1992). A guide to task analysis: The task analysis working group. In *A Guide To Task Analysis: The Task Analysis Working Group*. Taylor and Francis.
- Klein, G., Calderwood, R., and Zsombok, C. (1993). *Decision making in action: Models and methods*. Ablex.
- Kleiner, B. M., Hettinger, L. J., DeJoy, D. M., Huang, Y. H., and Love, P. E. D. (2015). Sociotechnical attributes of safe and unsafe work systems. *Ergonomics*.
<https://doi.org/10.1080/00140139.2015.1009175>
- Lee, J., Huang, Y., Cheung, J. H., Chen, Z., and Shaw, W. S. (2019). A systematic review of the safety climate intervention literature: Past trends and future directions. *Journal of Occupational Health Psychology*, 24(1), 66–91. <https://doi.org/10.1037/ocp0000113>
- Leveson, N. (2011). *Engineering a Safer World*. MIT Press.
- Leveson, N. G., and Thomas, J. T. (2018). *STPA Handbook*.
http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

- Liberty_Mutual. (2016). *LIBERTY MUTUAL WORKPLACE SAFETY INDEX*.
[https://business.libertymutualgroup.com/business-insurance/Documents/Services/Workplace Safety Index.pdf](https://business.libertymutualgroup.com/business-insurance/Documents/Services/Workplace%20Safety%20Index.pdf)
- Lintern, G. (2009). *The Foundations and Pragmatics of Cognitive Work Analysis: A Systematic Approach to Design of Large-scale Information Systems*. Lintern, G. <http://www.cognitivesystemsdesign.net/>
- McGrew, J. F. (2016). Proceedings of the Human Factors and Ergonomics Society. *Proceedings of the Human Factors and Ergonomics Society*, 367–371.
- Militello, L. G., and Hutton, R. J. (1998). Applied cognitive task analysis (ACTA): a practitioner's toolkit for understanding cognitive task demands. *Ergonomics*, 41(11), 1618–1641.
<https://doi.org/10.1080/001401398186108>
- Mitchell, M. (2009). *Complexity : a guided tour*. Oxford University Press.
- Mitchell, M. (2019). *Artificial intelligence : a guide for thinking humans*. Farrar, Straus, and Giroux.
- Naikar, N. (2009). 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 A. M. Bisantz and C. M. Burns (Eds.), *Applications of Cognitive Work Analysis*. CRC Press.
- Naikar, N. (2013). *Work domain analysis: Concepts, guidelines, and cases*. CRC Press.
- Naikar, N., Pearce, B., Drumm, D., and Sanderson, P. M. (2003). Designing teams for first-of-a-kind, complex systems using the initial phases of cognitive work analysis: Case study. *Human Factors*.
<https://doi.org/10.1518/hfes.45.2.202.27236>
- NEA/IAEA. (2006). *Proceedings of the Workshop on Future Control Station Designs and Human Performance Issues in Nuclear Power Plants NEA/CSNI/R(2007)8*.
- NEA/IAEA. (2012). *Oversight and Influencing of Licensee Leadership and Management for Safety, Including Safety Culture – Regulatory Approaches and Methods NEA/CSNI/R(2012)13* (Issue September 2011).
- Neilsen, K., and Randall, R. (2013). Opening the black box: Presenting a model for evaluating organizational-level intervention. *European Journal of Work and Organizational Psychology*, 22(5), 601–617.
- Norman, D. A. (1988). *The psychology of everyday things*. Basic Books.
- Norman, D. A., and Draper, S. W. (1986). *User centered system design*. Earlbaum Associates.
- NRC. (2004). *Human factors engineering program review model NUREG 0711-Rev 2*.
<http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA488603>
- NRC. (2011). *NRC Safety Culture Policy Statement (76 FR 34773)*. <https://www.nrc.gov/about-nrc/safety-culture/sc-policy-statement.html>
- Perrow, C. (1984). *Normal accidents: Living with high risk technology*. Basic Books.
- PPA. (2011). *Procedure Professionals Association (2011) Procedure Writers' Manual, PPA AP-907-005, Rev 1*.
- Rasmussen, J., Pejtersen, A. M., and Goodstein, L. P. (1994). *Cognitive Systems Engineering*. Wiley.
- Reiman, T., and Rollenhagen, C. (2014). Does the concept of safety culture help or hinder systems thinking in safety? *Accident Analysis and Prevention*, 68. <https://doi.org/10.1016/j.aap.2013.10.033>
- Robertson, M., Henning, R., Warren, N., Nobrega, S., Dove-Steinkamp, M., Tibirica, L., and Bizarro, A.

- (2013). 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 SUPPL.), 86–88. <https://doi.org/10.1097/JOM.0000000000000036>
- Robertson, M. M., and Courtney, T. K. (2004). A systems analysis approach to solving office work system health and performance problems. *Theoretical Issues in Ergonomics Science*, 5(3), 181–197. <https://doi.org/10.1080/1463922021000032320>
- Robertson, M. M., and Tubbs, D. (2016). Organizationa readiness for change: A systematic literature review and field experience as related to safety and wellness improvements at work. *European Academy of Management Annual Meeting*.
- Ropohl, G. (1999). Philosophy of socio-technical systems. *Techné: Research in Philosophy and Technology*, 4(3), 186–194.
- Roth, E. M. (2008). Uncovering the requirements of cognitive work. In *Human Factors*. <https://doi.org/10.1518/001872008X288556>.
- SAE. (2019). *Applying System Theoretic Process Analysis (STPA) to Automotive Applications SAE J3187 Work in progress*.
- Simons, K. J., Dainoff, M. J., and Mark, L. S. (2006). The Work Process of Research Librarians, Elicited via the Abstraction-Decomposition Space. In *Advances in Library Administration and Organization* (Vol. 24). [https://doi.org/10.1016/S0732-0671\(06\)24006-9](https://doi.org/10.1016/S0732-0671(06)24006-9)
- Thomas, K. (2019). Plant Modernization Pathway: Integrated Operations for Nuclear Capability Development. *LWRS Reactor Sustainability, INL*.
- Thomas, K. D., and Hunton, P. J. (2019). *Nuclear Power Plant Modernization Strategy and Action Plan*. INL/EXT-19-55852, Idaho National Laboratory, Idaho Falls, ID.
- Trent, S. (2019). Transforming the DOD with human-centered AI. *Human Factors and Ergonomics Society Annual Meeting*.
- Verma, S. K., Chang, W. R., Courtney, T. K., Lombardi, D. A., Huang, Y.-H., Brennan, M. J., Mittleman, M. A., Ware, J. H., and Perry, M. J. (2011). A prospective study of floor surface, shoes, floor cleaning and slipping in US limited-service restaurant workers. *Occupational and Environmental Medicine*, 68(4), 279 LP – 285. <https://doi.org/10.1136/oem.2010.056218>
- Vicente, K. J. (1999). *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. Lawrence Erlbaum Associates.
- Waterson, P., Robertson, M. M., Cooke, N. J., Militello, L., Roth, E., and Stanton, N. A. (2015). Defining the methodological challenges and opportunities for an effective science of sociotechnical systems and safety. *Ergonomics*, 58(4), 565–599.
- Woods, D. D. (1991). The cognitive engineering of problem representation. In G. Weir and J. Alty (Eds.), *Human-computer interaction and complex systems*. Academic Press.
- Woods, D. D., and Allspaw, J. (2019). Revealing the critical role of human performance in software. *Queue*, 17(6), 1–13. <https://doi.org/10.1145/3380774.3380776>
- Woods, D. D., Dekker, S., Cook, R., Johannesen, L., and Sarter, N. (2010). *Behind Human Error* (2nd Ed.). Ashgate.
- Zohar, D. (1980). Safety climate in industrial organizations: Theoretical and applied implications. *Journal of Applied Psychology*, 65(1), 96–102. <https://doi.org/10.1037/0021-9010.65.1.96>
- Zuboff, S. (1988). *In the age of the smart machine : the future of work and power*. Basic Books.

Appendix A

Exemplary Case Studies

A.1 Zumwalt Class of U.S. Navy Destroyers



Figure A-1. The *USS Zumwalt*.

The *Zumwalt* class of U.S. Navy guided-missile destroyers comprises three recently constructed ships (*USS Zumwalt*, *USS Michael Monsoor*, *USS Lyndon B. Johnson*). The class is characterized by radical departures from legacy destroyer designs in terms of fundamental naval architecture, and combat and support systems design. Most notably, the class (hereafter referred to as *Zumwalt*), required to significantly outperform legacy destroyers, was designed with two major system constraints in play:

- A requirement for a “stealth” design (specifically, a significantly reduced radar signature) led to breaks in traditional ship design (e.g., the location and design of the bridge) that required new technologies and crewing concepts to accomplish critical tasks.
- A Key Performance Parameter of a crew size of no greater than 95 personnel (excluding the air detachment).

Zumwalt was the first ship design that the USN approached from an explicitly ‘sailor-centric’ (as opposed to ‘engineering-centric’ perspective) (Hagan et al. 2011). Throughout the design, a significant role was played by a team of human-systems integration professionals whose responsibilities included requirements generation, cognitive and physical workload analysis, systems design and test, modeling and simulation, etc.

There are several key aspects of the *Zumwalt* design process that are of particular relevance to the nuclear modernization domain, including:

- The integration of human-systems integration processes within a traditional, systems engineering paradigm was largely successful, but required enormous initial effort, strong leadership and an ability to “speak the language” of systems engineering. Bringing together key stakeholders (sailors, designers, engineers, etc.) at each phase of the design and extracting their relevant expertise for incorporation into the design was one of the human systems integration team’s key activities.
- Development of a spreadsheet-based tool (the Manning Uncertainty Issues List) used to monitor the level of risk associated with the various novel technical systems—most involving automation, expert

systems, remote sensing, etc.—upon which the limited crew size concept relied. The Manning Uncertainty Issues List proved to be a highly effective tool for tracking risk and conveying its implications for the manning concept to program decision-makers.

There have been recent increases in the size of *Zumwalt*'s crew that are reportedly related to damage control issues involved in the ship's autonomic fire suppression system as well as the performance of several other systems supported by automated and remote sensing technologies. Organizational pressures on the design, a significant presence throughout, have also had an impact on crew size growth, such as additional personnel assigned to the crew to inspect areas of the ship—an activity already reportedly well-supported by remote sensing technology. The reduced crew concept also relies upon the concept of a centralized, shore-based maintenance facility for all ships in the class. This is an attempt to reduce the number of maintenance crew on each vessel and has thus far been largely successful and well-accepted by the fleet.

Zumwalt was a highly complex systems engineering effort and human systems integration had a significant impact both in terms of process and product. Several key commonalities between *Zumwalt* and nuclear modernization are:

- *Safety-critical system*—U.S. Navy warships are inherently safety-critical both in terms of the risk of the overall mission and in the potential risks to the personal safety and well-being of sailors and other personnel. Improving system safety and reliability are also generally viewed as key strategic, warfighting advantages and objectives.
- *High reliance on automation and remote sensing*—The significant reduction in crew size from legacy destroyers to *Zumwalt*, without sacrifice of operational capability, meant that enormous amounts of 'human workload' had to be replaced with automated and expert systems as well as remote sensing technologies for inspection and damage control.
- *Operational/life cycle costs*—A significant factor underlying *Zumwalt*'s design was a desire by the U.S. Navy to control the operational and life cycle costs associated with its surface warfare fleet. A major driver of these costs is manpower and therefore the Navy sought, through significant user of automation and integrated operations, to design a ship that could be a more cost-effective replacement of its legacy class.
- *Desire to leverage emerging technologies to replace human workload, improve safety and performance*—The emergence of new expert systems and automated technologies at the turn of the 21st century was a significant driver in the Navy's decision to explore the design and development of a highly automated ship.
- *Multiple stakeholders and significant government presence*—*Zumwalt*'s design incorporated inputs from over 1,000 sailors during its design as one means of ensuring a "sailor-centric" design. Additionally, inputs from across the breadth of the systems engineering team—which included multiple corporations and U.S. Navy agencies—were continually solicited and incorporated into the ship's design.
- *Reduced staffing and integrated operations*—Reducing the number of sailors onboard ships was, at the initiation of the *Zumwalt* program, a high-level U.S. Navy goal intended to support the more global objective of reducing overall costs of operation. Personnel costs (e.g., recruitment, training, retention, health costs, etc.) are by far the Navy's most significant budget item. As with the nuclear industry, reduced staffing through effective system design and integrated operations is seen as key to the Navy's future.
- *Operator fatigue*—A logical concern with reduced staffing is operator fatigue. Within the Navy, there are strong, cultural factors that can interfere with open, objective discussions of its risk factors. Fatigue and sleep-deprivation can be seen as "part of the job." To the extent this becomes an

organizational norm, systems can find themselves at increased risk of incidents commonly attributed to “human error.”

The *Zumwalt* design was intended to address many similar issues and opportunities currently confronting the nuclear power industry. Faced with a need to reduce operational costs associated with manning (i.e., staff size), the Navy pursued a highly novel, culturally disruptive design, heavily reliant on automation, remote sensing and other state-of-the-art technologies. The design process itself involved significant user input and a broad, human-systems integration focus that helped to counteract the effects of traditional systems engineering stovepiping.

Hagan, J., Crowe, K., Quintana, Q., Merenius, D., Browning, M. and Hettinger, L. (2011) Human-systems integration and crew design process development in the Zumwalt destroyer program. Special Report 306. Naval Engineering in the 21st Century, The Science and Technology Foundation for Future Naval Fleets.

A.2 Boeing 737 MAX



Figure A-2. The Boeing 737 MAX.

The Boeing 737 MAX is the fourth generation of the company's historically successful 737 airliner series. It succeeded the 737 NG and features a more fuel-efficient aerodynamic design, more efficient engines and other features. The 737 MAX entered commercial service in May 2017, remaining in service until its worldwide grounding in March 2019, following two fatal crashes that resulted in a total of 346 fatalities. A feature new to the 737 MAX, the Maneuvering Characteristics Augmentation System (MCAS) was identified as the key contributor to both accidents. MCAS is an automated system designed to improve aircraft handling characteristics and to decrease pitch-up tendencies at elevated angles of attack (e.g., stall conditions). Analyses of the accidents—both of which took place during take-off, pitch-up conditions—revealed that the flight crews had not received MCAS-specific training and, as implied through their unsuccessful attempts to control their aircrafts, were unfamiliar with its presence and its activities.

Each crew's apparent lack of awareness of the presence and behavior of a safety-critical, automated system appears to have been the most immediate contributor to both accidents. In the analyses and investigations following the two crashes, other design flaws have been uncovered. Additionally, significant focus has been devoted to the potential impact of Boeing's internal engineering culture as well as the company's relationship with the federal government, specifically the Federal Aviation Administration (FAA). The FAA, dealing with its own personnel shortages and budget cuts, had begun to cede some of its responsibility for what it considered routine verification of certain flight systems to Boeing. The FAA has also not wanted to be perceived as placing unnecessary impediments in the way of a critical industrial sector. While the testing involved was considered to be routine, the absence of direct FAA involvement has raised questions about the appropriate role of governed oversight in the design and test of safety-critical systems (New York Times, January 10, 2020).

Boeing's commercial aircraft sector has long been in widely-publicized competition with the few remaining companies in its business sector, notably Airbus. The 737 MAX was specifically designed to compete with the latest versions of the Airbus 320. Significant organizational, economic and business pressures were powerful drivers behind Boeing's design and roll-out of the 737 MAX. Their influence on activities such as systems engineering, design, test, production, marketing, support for training, etc. appears to have significantly influenced the conditions that contributed to the accidents.

As of January 29, 2020, estimated costs associated with the accidents, grounding, etc. are in excess of \$18B for Boeing, or about 20% of its annual sales. The company has also incurred significant reputational damage related to the trustworthiness of its processes and products, the long-term effects of which are yet to be determined.

Several key areas of potential overlap with nuclear modernization include the following:

- *Safety-critical system*—Commercial aircraft are responsible for transporting hundreds of thousands of people throughout the world each day. Crashes result in catastrophic loss of life, significant human suffering and enormous economic costs. They also incur significant reputational damage to airlines and aircraft manufacturers.
- *Competitive pressures and costs of staying in business*—The commercial aircraft design and manufacturing industry is enormously competitive and cost-sensitive. Competitive pressures naturally tend to lead organizations to look for ways to improve efficiencies within their internal operations, optimize delivery schedules and maximize profits. Occasionally, critical factors impacting system safety may suffer as a result.
- *Design and use of automation*—Most accounts of the two fatal accidents that have occurred to date have focused on the role played by the MCAS automated system. At this point in time the preliminary conclusion that the crews were (a) not aware of the presence or behavior of the malfunctioning automation, and (b) were put into a position of actively “fighting against” it in their unsuccessful attempts to regain control. This lack of transparency into the presence and activity of the automated MCAS appears to have been a significant flaw in the aircraft’s design.
- *Use of simulation*—In an attempt to gain a marketing edge in its promotion of the 737 MAX, Boeing informed potential customers that the design of the new aircraft was sufficiently similar to legacy models that 737 MAX-specific simulators would not be required—a significant cost savings. Unfortunately, this effectively shut off one means of familiarizing aircraft with the behavior of the new MCAS system.
- *Role of government agencies*—As mentioned above, the FAA has played something of a receding role in commercial aircraft system testing and verification. While still involved in the testing and verification of what it perceives to be the most critical systems, its own personnel and fiscal pressures have encouraged it to turn over responsibility for certain tests to the aircraft manufacturer. Additionally, the FAA reportedly does not wish to be an impediment to innovation in the aviation industry—a cultural pressure that may have impacted its decision-making regarding the 737 MAX.

While the Boeing 737 MAX experience has many potential lessons for the nuclear power industry, there are two in particular that stand out. The first is that the design of automation must never leave operators in a state of confusion about its behaviors in safety-critical situations and what, in return, is expected of them in terms of successful interactions and outcomes. Second, high-level management decisions, based heavily on legitimate, competitive concerns, were such that deficiencies in the design, test and roll-out of the system arose as a consequence.

New York Times, January 20, 2020, “‘I honestly don’t trust many people at Boeing’: A broken culture exposed.”

A.3 Deepwater Horizon



Figure A-3. The *Deepwater Horizon*.

On April 20, 2010, the floating drill rig *Deepwater Horizon* experienced a catastrophic explosion and fire, killing 11 crew members and injuring dozens more. While the locus of the specific failure mechanism(s) underlying the events is still uncertain and a matter of debate, the *Horizon*'s inability to prevent the escape of high-pressure hydrocarbon gas into the surrounding environment was ultimately the source of the catastrophe (Blossom 2016). The gas, having once escaped, was quickly ignited by an unknown source, leading to the conflagration.

Within 2 days of the explosion, the *Horizon* capsized and sank, one effect of which was to free the release of oil from the *Macondo* well underneath. The flow of oil into the Gulf of Mexico continued unabated until a temporary cap was successfully installed in mid-July. By that time, an estimated 4.9 million barrels of crude oil had spilled into the Gulf, almost 20 times the amount spilled in the *Exxon Valdez* accident, resulting in one of the worst ecological disasters in U.S. history. The economic impact of the accident is difficult to gauge, although the corporations involved incurred tens of billions of dollars in liability expenses and immense reputational damage. Additionally, the lives and livelihoods of hundreds of thousands of people in communities along the Gulf of Mexico were severely impacted.

There are many potential organizational and human-systems integration influences to consider in the case of the *Deepwater Horizon*. For instance, with regard to overall workplace safety there appears to have been a heavy emphasis on managing Occupational Safety and Health Administration (OSHA)-recordable accidents versus managing overall system safety—the lack of an effective “engineering culture” as noted in the discussion in the main text (see Section 4.1.8.3). Ironically, the rig’s crew received an award the morning of the explosion for having gone several months without an OSHA-recordable incident.

Significant competitive and economic pressures within the oil industry also had an impact on the accident. Tradeoffs between quotas, schedules and other metrics of production vs. operational safety is a common phenomenon in industry and these pressures were central to the *Deepwater Horizon* accident. Operator and equipment fatigue, use of comparatively unqualified personnel, deferred maintenance, etc. are all aspects of the productivity vs. safety tradeoffs underlying the *Deepwater Horizon* explosion.

Deepwater Horizon is an example of a complex sociotechnical system in which organizational and human-systems integration factors negatively influenced a catastrophic outcome. Several key commonalities between *Deepwater Horizon* and issues facing nuclear modernization are:

- *Safety-critical system*—As is the case with a NPP, the *Deepwater Horizon* is a highly safety-critical system. The accident resulted in significant fatalities and life-altering injuries as well as enormous environmental damage. The costs associated with a significant accident can be very high.
- *Competitive pressures and costs of staying in business*—The oil industry, extraction, refinement, delivery, etc., is a highly-competitive enterprise. Entities within the oil industry frequently seek competitive advantage by attempting to optimize staffing (i.e., number and type of employees) and streamline work processes, often by means of leveraging advances in automation, remote sensing and integrated operations.
- *Safety Focus*—A focus on managing OSHA-recordable injuries, while important, was maintained as opposed to a broader focus on overall system safety. This may be partially attributable to OSHA's focus on the former as opposed to the latter, thereby unintentionally encouraging an over-focus on that area.
- *Productivity vs. Safety tradeoffs*—Operating in a highly-competitive environment and uncertain global oil market, speed and efficiency became the most important objectives in the *Deepwater Horizon*'s activities prior to the accident. It is not uncommon for organizations to try to push the envelope of safe operations, whether consciously or not, in the pursuit of greater speed and efficiency.
- *Operator fatigue and system mental models*—Human operators on the *Horizon* were operating under conditions of chronic fatigue, which may have contributed to the decision-making and other activities that preceded the explosion. Additionally, a significant lack of correspondence between the operators' perceptions of the well status and activity and its true state—partially attributable to lack of training and effects of fatigue—clearly contributed to the accident.

The *Deepwater Horizon* disaster illustrates several general issues that are relevant to the nuclear power industry. Beyond relatively obvious ones, such as closely monitoring and managing operator and maintainer fatigue and overall fitness for duty, this accident especially illustrates the potentially deleterious effects of inadequate and/or mismatched mental models of system status and behavior among key personnel in safety-critical situations. The maintenance of accurate, shared mental models is a critical, multi-faceted design and management challenge involving domains such as human-system interface, training, personnel management, etc. Future nuclear systems design should explore potential means for enhancing this important aspect of human-system behavior.

Blossom, J.M. (2016). *Deepwater Horizon: A systems analysis of the Macondo Disaster*. Cambridge, MA: Harvard University Press.

A.4 USS John S. McCain Accident



Figure A-4. Damage sustained by the *USS John S. McCain* in its collision with the tanker *Alnic MC*.

On August 21, 2017, in the Straits of Singapore, the U.S. Navy destroyer *John S. McCain* was involved in a collision with the Liberian-flagged oil and chemical tanker *Alnic MC*. The collision resulted in 10 deaths and 48 injuries, all U.S. sailors. In addition to its casualties, the *McCain* sustained over \$100 million in damage and was rendered unable to fulfill its assigned missions (NTSB 2019).

The *McCain* had been attempting to overtake the *Alnic MC* when a loss of steering was experienced on the bridge, causing it to veer into the path of the oncoming tanker. Immediately preceding the loss of steering, the crew on the *McCain*'s bridge had been attempting a transfer of control of thrust and steering from one bridge control station to another, a potentially complicated task whose attempted execution under high-workload conditions (i.e., while the ship was in a congested waterway) appears to have contributed to the accident.

The National Transportation Safety Board report of the collision identified a number of factors that are potentially relevant to the design and operation of modernized nuclear power systems and operations. These include:

- *The decision to transfer the location of thrust control while in a congested waterway*—Executing potentially complex tasks under conditions of high workload can result in significantly increased system risk. Even adequately trained operators can find such procedures difficult. Sufficient and verified training, adequate interface design to support appropriate mental models of processes being executed and their status, and intelligent use of automation under conditions of high operator/system workload are among the potential system design lesson learned from this accident.
- *Lack of adequate communications between the McCain and Alnic MC*—Failures in communication, whether due to equipment, procedures, training or some combination of all three, are very commonly directly involved in serious accidents. In this case, some of the more critical communications failures occurred *between* the two systems (ships) involved. However, communications failures *within* individual systems (e.g., nuclear plants) can have similar consequences.
- *Operator fatigue*—While the *McCain* is not an “optimally-manned” vessel along the lines of *Zumwalt*, watchstander fatigue is still a major operational concern and, in this case, an apparent contributing factor to the accident. As previously noted, performing under conditions of acute or chronic fatigue has long been a feature of Naval culture—an example of a cultural norm clearly interfering with objectives of safe and effective system performance.

- *U.S. Navy oversight of the McCain*: The multiple factors contributing to the accident brought the U.S. Navy's overall assessment and certification processes into question. While the Commanding Officer has responsibility for assuring that watchstanders are properly trained and qualified, the Commanding Officer's superiors are responsible for certifying that the ship is safe to operate and that watchstander qualification procedures are adequate. The *McCain* accident illuminated significant, systemic shortcomings within the Navy regarding these factors.

The lessons of the *McCain* for NPP design and operation lay principally in the immediate circumstances surrounding the accident itself. Notably, the attempt to execute a complex, high-workload task under conditions of high external workload overtaxed the performance capabilities of the crew and supporting systems and led to the collision. A potential mitigation, one that has been successfully applied in numerous settings, is to conduct human-in-the-loop simulation testing of prototype system designs as representative operators perform routine and non-routine tasks under varying workload conditions. To be effective, this must be conducted as part of the design and acceptance phases of systems acquisition. At a broader level, the *McCain* accident is also a compelling example of the impact of the absence of sufficient high-level commitment to safe operations, including assessment and certification.

NTSB, 2019, *Collision between US Navy Destroyer John. S. McCain and Tanker Alnic MC, Singapore Strait, 5 Miles Northeast of Horsburgh Lighthouse, August 21, 2017*, Marine Accident Report 19/01, Washington DC: National Transportation Safety Board.

A.5 Westinghouse Commercial NFD TQ Program

The Westinghouse Commercial NFD established a TQ program around 1980 that resulted in it receiving the first Malcolm Baldrige National Quality Award in 1988. The Baldrige Award is the only Presidential national award for performance excellence, and is overseen by the National Institute of Standards and Technology (NIST). The American Society for Quality assists in administering the award program under contract to NIST.

This Case Study provides a brief description of the TQ program developed by the NFD that resulted in it receiving the Baldrige Award. The Case Study is based almost entirely on a description of the NFD Baldrige Award contained on the NIST and other websites. Recent information about the Baldrige Award is available on the internet. In addition, a brief description is provided near the end of the Case Study of three projects performed in support of the TQ program.

The NFD made fuel-rod assemblies that were installed in electric utility NPPs. The U.S. NRC on its web site provides the following definition of fuel-rod assemblies:

A structured group of fuel rods (long, slender, metal tubes containing pellets of fissionable material, which provide fuel for nuclear reactors). Depending on the design, each reactor vessel may have dozens of fuel assemblies (also known as fuel bundles), each of which may contain 200 or more fuel rods.

At the beginning of the NFD TQ program, it had been found that the fuel-rod assemblies had high reliability. A goal was then established of 99.995% reliability and the assemblies viewed as performing flawlessly. NFD top management realized that future business depended on continued excellence in product performance, and it needed to increase its all-important dependability rating even higher.

Prior to the early 1980s, the NFD quality goals were geared toward satisfying regulatory requirements for fuel-rod assemblies. Then, motivated by stiff competition and demanding customer requirements, it established the objective of being recognized as the world's highest-quality supplier of commercial nuclear fuel.

NFD used state-of-the-art technology, such as robotics and other automated processing equipment, supercomputer simulations, expert systems and laser-diagnostics, and laser welding. It estimated that quality-related decisions had dictated 75 percent of its capital allocations during recent years (through 1987). Management, however, attributed NFD's substantial improvements in quality and efficiency not so much to advanced technology as it did to a "turned on" work force and to NFD's TQ approach to operations.

NFD used a TQ approach built upon four imperatives for continuous quality improvement:

- Management leadership
- Product and process leadership
- Human resource excellence
- Customer satisfaction.

Progress was measured by a unique system called "Pulse Points." The system tracked improvements in over 60 key performance areas identified with statistical techniques and other evaluative tools, and it helped set measurable goals within each unit of NFD, down to the jobs of hourly workers.

The NFD built a quality culture that asked employees to do "the right things right the first time." This philosophy made every action by every employee a quality initiative. Customer satisfaction was the guiding principle, whether it was the ultimate customer or the next NFD person in the process.

Product and service improvements attributable to the seven-year old program paid business dividends. The value of new orders in 1987 was the highest in the decade. Existing customers accounted for more than 90 percent of the orders placed in 1987.

NFD TQ Program

Rather than having a chief quality officer, NFD assigned responsibility for directing and coordinating quality improvements to the general manager of each major organization and his various staff functions. These managers formed the NFD's Quality Council, which set policies, plans and strategies, and directed the quality improvement process. Management's rationale was that quality concerns must be fully integrated into all design, production, and customer service activities.

In strategic planning, top management developed formal quality initiatives and Pulse Points that were deemed most critical to improving performance and customer satisfaction. Supporting, measurable goals, all aimed at accomplishing divisional objectives, were developed in each of the departments and then for each worker. Progress was monitored through an extensive data-collection and trend-analysis system. Pulse Point trends were reviewed each month in a teleconference that included top management at each of three division sites.

A triangle was developed by NFD that identified conditions of excellence to fulfill TQ requirements (Figure A-5).

Workers directly addressed quality improvement opportunities and helped devise initiatives through their participation in project oriented teams. Nearly 1,400 of about 2,000 employees were members of 175 such teams in 1987. About 90% of all workers underwent quality awareness or quality-related training from 1984 through 1987.

NFD maintained close—usually daily—contact with its utility customers and regularly collected technical data to evaluate the performance of its fuel assemblies. Customer service plans were created for each client and were jointly reviewed each quarter. A customer's Fuel Users Group met twice a year to share information and discuss needs for new products. Consistently high scores in surveys and customer-conducted audits reflected high levels of satisfaction. A more telling indicator, however, was repeat business. Existing customers accounted for more than 90% of the orders placed in 1987.



Figure A-4. Triangle developed by NFD that identifies conditions of excellence to fulfill TQ requirements.

Although Westinghouse's eye was on the bottom line, NFD management deliberately did not include cost concerns in its quality improvement program, believing that gains in quality would spawn cost-reductions through increases in efficiency. Results achieved between 1984 and 1987 confirm this belief. For example, first time through yields in the manufacture of fuel rods increased from less than 50% to 87%, substantially reducing scrap, product reworking, and manufacturing cycle time. This helped NFD achieve over three years of 100% on-time delivery of high-quality products.

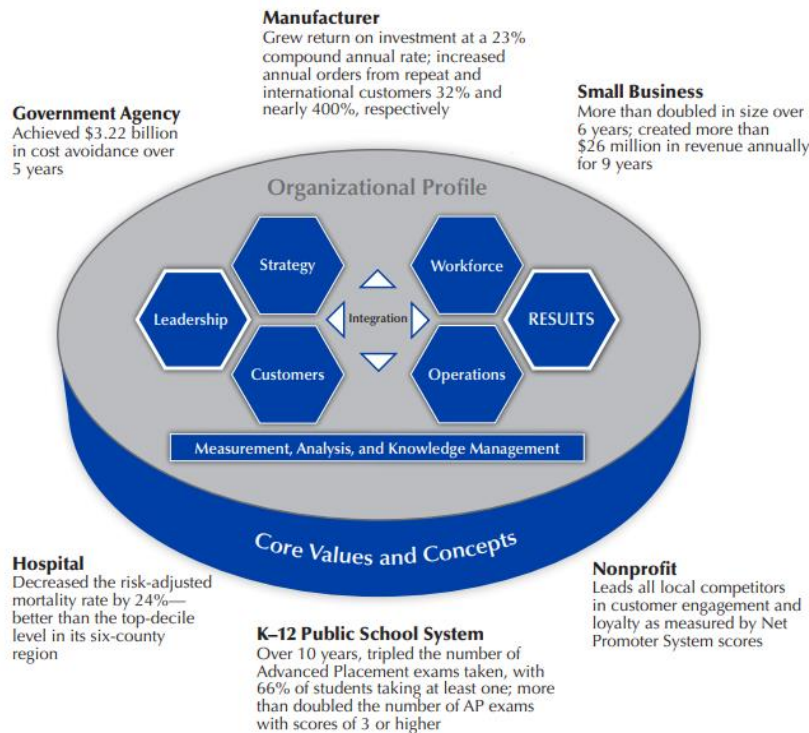
Baldrige Award Criteria

The criteria for selecting Malcolm Baldrige Award winners have changed somewhat over the years. The NFD was assigned to the manufacturing category in 1988. The Award is now given to organizations in six eligibility categories: manufacturing, service, small business, education, health care, and nonprofit.

A Baldrige Excellence Framework has been developed and is available for download from the internet. The Baldrige Excellence Framework includes the Criteria for Performance Excellence, core values and concepts, and guidelines for evaluating an organization's processes and results. This Framework may be used as guidance in establishing an integrated performance management system or for self-assessing progress.

Figure A-6 was copied from a publication providing information about the Baldrige Excellence Framework with the Table of Contents for the publication shown below the figure.

The Baldrige Excellence Framework



Contents

2 About the Baldrige Excellence Builder

The Baldrige Excellence Builder represents proven leadership and management practices for high performance.

4 Core Values and Concepts

5 Baldrige Excellence Builder

Answer these questions about the most important features of organizational performance excellence.

14 Assessing Your Responses

Assess your answers to the Baldrige Excellence Builder questions.

16 Glossary of Key Terms

Learn the definitions of key terms in the Baldrige Excellence Builder.

Figure A-5. Baldrige Excellence Framework with Table of Contents for document describing Framework shown at bottom.

A self-assessment worksheet is provided for organizations to determine their own quality status. The evaluation criteria include:

- Leadership

- Strategy
- Customers
- Management, Analysis, and Knowledge Management
- Workforce
- Operations
- Results.

These criteria form the basis for evaluating applications for the Baldrige Award.

Three Projects Performed in Support of The NFD TQ Program

The case study author (L. Hanes) was a minor participant in the NFD TQ program. He was a member at the time of the Westinghouse Corporate Productivity Council, which responded to Business Unit requests for help when facing a productivity problem. Because of this assignment, he was requested to provide support to the NFD in its TQ program.

The first project was performed very early in the TQ program. Top NFD management wanted to identify quality problems and possible solutions perceived by Division stakeholders. The project involved a four-day workshop conducted with about 12 stakeholders. The workshop mainly involved application of NGT. A workshop report was created and submitted to the top NFD manager and his staff. The manager implemented most of the recommendations, and his staff briefed workshop participants with reasons for not implementing the remaining recommendations.

The second project involved two tasks: (1) identifying methods and tools that project oriented teams (see above) could use in problem solving, and (2) training the NFD personnel who trained the 175 teams.

The third project involved helping solve a radiation problem. Workers on the manufacturing floor used glove boxes to work with radioactive fuel pellets (each pellet about the size of a fingernail). The worker would insert his/her hand into a glove, which was positioned inside the glove box. The worker picked up a pellet in the glove box and performed required tasks. The problem was that some workers were being exposed to radiation levels higher than permitted. This was viewed as a quality problem. The solution involved stakeholders participating in a workshop and follow-up activities. The NGT was used to identify reasons for the radiation exposures and possible fixes. Based on workshop results and recommendations the glove box design was modified somewhat, procedures and training were modified, and a short presentation prepared describing the importance of minimizing radiation exposure. An evaluation somewhat later found that radiation exposure while using glove boxes had decreased significantly.

Appendix B

The Translation Problem

For our purposes, perhaps the best perspective on the translation problem mentioned in Section 5 of the main text of the report comes from the concept of Pasteur's Quadrant (Stokes 1997). As Stokes was analyzing the conventional view of a one-dimensional continuum with basic "pure" science at one end and application at the other, he wondered where to place Louis Pasteur. Pasteur had made fundamental discoveries in microbiology (e.g., discovery of anaerobic bacteria) while pondering the practical questions of more effectively extracting alcohol from beet juice. Stokes points out: "The mature Pasteur never did a study that was not applied, as he laid out a whole new branch of science." (Stokes 1997, p. 13). Accordingly, Stokes transformed a one-dimensional continuum into a two-dimensional classification.

As seen in Figure B-1, scientific research can be classified by whether it advances human knowledge by seeking a fundamental understanding of nature, or whether it is primarily motivated by the need to solve immediate problems. In the upper left of the diagram, is located pure basic research, unconcerned with practical applications. This is labeled Bohr's Quadrant, in honor of the early 20th century nuclear physicist. While it might be considered the height of hubris to argue that nuclear physics has nothing to do with practical applications in this particular report, Stokes argues that Bohr's quest for atomic structure was, in fact, divorced from any practical applications. The lower right of the diagram is labeled Edison's Quadrant in honor of the inventor who was focused on narrowly targeted commercial inventions, with no interest in following up any associated scientific questions. Pasteur's Quadrant, however, is characterized by use-inspired basic research.

An anonymous Wikipedia author comments that members of university science departments are typically like Bohr in being motivated by, and rewarded for, knowledge generation. Members of commercial and governmental laboratories are, with some interesting exceptions, closer to Edison in their search for practical solutions. However, members of university engineering departments may fall between Bohr and Edison, looking to enhance both knowledge and utility. Since, a high degree of specialization is a characteristic of modern science and engineering, it is unlikely that a single individual will fall into Pasteur's quadrant.

The university scientist is much like Bohr, with the major motivation being new knowledge. The governmental engineer is behaving like Edison, with the greatest interest in utility, and considerably less interest in knowledge for knowledge's sake. Therefore the solution is: "*a systems engineering approach, where the Pasteur cell consists of numerous researchers, professionals and practitioners to optimize solutions*" [italics not in original] (https://en.wikipedia.org/wiki/Pasteur%27s_quadrant#cite_note-2). The term Applied Research is sometimes used to describe some of the activities mentioned above.

Applied and Basic research




		Considerations of use?	
		No	Yes
Quest for fundamental understanding?	Yes	 Pure basic research	 Use-inspired basic research
	No	—	 Pure applied research

Figure B-1. Stokes' Two Dimensional Classification of Research
https://en.wikipedia.org/wiki/Pasteur%27s_quadrant#cite_note-2

Thus, the pathway through the need for translation and Pasteur's quadrant leads us to a main theme of this report; a collaborative systems engineering approach. In this regard, the field of HFE and Ergonomics might be itself considered to live in Pasteur's Quadrant since it exists in the interstices of other disciplines (e.g., psychology, industrial engineering, systems engineering, biomechanics, computer science, etc., etc.).