INL/RPT-22-68076

Light Water Reactor Sustainability Program

Using Information Automation and Human Technology Integration to Implement Integrated Operations for Nuclear

July 2022

U.S. Department of Energy

Office of Nuclear Energy

INL/RPT-22-68076

Using Information Automation and Human Technology Integration to Implement Integrated Operations for Nuclear

Marvin J. Dainoff
Larry J. Hettinger
Jeffrey C. Joe

July 2022

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

ABSTRACT

The purpose of the research effort described in this report is to develop and demonstrate an approach to the design and implementation of advanced, automated systems intended to increase operational efficiencies at nuclear power plants. In particular, we describe methods for considering human-technology integration (HTI) issues throughout the various phases of system design, test, and implementation and how these considerations help promote effective design. This research project will develop planning tools and comprehensive guidance on how HTI principles and methods, in combination with information automation technologies, can enable effective data integration and coordination for full nuclear plant modernization. Specifically, this research project will develop an approach to automate the mapping of data from plant systems and processes to application needs, thereby significantly reducing the amount of human workload currently required for the execution of these tasks. In addition to developing an automated solution as a replacement for these tasks, this research will also analyze digitalization's effectiveness in reducing operational costs of compliance related activities. Compliance activities are estimated to account for as much as 50% of operations and maintenance (i.e., non-fuel and non-capital) costs of plant operation.

CONTENTS

FIGURES

TABLES

ACRONYMS

AI	Artificial Intelligence
CAP	Corrective Action Program
CR	Condition Report
CWA	Cognitive Work Analysis
DOE	Department of Energy
EID	Ecological Interface Design
HFE	Human Factors Engineering
HCI	Human Computer Interface
HTI	Human Technology Integration
I&C	Instrumentation and Controls
INL	Idaho National Laboratory
IP	Inspection Procedure
LWRS	Light Water Reactor Sustainability
ML	Machine Learning
MRM	Management Review Meeting
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PI&R	Problem Identification and Resolution
R&D	Research and Development
RADS	Reliability and Availability Data System
SPDS	Safety Parameter Display System
SRK	Skill, Rule, Knowledge
STAMP	System Theoretic Accident Model and Process
STPA	Systems-Theoretic Process Analysis
TMI	Three Mile Island
UCA	Unsafe Control Action
US	United States
WDA	Work Domain Analysis

USING INFORMATION AUTOMATION AND HUMAN TECHNOLOGY INTEGRATION TO IMPLEMENT INTEGRATED OPERATIONS FOR NUCLEAR

1. INTRODUCTION

The purpose of the research effort described in this report is to develop and demonstrate an approach to the design and implementation of advanced, automated systems intended to increase operational efficiencies at nuclear power plants (NPPs). In particular, we describe methods for considering human technology integration (HTI) issues throughout the various phases of system design, test, and implementation and how these considerations help promote effective design.

Current trends in complex systems design and use emphasize the importance of several key factors that are central to HTI and to the approach adopted in the current work.

User centered design – Given the ubiquitous nature of interactions between humans and technical systems, automated or otherwise, in complex systems, considerations of how technology can best address user needs is essential. A central component of HTI is its insistence on the inclusion of end user input in all phases of the effort to provide a functional, real-world perspective on the requirements of new technologies and systems.

Multidisciplinary design teams – The design or redesign of very complex sociotechnical systems such as NPPs requires the inputs of multiple domains, working *collaboratively* to address system design goals and challenges. Traditional "engineering-centric" approaches to systems design generally do not take adequate account of human-use considerations during all phases of design and implementation. Inclusion of HTI methods, such as those described in detail in subsequent sections of this report, as part of a multidisciplinary effort helps to reduced risks associated with poor system performance upon deployment.

Systems approach – Some contemporary HTI approaches, such as those used in the current work, are based on a so-called systems approach which views humans and technical systems as interacting components within a broader sociotechnical system. The nature of these interactions may either promote or delay efforts toward greater system efficiency, therefore it is important to understand where potential dysfunctional or non-existent connections between system components exists in a potential design. A number of systems approaches and methods have emerged within HTI in recent years in an attempt to address these issues. In the work that follows, we present the case for the use of several of these methods, including cognitive work analysis (CWA), work domain analysis (WDA) and systems-theoretic process analysis (STPA).

The remainder of this section provides additional background information on the issues that are at stake in attempting to introduce automation into an existing sociotechnical system, and how HTI can support engineering design, development, and implementation.

1.1 Socio-Economic Challenges Facing the Nuclear Energy Industry

The United States (U.S.) Department of Energy (DOE) has sponsored 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 reduce costs associated with operating and maintaining legacy instrumentation and control (I&C) and information systems in operating U.S. commercial NPPs (i.e., light water reactors). This work involves two major goals: (1) ensuring that legacy analog II&C systems are not life-limiting issues for the NPP

fleet, and (2) implementing digital I&C technology in a manner that enables broad innovation and business improvement in the NPP economic operating model. Improving overall system performance with the deployment of new digital I&C systems contributes to reducing operating costs for the NPPs, which are vital to the nation's energy and environmental security and economic prosperity.

The Plant Modernization Pathway of DOE's LWRS Program contains a strategic action plan that lays the groundwork for a digital transformation of the nuclear industry, embodying an advanced concept of operations with an end point vision where the digital infrastructure for a nuclear plant is designed as an integrated set of systems that together enable a technology centric operating model. As seen in Figure 1, Joe, Miyake, and Hall (2021) further described the conceptual overview of R&D that must be performed to achieve this end point vision. Designing and operating such integrated systems will, of course, require new, automated technologies. In addition, a new way of working, both in the design and operational phases, will be required. A sustained commitment from top management in terms of visible priorities and goals must percolate downward to the level of systems engineering in design and operations. For this effort to succeed, a strict discipline is required for the integration of multiple tightly coupled functions to ensure that all stakeholders in the systems engineering process are participating in a coordinated manner.

The future viability of the nuclear fleet in the U.S. will also be impacted by rising costs of doing business in a competitive energy marketplace. Much of these costs relate to the sheer number of workers that it takes to operate a nuclear plant as compared to non-nuclear power generation plants. There is a compelling need to introduce broader digitalization, as discussed above, while at the same time introducing effective automation into plant systems where appropriate. The ultimate goal of the work descried in this report is to introduce methodologies to the design process to enable joint optimization of technical and personnel resources within a modernized, digitized information ecosystem.

1.1.1 Plant Modernization Research Pathway

This section provides a description of the Plant Modernization Research Pathway with its four interacting components. As such, it provides useful context and direction for HTI within the overall research effort.

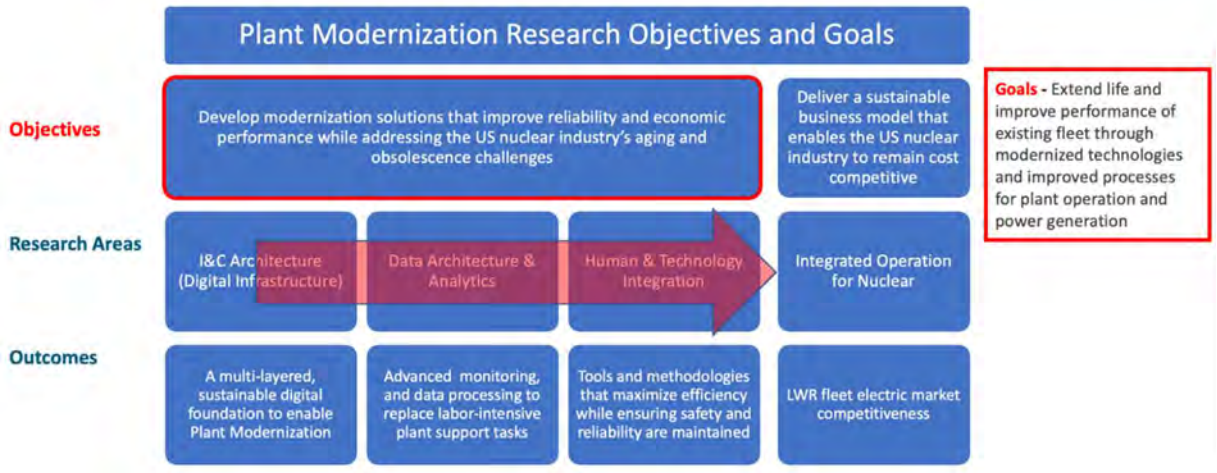

Figure 1. Conceptual overview of LWRS Plant Modernization Pathway (Joe, Miyake, and Hall 2021).

The research problem and its problem space are multi-faceted and multi-dimensional, encompassing numerous technical domains and areas of expertise. There are multiple perspectives from which to view and understand the grand challenge of this research – that being to extend the life and improve the performance of NPPs in the existing fleet by applying modernized technologies and improved processes for plant operation and power generation.

As Figure 1 above reflects no single individual can be an expert in all the perspectives and research areas needed to address the full scope of this research effort. In practice, this means that individuals must be self-aware enough to recognize the limits of their expertise. They must demonstrate a willingness and commitment to work with others creatively and synergistically. Therefore, the most likely way to successfully meet the multifaceted demands of this research is, therefore, for a multi-disciplinary team to work collaboratively.

Ultimately, NPPs are complex systems whose viability and effectiveness will depend on humans and technology working creatively and synergistically. Developing complex sociotechnical systems requires inputs from multiple technical areas and layers of expertise working together in a collaborative fashion. One of the chief opportunities for effective design lies in adapting existing human-technology design and integration tools and techniques to assist at all levels of the process. We turn to this topic in the next section.

1.1.2 The Role of Human-Technology Integration

Within the overall conceptual framework of the LWRS Plant Modernization Pathway, HTI is downstream of the Digital Infrastructure and Data Architecture & Analytics research areas, as seen in Figure 1 above**.** As such, it receives the outputs of those research efforts. Those outputs can be viewed as technologies that HTI uses as inputs to be integrated with the individual and teams that must use them.

Based on prior research experience, HTI R&D activities – in particular the Efficient Plant Operating Concept using HTI project (Kovesdi et al. 2021a) – has recognized three key barriers that must be overcome to adopt this technology-centric operating model. The three barriers are:

- Business case: developing a clear business case regarding the actual cost reductions seen with implementing advanced technology.
- Perceived risk: the perceived regulatory, licensing, and cybersecurity risk affecting technology acceptance and its HTI aspects.
- Incomplete guidance: insufficient guidance on performing significant digital modifications to the power generation side of the plant.

The role of HTI within system design, test, and implementation has become increasingly ubiquitous, primarily as a result of increased technical complexity in systems and the associated risk of human error or other failure in system performance. Ideally included in all phases of system design, HTI's ultimate purpose is to advocate for the user (whether an individual or an entire organization) by incorporating techniques derived from domains such as human factors engineering (HFE) and traditional systems engineering. Our major purpose in the current effort is to demonstrate how several of these techniques can contribute to the development of advanced automated systems, primarily through increased efficiency of representative NPP business functions.

1.1.3 Framework for Data Evolution

A fundamental concern in the synthesis of I&C Architecture, Data Architecture and Analytics, Human and Technology Integration, and Integrated Operation for Nuclear is the question of data; how it is collected, stored, and organized in meaningful patterns so that it can be used as a basis for action. This problem applies equally to human or machine actions. This is the problem of **data evolution**.

Whether it is a 7-year-old girl selling Girl Scout Cookies, or the operation of a NPP, a fundamental concern is how data is collected, stored, and organized in meaningful patterns so that it can be used as a basis for action. This is the data evolution problem. In the following section, a conceptual overview of the data evolution problem within the context of plant modernization will be developed. This framework is based on a Idaho National Laboratory (INL) planning memorandum sent on June 8, 2022 from Craig Primer (personal communication).

The data evolution concept has two basic but interwoven components: mapping and management. Mapping refers to the pathways along which data flows, and management refers to appropriate structure, format, tagging, and transformation. In the case of NPP modernization, these can be applied to three areas: (1) Acquiring appropriate data; (2) Analysis of the data; (3) Developing appropriate actions based on analysis (including visualization). In terms of the goals of the modernization pathway described above, concepts of "information automation" and "digitalization" will need to be closely examined and clarified in order to transform and modernize legacy data infrastructure.

For example, acquiring appropriate data may include developing advanced methods of data gathering, automation (e.g., sensors, drones, and robots), data preprocessing, and data reconciliation. Subsequent analysis of the data may involve application of artificial intelligence (AI)/machine learning (ML) analysis techniques to assist plant personnel to monitor plant performance and compliance efficiently and safely with NRC regulations (e.g., time series analyses for anomaly detection/condition-based maintenance, natural language processing, and computer vision). Developing appropriate actions based on these analyses would-provide the data architecture design necessary to significantly reduce plant operations and maintenance activities. This also includes how data are visualized; the traditional purview of HFE, with its concentration on ideas of transparency, explainability, data confidence, etc.

Finally, LWRS research activities related to data evolution should tie into three main "automation" areas for the organization:

- Process automation/analytics (supporting component, system, and plant level performance monitoring automation)
- Program automation/analytics (supporting assurance and compliance automation)
- Business automation/analytics (supporting organizational performance monitoring automation)

1.1.4 Scope

Within the broad framework of the Modernization Pathway described in Section 1.1.1 and Section 1.1.3, this research project will develop planning tools and comprehensive guidance on how HTI principles and methods, in combination with information automation technologies, can enable effective data integration and coordination for full nuclear plant modernization.

Within the specific data evolution framework described in Section 1.1.3, and in collaboration with industry, this research project will develop an approach to automate the mapping of data from plant systems and processes to application needs, thereby significantly reducing the amount of human workload currently required for the execution of these tasks. In addition to developing an automated solution as a replacement for these tasks, this research will also analyze digitalization's effectiveness in reducing operational costs of compliance related activities. Compliance activities are estimated to account for as much as 50% of operations and maintenance (i.e., non-fuel and non-capital) costs of plant operation.

1.1.4.1 Develop an Approach to Map Plant Data to a Compliance Application Need

Our primary focus will be in the area of plant compliance activities, particularly those related to specific NRC requirements and associated metrics. As described in Kovesdi et al. (2021), these activities, as currently configured in most plants, require a great deal of human workload, adding significant time and cost to activities such as forcing function meetings and management review meetings. Automating the mapping of plant data to individual decision makers' specific needs could significantly reduce operations and maintenance costs while improving overall efficiency of compliance activities.

We will concentrate on the mapping component of data evolution as applied to NRC inspection (compliance need). Data mapping will emerge from WDA analyses.

1.1.4.2 Develop the Method for Automating Organization Information Sharing Based on Defined Business Rules

Intent-based modification of WDA, combined with STPA control structure analysis will be used to characterize the informational requirements for specific inspection decisions (defined business rules). This characterization will enable automated access to such information. This effort is similar in concept to previous work with an industry partner on the design of management review meeting (MRM) dashboards based on an information automation concepts (Kovesdi et al (2021b). These methodologies can also identify candidate subsets of inspection task data for advanced automation using ML or other forms of AI.

1.1.4.3 Evaluate the Use of Organizational Information Sharing to Provide a Common Link to Enable Digitalization

As in the MRM dashboard work, we envision developing a common, digitalized source of meaningful chunks of information to enable inspector analysis and decision making. This digitalized source, instantiated in the form of information automation supporting compliance activities will serve as a model for expanded application of the concept across other NPP activities and requirements.

1.1.4.4 Demonstrate the Use of Organizational Information Sharing in Data Mapping and Data Management to Determine Feasibility of Proposed Digitalization Methods

Data mapping requires that the needed data flows to the right place at the right time. Data management requires that it is in the right format to enable effective visualization. As above, data becomes transformed to information when it is presented in meaningful chunks, where meaningful implies allowing effective action. As part of the current research, we demonstrate how systematic application of CWA, WDA and STPA provides an efficient and effective method for optimizing the integration of humans with new technologies and new modes of doing business.

1.2 Objectives

This section provides a description of the four principal objectives of the current work. All are related to the goal of identifying a path forward for the development of information automation and its successful implementation within the nuclear industry.

1.2.1 Objective One: Provide Planning Tools and Comprehensive Guidance on How HTI Principles and Information Automation Technologies Enable Data Integration and Coordination for Full Nuclear Plant Modernization

As discussed above, HTI represents one of several major research-stream components required to successfully address the design of complex sociotechnical systems such as NPPs. Its role is to ensure effective integration of humans – individually and in groups – with novel technical systems. It does this through systematic application of systems-based techniques such as CWA and STPA and impacts areas as diverse as human-computer interface (HCI) design and organizational design. Our objective is to demonstrate the utility of these methods in addressing issues involved with the design and implementation of information automation.

1.2.2 Objective Two: Develop a Conceptual Model of Information Automation Within a NPP Information and Computer Architecture Ecosystem

The specific application of HTI principles and methods within this effort will involve several forms of analysis, as discussed elsewhere in this report. One of our principal milestones in the development of functional information automation will be the development of a basic conceptual model of information automation within an NPP information ecosystem. Achieving consensus on a common model of information automation structure and function across a multi-disciplinary team of LWRS, INL, and industry experts is an essential step in promoting coordinated system design and development.

1.2.3 Objective Three: Illustrate Potential Applicability to a Specific Use Case

The third objective of the current effort is to illustrate the potential applicability of the design approach described herein to a specific use case of direct relevance to the nuclear industry's modernization efforts. As described above, in conjunction with our industry research partners we have selected the compliance domain as a potentially fruitful area for the introduction of effective automation. Specifically, the design of effective human-computer interfaces based on the design of the underlying information automation architecture.

1.2.4 Objective Four: Identify Potential Near- and Longer-term IO Application Areas

The fourth objective of the current work will be to identify near- and longer-term applications of information automation within NPPs. Prior work has demonstrated the concept's potential utility in supporting more efficient and less workload-intensive forcing function and management review meetings. Other potential applications will be identified through discussions with other LWRS and INL personnel working in related areas, as well as with industry partners.

2. APPROACH

2.1 The Data Development Ecosystem

Figure 2 presents a notional depiction of the NPP information ecosystem within which information automation will reside. To promote multidisciplinary discussion and revision throughout the design process, it purposely depicts the system at a high level of abstraction and is intended to serve three functions:

- To support discussion amongst the requisite, multidisciplinary technical and subject matter experts whose inputs will improve and refine it. The former may include LWRS, INL, and industry experts in relevant domains of computer science and architecture, AI/ML, HCI design, etc., while the latter would primarily comprise industry end-users, system architects, etc.
- To begin to identify design questions and issues that will need to be addressed to support successful information object (i.e., information automation) development and implementation and chart a path toward their resolution.
- To begin the development of an accurate and commonly held mental model of the data development ecosystem.

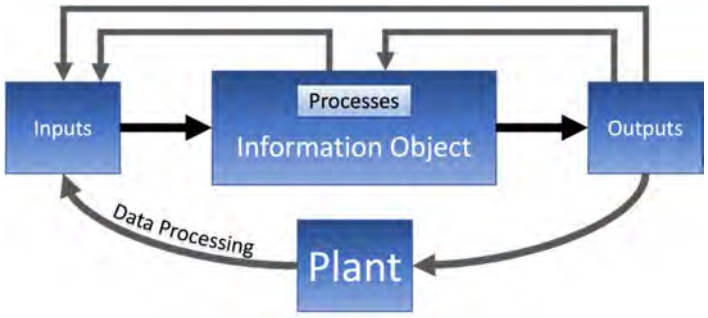

Figure 2. Notional depiction of information objects (i.e., information automation) within a NPP information ecosystem

2.2 Conceptual Roots of the Model

The broad issues outlined in the previous section have been addressed in a very specific manner a number of years ago by two key papers: Joyce and Lapinsky (1983) and Dinadis and Vicente (1999). These seminal papers will be briefly reviewed since their definition of the problem and proposed solutions are still highly relevant.

2.2.1 The Response to Three Mile Island (TMI): Safety Parameter Display System (SPDS)

In a review of the investigations of the TMI accident, by Joyce and Lapinsky (1983), the authors observe:

> A major premise discovered by most investigators was that no one in the TMI control room appeared to be able to assemble and integrate the correct combination of symptoms that would allow an early recognition of the fact the critical safety functions of the plant had been compromised, that is, that the core was being inadequately cooled (Joyce and Lapinsky 1983, 144.)

In short, the common factor in the failure at TMI was that none of the control room staff had a sufficient overview of the state of the plant. The investigators argued that what was required to accurately assess plant status was: (a) a mental model of plant processes allowing the identification of safety-critical information; (b) a means of gathering information from dispersed areas of the plant; (c) the capability for remembering the information so as to be able to make comparisons and determine interrelationships; and (d) integration of this material into an updated mental model of the plant.

A central component of this argument was the need for an accurate mental model consistent across all operators. It was pointed out that in the absence of a consistent mental model, each operator would develop idiosyncratic mental model which, under the conditions of stress during the TMI accident, were, "...overly complex or incomplete and, therefore, useless and inappropriate." (Joyce and Lapinski 1983, 144.)

Consequently, a means of organizing information in such a way that the cognitive processes of operators could easily generate accurate mental models of plant function was required. This recommendation was translated into the requirements and specifications for Safety Parameter Display Systems (SPDS) in NUREG-0696. As such, the core contribution of the field of HFE, with integration of research findings from cognitive psychology into engineering practice, became recognized. That is, utilizing the knowledge and understanding of the cognitive capabilities and limitations of the human operator so as to design information systems allowing safe and effective performance.

It must be emphasized that this fundamental statement of the problem and general solutions from almost 40 years ago are still relevant to the data evolution issues raised in Section 1.1.3. The solutions are as applicable to non-control room operations (e.g., compliance activities) as they are to the control room. In each case the end-goal is to gracefully integrate human and technical capabilities to contribute to overall system safety, resilience, and performance. However, as will be seen, the methods and technologies available for solving the problem have advanced considerably.

It is of some interest that references cited in this paper include works from the 1970s on the psychology of information integration and pattern recognition. However, there is also an early paper by Rasmussen, Pejtersen, and Goodstein (1994), who will become a major figure is this development.

2.2.2 Abstraction Hierarchies and Ecological Interface Design

Working within the nuclear industry, Rasmussen, Pejtersen, and Goodstein (1994), realized that the complexity of plant design and operation required a more systematic way to address the fundamental issues raised by the TMI accident. Based on these foundations, Dinadis and Vincente (1999) presented a practical demonstration of how to design what they described as an ecological interface for the engine and fuel system of a Lockheed Hercules C-130. Using what is now called WDA (combination of means-end, and part-whole abstraction hierarchies), an interface display was designed that:

> (a) provided a systematic approach to identifying interface information, (b) presented higher order functional information and lower-level physical information, (c) took advantage of the power of emergent features, and (d) provides a model-based visualization that can support problem-solving activities and the development of more accurate mental models.
> (Dinadis and Vincente 1999, 246).

Two separate but related conceptual threads are required to conduct ecological interface design (EID). The first, as mentioned above, are the analytic tools of abstraction hierarchies, which allow the full complexity of the work system to be characterized in functional terms. The second was Rasmussen's (1986) Skills-Rules-Knowledge (SRK) taxonomy of human performance.

The SRK taxonomy is brought to bear based on the realization that the operator has two separate demands. The first demand is to be an adaptive problem solver able to respond to unanticipated and

perhaps novel situations. The second is also to be able to efficiently cope with routine tasks as well. To satisfy both demands, the EID design principles apply to the SRK taxonomy as follows:

1. The first level of the taxonomy, Skill-Based Behavior, supports direction interaction with space-time signals (e.g., joysticks) with the interface.
2. Rule-Based Behavior provides a consistent one-to-one mapping between attributes of the work system and the signs provided by the interface (e.g., the color red consistently means a given subsystem is "off").
3. Knowledge-Based Behavior uses the structure of the abstraction hierarchy to construct a display which represent the functionality of the work system. This allows the operator to develop an accurate mental model to support problem solving.

The bulk of the Dinadis and Vicente (1999) paper consists of a practical demonstration of how these principles were used to construct an ecological interface for the fuel system of a Lockheed C-130.

While originating in the nuclear industry, EID is broadly applicable to different kinds of sociotechnical systems. Rasmussen, Pejtersen, and Goodstein (1994) demonstrated that sociotechnical systems could be classified on a continuum ranging from causal to intentional. This has been elaborated by Naikar (2013, 38-39). At one extreme, NPPs are used as an example of causal systems; such systems can be described as tightly coupled technical equipment related to physical processes governed by natural laws. At the other extreme, an example would be an entertainment streaming service; characterized by individual objectives, values, and goals. This distinction becomes critical in terms of the nature of the user/operator mental model. For causal systems (e.g., NPPs), the mental model must bear a close relationship to the actual physical constraints of the system. On the other hand, for an intentional system, the goal is to support the initial mental model which the user brings to the system (e.g., I want to find a certain kind of music.) This discussion is relevant to ensuring that the widely used HFE principle of user-centered design is not misunderstood. In fact, Flach and Dominguez (1995) have argued from this logic that "user-centered design," should be replaced by, "use-centered design."

2.3 Core Concepts: Conceptual Architecture, STAMP and STPA

This next section builds on the principles described in Section 2.2 to develop core concepts for addressing the issues of data evolution (Section 1.1.3). Leveson (2020) argues that the standard V model of systems engineering is flawed in that physical connections among components can be designed and implemented in hardware before the potential interactions among such components are understood. This is problematic in complex systems and potentially creates design flaws leading to security or safety issues only becoming apparent after the fact when remedies are typically highly expensive. See also, Leveson, (2009), Poh (2022), and Leveson and Thomas (2018, Appendix G).

The practical methodology for developing a conceptual architecture is based on a causality model called System Theoretic Accident Model and Process (STAMP) in which the emphasis shifts from preventing failures to enforcing safety constraints (Leveson 2011, Chapter 4). Within the overall STAMP framework, there are specific analytic tools. The tool to be focused on in this project is System Theoretic Process Analysis (STPA); an approach to hazard analysis based on the STAMP causality model (Leveson 2011, Chapter 8; STPA Handbook 2018). STPA is the method which is at the basis of the conceptual architecture proposal just described. Moreover, this approach incorporates and expands the foundational work on CWA (Rasmussen, Pejtersen, and Goodstein 1994; Dinadis and Vicente 1999) discussed earlier.

STPA has already been shown to be effective for examining existing systems; however, its utility in defining high level safety constraints prior to implementing specific system functionality would seem to be particularly relevant to the present case of examining digitalization/automation aspects of data evolution within the context of HTI.

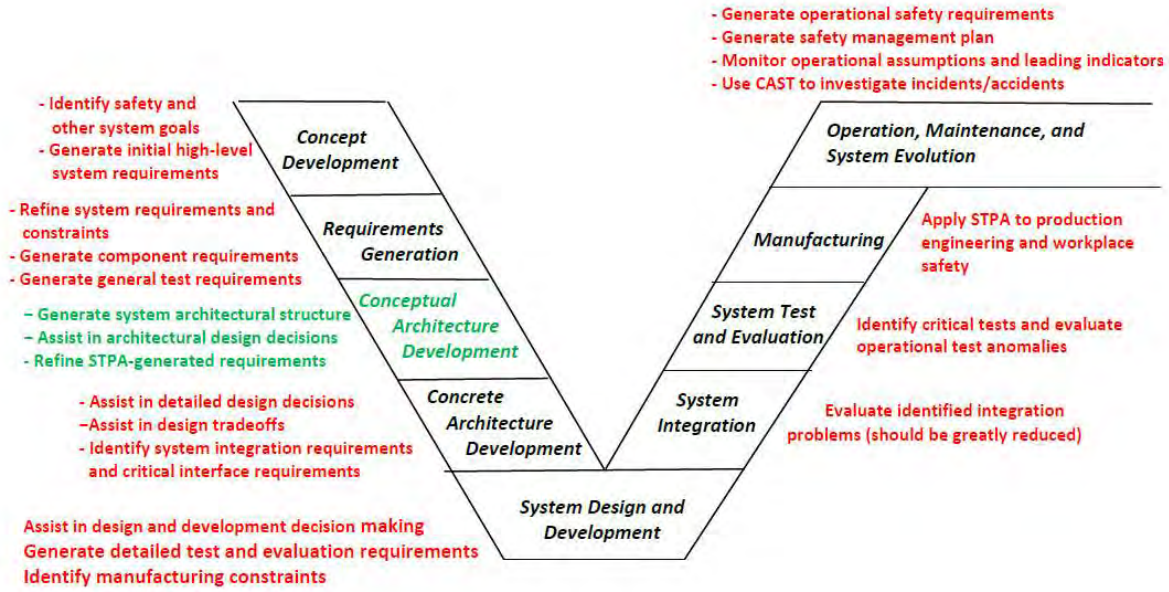

Figure 3. Standard V model of systems engineering with a new conceptual architecture development stage added. Annotations indicate the role of STPA at each state. (Reprinted from Leveson 2000, Figure 2 with permission).

2.3.1 Cognitive Work Analysis

2.3.1.1 Work Domain Analysis

Within the overall theoretical framework of STAMP, Leveson has modified and expanded the essential concepts of CWA to be included within the STPA methodology. The specific modifications are: (a) using STPA as a conceptual architecture early in the system design process (discussed above), and (b) modification of Work Design Analysis to include intent-based specification.

WDA is the first component of CWA. The utility of WDA for EID is that it characterizes the work domain in formative, rather than descriptive or normative terms. Simply put, this implies that WDA reveals the space of possibilities for action on the domain. This tool allows for characterization of the overall landscape of work, embodying all possibilities for action. A key step is the identification of what might be called intrinsic behavior-shaping constraints. These provide a boundary within which a variety of different actions are possible. This is a central concept in CWA; the goal is to characterize this landscape at a level of abstraction which is independent of any particular technology. An example might be a road map. The indicated roadways are intrinsic constraints on the landscape which limit the possibilities for action for an ordinary driver and vehicle. However, within this set of possibilities, many alternative routes might be chosen. To continue the analogy, if off-terrain vehicles are available, such as in a military context, the domain would be better described with a contour map showing geographical features (e.g., streams and elevations) in more detail.

The WDA has two dimensions: the Means-End Abstraction Hierarchy, and Part-Whole Decomposition. The Means-End Hierarchy provides a logical framework for analysis of the functional possibilities for action within the work domain. This framework includes the structural relationships: WHY, HOW, and WHAT. To pick a simple example: two people who live together have an appointment at the same place and time. The WHY question is one of basic goals: they need to get from where they live to the location of the appointment. The HOW question might involve consideration of whether they will take one car or two. The WHAT question relates to which route they will take. Note that the lower-

level question contains the *means* by which the *ends* of the next level are achieved. In a typical analysis, there are five levels in the hierarchy, and we can envision the WHY, HOW, and WHAT questions sliding up and down the hierarchy. These levels are conventionally labeled as follows: Functional Purpose, Values and Priorities, Purpose-Related Functions, Object-Related Processes, and Physical Objects.

The second dimension of WDA is Part-Whole Decomposition. Most of the system investigation using CWA are complex enough that the overall system requires decomposition into its constituent parts. In this example, each of the people described above will be driving independently, so a separate analysis might be done for each of them. For example, they may each have different tasks to accomplish on their way home.

Leveson's (2020) modification of basic WDA principles is called *Intent Specification.* She argues that too often, in the development of complex systems, the original designer's intent for particular solutions is either not made explicit, or if explicit, is not readily available when modifications need to be made. Accordingly, at an early stage in the system development process, a systematic description of system goals, potential unacceptable system losses, hazards that might lead to such losses, safety constraints that might mitigate against hazards, and relevant environmental and design assumptions. These would typically be located at the Values and Priorities level of the Means-End Abstraction Hierarchy. The highest-level specifications would be located at the system level of the Part-Whole Decomposition dimension. These high-level specifications would be inherited at lower levels of the dimension along with any more detailed supplemental specifications.

2.3.1.2 Formative Nature of Work Domain Analysis in Terms of Automation Possibilities

A WDA is meant to be formative, rather than descriptive, or prescriptive. What this implies, practically, is it should be like a road map, revealing many alternative possibilities for action. In ecological analyses, these are called affordances. Hence, the physical data objects populating the lowest level should be types rather than specific instances. This is particularly relevant for the current project which is concerned with the potential automation of NPP function.

Consequently, a full WDA of NPP processes judged to be amenable to automation would have the benefit of revealing possibilities for automation based on existing structures. Using the roadmap analogy, multiple possibilities for action on these structures might exist. The next stage of analysis, defining the control structure, elaborates such possibilities. However, if the road map reveals inadequacies (e.g., there is no direct route from A to B), redesign may be necessary.

2.3.2 Ontology

"Ontology provides a means for capturing and modeling categories of entities, their attributes or properties, processes, and relations for a given domain of interest" Little (2009, p. 204). Ontological systems are hierarchical. At the upper level are *rational constructs* –objects that are clusters of logically grounded formal relationships. At the lower level are *empirical constructs*—materially grounded objects that capture and utilize the specific knowledge of subject matter experts. With two abstraction hierarchies as a primary analytic tool, Little (2009) argued that the elemental components of such hierarchies be described in terms of their underlying ontological structure. Al Rashdan, Browning, and Ritter (2019) have defined such ontologies for NPPs.

2.3.3 STAMP and STPA

2.3.3.1 Basic Description of STPA

STAMP is a systems-theoretically based accident causation model (Leveson 2011). 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 of the system maps out the interaction between controllers and controlled processes. See Figure 4 for a generic example. 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 (Leveson and Thomas 2018):

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

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. The advantage of this approach is that mechanical and human control actions can be analyzed within the same conceptual framework; reinforcing the sociotechnical perspective towards systems engineering emphasized in Dainoff, Hettinger, Hanes, and Joe (2020).

The first step of STPA can be accomplished through the process of intent specifications, described earlier in Section 2.3.1.1. The second step maps out the networks (existing or proposed) of control relationships between controllers and controlled components in terms of command/control links and feedback links. As such, it provides a specification of the action possibilities within the identified constrains of the work domain.

The third step of STPA consists of a systematic examination of each individual control action in detail to determine if unsafe control actions (UCA) are possible. A structured series of questions are posed: is an UCA possible if the action is (a) provided; (b) not provided; (c) provided too early or too late; (d) stopped too soon, or applied to long? (In some cases, it is only necessary to pose questions [a] and [b]). The definition of unsafe is determined with respect to whether or not the analyzed action would result in one of the system hazards defined in the first step.

In the fourth step of STPA, scenarios are constructed once the set of UCAs has been determined. A scenario describes the causal factors that could lead to the UCA and the associated hazard and corresponding losses (Levenson and Thomas 2018). Multiple scenarios can be proposed for any single UCA. The scenarios can also be used to determine the safety constraints which might have been compromised.

2.3.3.2 Human and Automated Controllers

Figure 4 from Leveson (2020), represents a generic conceptual control structure involving the interaction of human and automated controllers. The prototype example of this kind of interaction would be a commercial airline pilot in a modern automated cockpit. However, this could also be utilized to examine any kind of interaction between human and automated systems. The top component is based on an extended model of the human controller developed by France (2017).

The conceptual advantage is that essentially the same analytic logic can be used for both human and automated functioning. This kind of multidisciplinary approach, blending human factors and cognitive psychology with data science and control engineering, is often encouraged but rarely implemented.

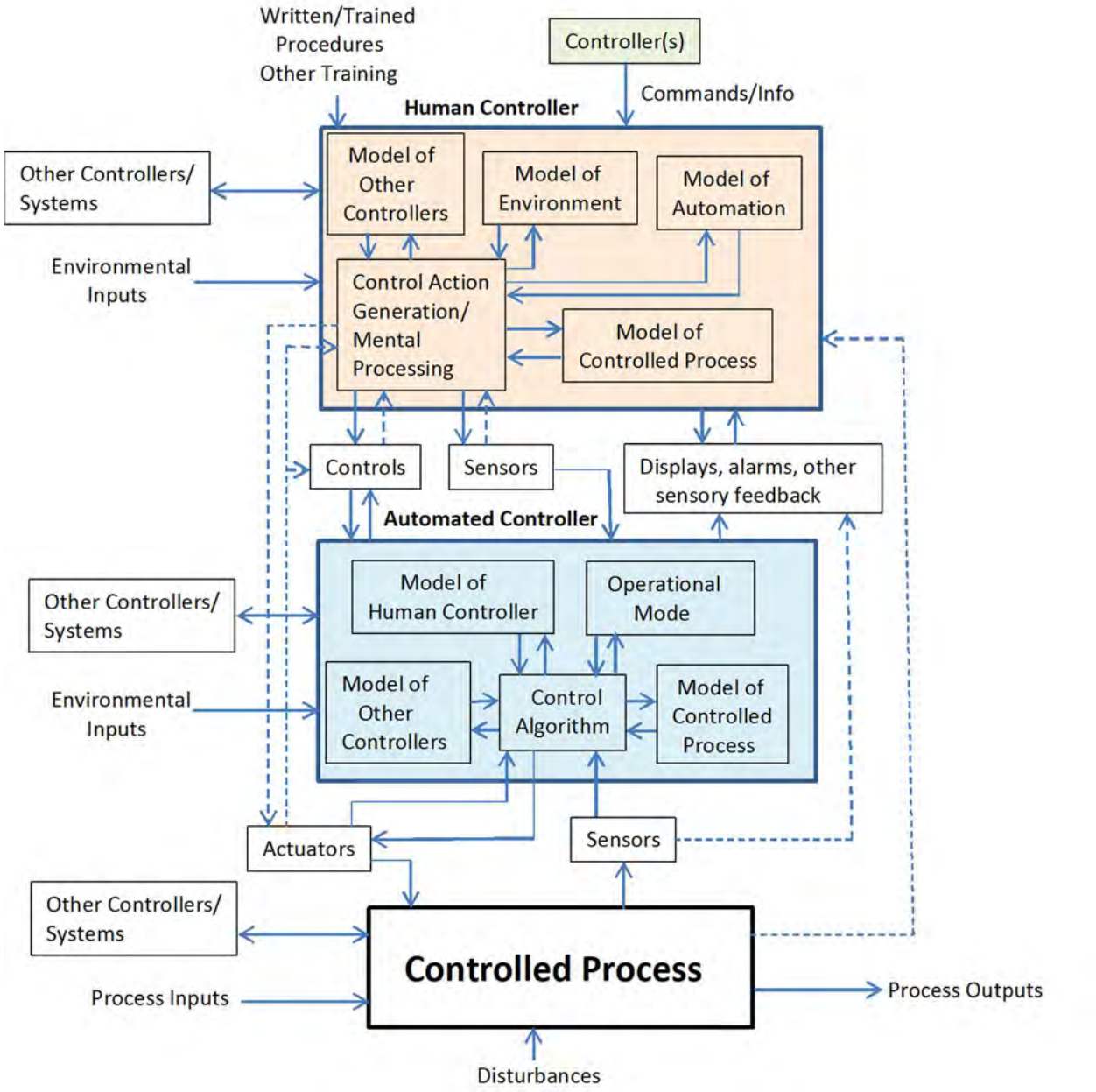

Figure 4. Generic Human and Automated Controllers (Leveson 2020, Figure 10)

While this is not the place to describe this architecture in depth, it can be seen that the human controller needs to have different kinds of mental models: models of other human controllers, models of the environment, and models of the controller process. In addition, models of automation, if present, are required. These models combine to determine the control actions (decisions) carried out by the operator. These actions are part of a perception-action cycle in which feedback results in corrective action and possible modification of one of the mental models. Note that the term Situation Awareness can simply be interpreted in terms of degree of correspondence between user mental models and the actual situation. This argument will be expanded in the following section.

2.3.4 The Logic of Ecological Interface Design in Solving the Visualization Problem

Up to this point, the basic issues related to data evaluation can, at least potentially, be addressed by the STPA/WDA methodology. The abstraction hierarchies can be used to trace the mapping of data from the point of acquisition until it has been transformed to the point of being useful for analysis by a decision maker—either automated or human. The logic of those decisions, and the potential for failure, can be defined by the STPA process, to whatever level of detail is required. However, to the extent a human operator is involved, the final step involves visualization of the information in a manner which allows effective performance.

The visualization problem can be best considered using a more dynamical form of representation. The logic underlying EID as proposed by Bennett and Flach (2011) provides a useful approach. This approach provides an alternative way of looking at the information contained in the work domain and control structure

Fundamentally, this logic embodies a three-part relationship among: (1) the ecology or work domain: (2) the representation of that domain (i.e., the user interface), and (3) the underlying cognitive constructs (mental models) used to understand the domain. See Figure 5.

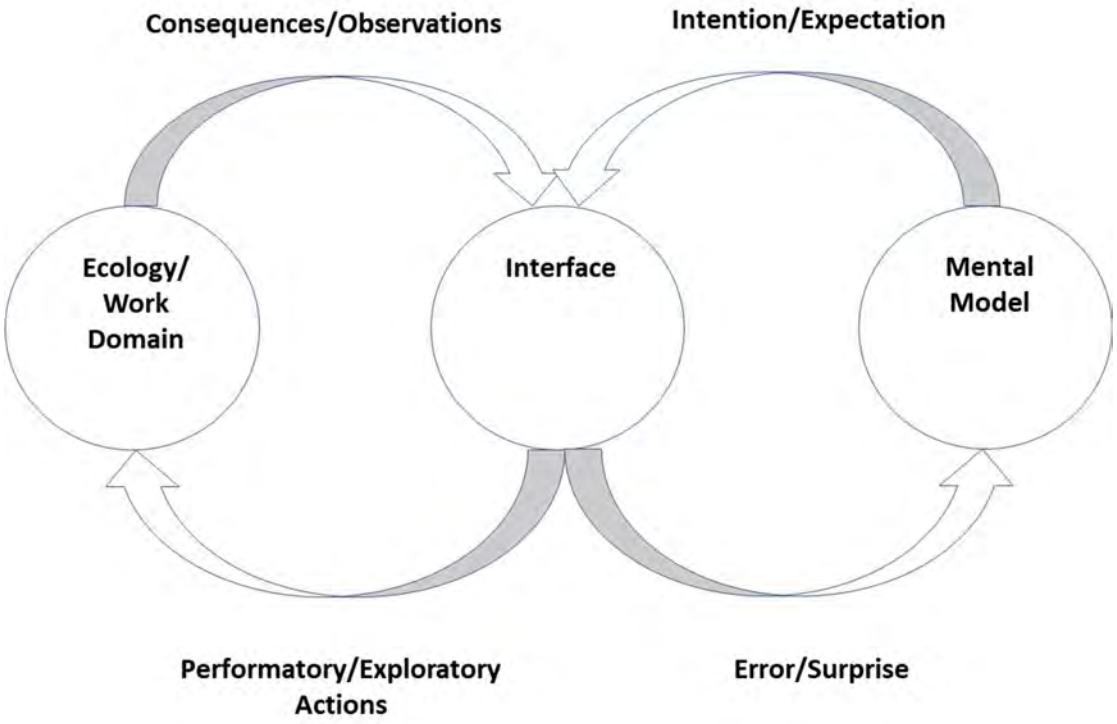

Figure 5. Three-part framework for EID. Modified from Bennett and Flach (2011, Figure 2.3).

The major components in this logic framework are, reading from left to right, work domain, user interface, and user mental model. These components are connected by two perception links and two action links. Together, these elements reflect the dynamic linkage which always exists between perception (What do I experience?) and action (What do I do?). Understanding these dynamics is critical to the practical demands of solving the visualization problem by constructing an effective user interface.

The first part of the problem involves understanding the Situation, which is also called the work domain, or ecology, of the system. This understanding involves analyzing the contents of the information objects related to the user's problem and organizing these contents into meaningful chunks. In this case,

"meaningful" means revealing possibilities for action and associated consequences. WDA is used to accomplish this task.

Having understood the Situation, the second part of the solution involves understanding the Awareness of the decision maker. Specifically, this means understanding the possible sets of actions that could be carried out by the decision maker given the information available and within behavioral/cognitive capabilities of the individual. The goal is to allow the decision maker to establish a mental model which corresponds to the physical reality depicted in the WDA. This correspondence requirement, while not found in all applications of Situation Awareness, is particularly relevant to safety critical systems, such as an NPP, which are grounded in physical laws. (See the earlier discussion of the distinction between causal vs. intentional systems in Section 2.2.2).

The Awareness component is analyzed through STPA, which, as discussed above, uses the information structure of the WDA as a template or map upon which to superimpose potential control actions which can accomplish the desired goal. The resulting control structure diagram can be used to establish possible mental model structures which meet the correspondence requirement just discussed.

Finally, the third part of the solution is to integrate Situation and Awareness. This is accomplished through the actual construction of the ecological interface/dashboard. This is as much art as science and requires integrating the findings of WDA with STPA. The meaningful chunks discovered in the WDA must be represented in the interface in such a way that the control actions can be effectively carried out with known cognitive capabilities of the human user. Using the SRK taxonomy discussed in Section 2.2.2 provides a template to ensure that the interface allows the user to engage Skill, Rule, and Knowledge based behaviors. Bennett and Flach (2011) and Burns and Hajdukiewicz (2004) provide extensive guidance in constructing ecological interfaces.

2.4 Use Case: NRC Inspection

In order to demonstrate the feasibility of the approach discussed in Section 2.3, a use case was constructed based around the NRC Reactor Oversight Process, specifically its Problem Identification and Resolution (PI&R) program as described in Inspection Manual Inspection Procedure (IP) 71152 (NRC 2015). For ease of communication, the use will be restricted to the Routine Review component of PI&R, and, within that process, to the Verify Corrective Actions task within that component. Specifically:

> Verify that corrective actions commensurate with the significance of the issue have been identified and implemented by the licensee. An in-depth review of selected issues may be conducted in accordance with Section 02.03 of this IP (NRC 2015, Section 02.01.b).

The presumed context generating this use case will attempt to automate certain aspects of the inspection task. While this is a long-term goal, the present demonstration will focus on the actions and resources available to the human inspector; realizing that this kind of work analysis is typically a necessary step prior to any automation. In addition, as a feasibility demonstration, the analysis will lack some detailed technical support information, for reasons of practicality, and will therefore rely on placeholders in some cases.

3. FINDINGS

This section illustrates the STPA/WDA approach to understand the data evolution problem (Section 1.1.3) as applied to the NRC PI&R program as restricted to the case of Routine Screening -Verify Corrective Actions.

3.1 Work Domain Analysis

As previously discussed, WDA, can be described along two dimensions. The horizontal dimension represents part-whole relationships, whereas the vertical dimension represents means-end relationships. In this analysis, there will be three components to the part-whole reduction: System, Subsystem, and Component. The full analysis is depicted in Figure 5. The System level represents the high-level Reactor Oversight Framework, the Subsystem level represents the PI&R process, and the Component level represents the Verify Corrective Actions Task of the Routine Screening Inspection. It should be noted that in a complete analysis, Routine Screening would itself be represented at an intermediate Sub-Sub System level prior to the Component level.

Figure 6 is meant to give an overview of the entire analysis. However, in further discussion, in order to facilitate readability, individual slices of the horizontal part-whole dimension will be shown.

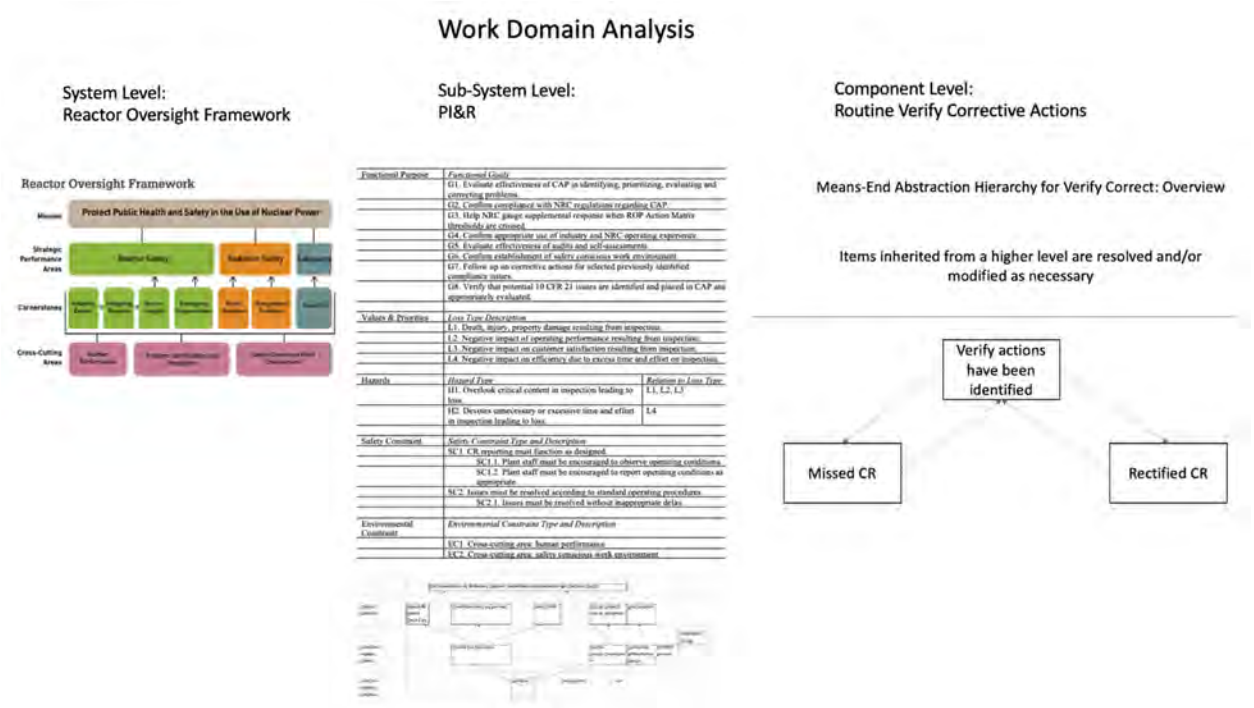

Figure 6. Full Work Domain Analysis: PI&R

3.1.1 System Level Analysis

The current PI&R analysis occurs within the overall context of the NRC Reactor Oversight Process Framework. Figure 7 depicts the NRC's own representation of that framework; its structure is similar enough to that of WDA that it can serve as a placeholder for purpose of this analysis.

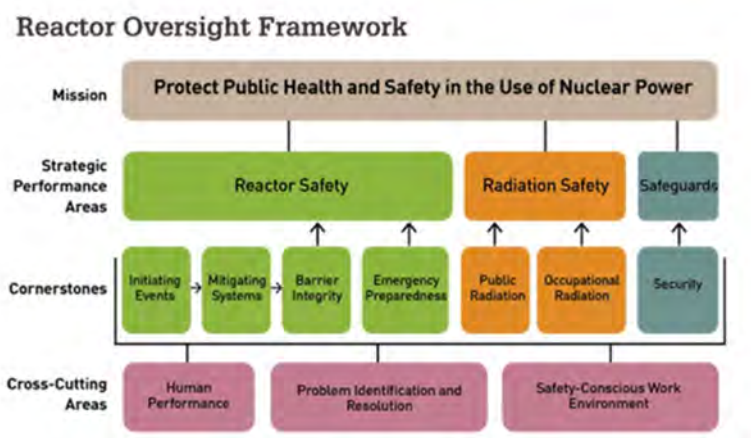

Figure 7. Reactor Oversight Framework (Source: https://www.nrc.gov/reactors/operating/oversight/rop-description.html)

3.1.2 PI&R

The work domain comprising the PI&R component is depicted as a Means-End Abstraction Hierarchy with four levels in which each lower level describes the means of achieving the ends represented by the next higher levels. It is assumed that the individual means-ends relationships between elements of this hierarchy can be made compatible with the ontological framework laid out in Al Rashdan, Browning & Ritter (2019). See also Little (2009) and the discussion in Section 2.3.2. Specifically, components higher in the hierarchy consist of functions to be accomplished, whereas components lower in the hierarchy consist of ways in which accomplishment can take place. These may be descriptions of processes, or actual physical objects, such as documents or computerized records.

Table 1 depicts the top level of the abstraction hierarchy: Functional Purpose and Values and Priorities. This is the point at which we use Leveson's (2020) modification of basic WDA principles (See Section 2.3.1.1). Leveson has called her approach Intent Specification. She argues that too often, in the development of complex systems, the original designer's intent for particular solutions is either not made explicit, or if explicit, is not readily available when modifications need to be made. Accordingly, she argues that a systematic description of system goals, potential unacceptable system losses, and hazards that might lead to such losses, along with safety constraints that might mitigate against hazards as well as relevant environmental and design assumptions should be explicitly described at an early stage in the system development process. By doing this, intent specification is achieved.

The elements depicted in Table 1 are to be considered placeholders. They represent an attempt to communicate examples of intent specifications. These examples have been taken from NRC documents and other sources. However, a full set of such specifications would require expert knowledge to be integrated into the systems engineering process. At the same time, Leveson argues strongly that consensus on such specifications must precede detailed system development. Such consensus development would be an integral part of the socio-technical approach to systems development (Dainoff et al. 2000).

At the highest level, Functional Purpose, a set of goal statements is provided. These are a restatement of the inspection objectives taken from Inspection Manual IP 71152. The next level down, Values and Priorities, contains Losses, Hazards, Safety Constraints, and Environmental Constraints. See Table 1.

Table 1. Work Domain Analysis: Means-End Abstraction Hierarchy for NRC PI&R Subsystem

Functional Purpose	*Functional Goals*	
	G1. Evaluate effectiveness of CAP in identifying, prioritizing, evaluating and correcting problems.	
	G2. Confirm compliance with NRC regulations regarding CAP.	
	G3. Help NRC gauge supplemental response when ROP Action Matrix thresholds are crossed.	
	G4. Confirm appropriate use of industry and NRC operating experience.	
	G5. Evaluate effectiveness of audits and self-assessments.	
	G6. Confirm establishment of safety conscious work environment.	
	G7. Follow up on corrective actions for selected previously identified compliance issues.	
	G8. Verify that potential 10 CFR 21 issues are identified and placed in CAP and appropriately evaluated.	
Values & Priorities	*Loss Type Descriptions*	
	L1. Death, injury, property damage resulting from inspection.	
	L2. Negative impact of operating performance resulting from inspection.	
	L3. Negative impact on customer satisfaction resulting from inspection.	
	L4. Negative impact on efficiency due to excess time and effort on inspection.	
Hazards	*Hazard Type Descriptions*	*Relation to Loss Type*
	H1. Overlook critical content in inspection leading to loss.	L1, L2, L3
	H2. Devotes unnecessary or excessive time and effort in inspection leading to loss.	L4
Safety Constraint	*Safety Constraint Type and Descriptions*	
	SC1. CR reporting must function as designed.	
	SC1.1. Plant staff must be encouraged to observe operating conditions.	
	SC1.2. Plant staff must be encouraged to report operating conditions as appropriate.	
	SC2. Issues must be resolved according to standard operating procedures.	
	SC2.1. Issues must be resolved without inappropriate delay.	
Environmental Constraint	*Environmental Constraint Type and Descriptions*	
	EC1. Cross-cutting area: human performance	
	EC2. Cross-cutting area: safety conscious work environment	

Losses and Hazards statements are taken from the STPA Handbook (Leveson and Thomas 2018) and represent typical statements for the nuclear industry. They have been modified to reflect losses due to inspection failures. Hazards are defined as:

> A system state or set of conditions that, together with a particular set of work-case environmental conditions, will lead to an accident (i.e., loss) (Leveson 2011, 182).

Note that each hazard is associated with a specific set of losses. Note also that this is a high level of specification. If required, a finer grain of analysis can be carried out.

Safety Constraints are those behavioral constraints that must be enforced in order to maintain the safety of the system (Leveson and Thomas 2018). Illustrated here are sample constraints and sub-constraints for reporting process and resolution. These constraints will be explored in more detail in a later section.

Finally, the Environmental Constraints represent factors influencing the system but outside of it. In this case, according to IP71152, while PI&R is the focus of this analysis, the other two cross-cutting areas, Human Performance, and Safety Conscious Work Environment, would be part of the system environment.

Figure 8 contains the lower three levels of the Means-End Abstraction Hierarchy. The Purpose-Related Function Level depicts the four phases of the inspection cycle: Routine, Semiannual, Follow-up, and Biennial. These four functions constitute the means by which the values and priorities articulated in the level above can be achieved. In this example, only the Routine phase is described.

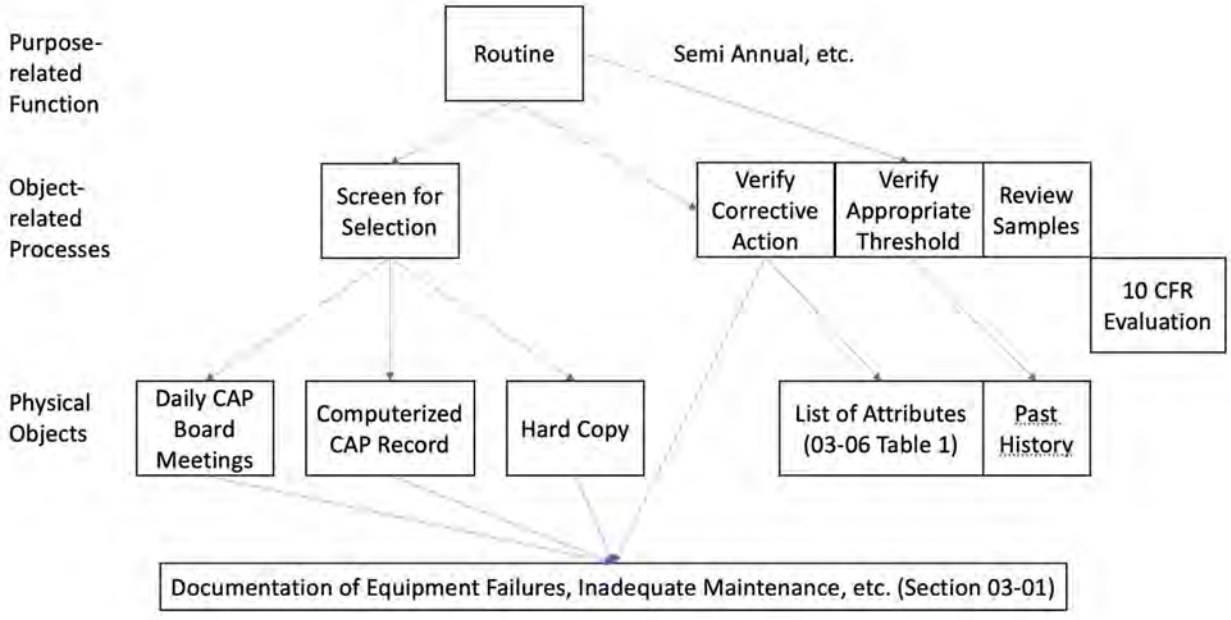

Figure 8. PI&R. Purpose-related Function, Object-related Processes, and Physical Objects: Means-End Abstraction Hierarchy

The Routine phase ends are achieved by four object-related processes: screen, verify correctness, verify threshold, and review samples. A fifth process, evaluation of 10 CFR 21 Reporting requirements, is carried out in parallel with the other four. Not illustrated are the three subcomponents of the verify threshold process: equipment, human performance, and program. Also not illustrated are the cornerstone functions (See Figure 7); each of which is expected to be represented in samples selected to be reviewed.

Finally, the lowest level contains the physical data objects upon which the processes depicted in the previous level operate. In the present example, these items are described in generic form, but an actual analysis would be much more specific; based on subject matter expertise.

3.2 Verify Correct Identification: Routine Screening

In this section, we move to the right on the part-whole dimension of the work domain and examine a component of the routing screen phase; Verify Correct Identification. The exact language from IP 71152 is:

Verify that corrective actions commensurate with the significance of the issue have been identified and implemented by the licensee.

Figure 9 contains an overview of this analysis. At the two upper levels of the Means-End Abstraction Hierarchy is a notation that, for this particular version of the analysis, the Functional Purpose and Values and Priorities contained in Table 1 are inherited from the previous portion of the part-whole dimension—PI&R and are, therefore applicable to the Verify function. If this were a full analysis, the contents of Table 1 would be most likely be supplemented with more detailed items.

At the level of Purpose-related Function is the single function associated with this task: Verify correct actions have been identified. The means for accomplishing this as specified by two Object-related Processes: verification of identified condition reports (CRs) which have been rectified, and search for situations in which CRs should have been created but are actually missing. In this figure, the lowest level, Physical Objects, is not required.

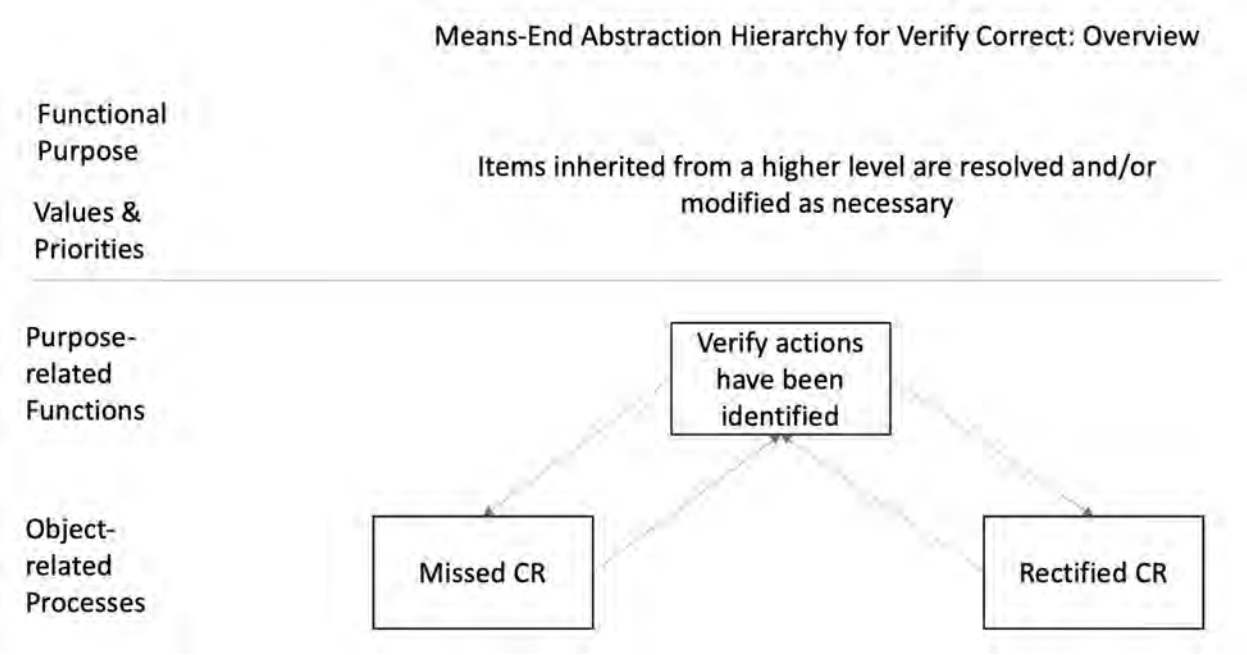

Figure 9. Overview for Verify Correct Identification: means-end abstraction hierarchy

3.2.1 Missing CRs

In Figure 10, we zoom in on that portion of the lower three levels of the means-end abstraction hierarchy corresponding to the search for missing CRs. For simplicity, this diagram relies on context to make the distinction between processes and physical data objects.

The logic underlying this analysis is that the inspector must identify situations where some deficiency occurred but was not specifically logged in a CR. To accomplish this, it is necessary to first select a sample of significant equipment to examine. The NRC Reliability and Availability Data System (RADS) (https://nrcoe.inl.gov/RADS/) contains general guidance on significance; in addition, each licensee will have its own list of significant equipment.

Within these constraints, a process of reviewing individual cases must be established. Two separate sources of such cases are identified: examination of work records accomplished but not resulting in a CR and Walk Down inspection. The examination of work records involves access to the plant work management database. In the case of the Walk Down, the default will be the Resident Inspector with his/her detailed skilled knowledge of the plant. However, it may be necessary to bring in NRC Specialists

in certain situations. (Note: these decisions would be the subject of an even more detailed drill-down analysis).

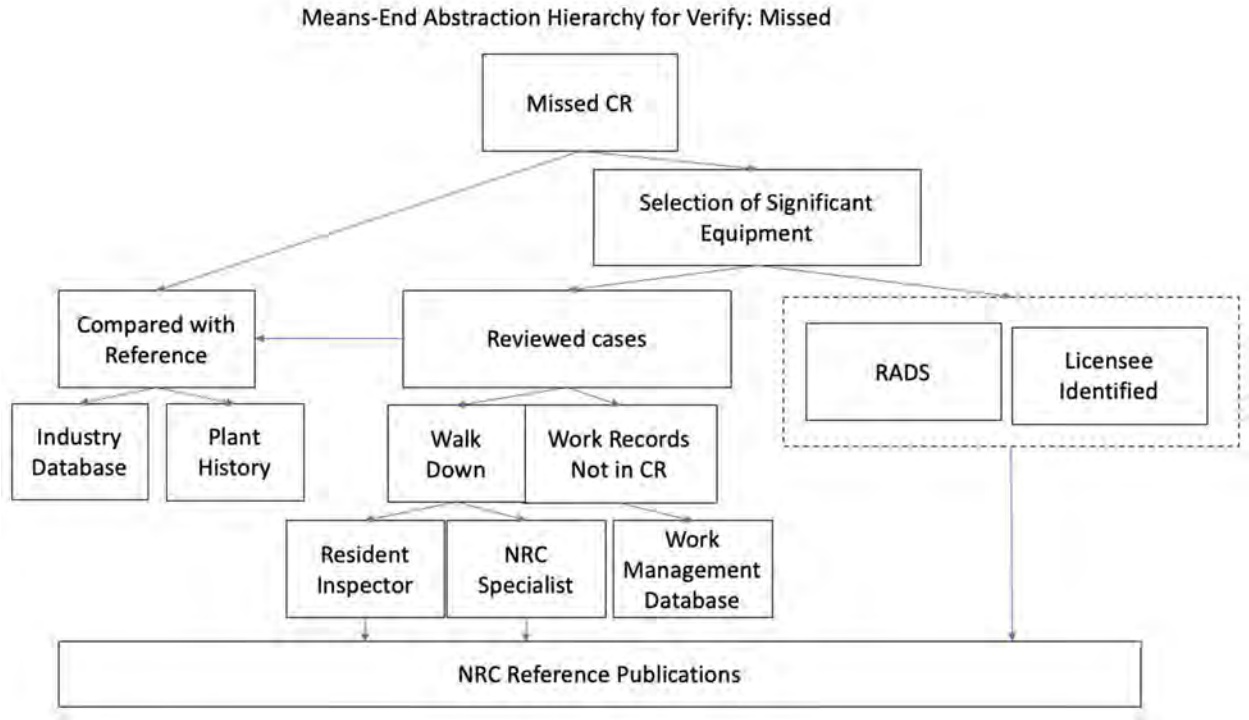

Figure 10. Missing CR Drill-down of Verify Correct Identification

Finally, there must be a process by which the reviewed cases are compared with source references to give a sense of frequency and duration by which these omissions occurred. These reference sources include previous omissions with the plant itself, as well as industry-wide data. As can be seen, NRC publications are a reference source at several points in the process.

3.2.2 Rectified CRs

Figure 11 completes the depiction of the Verify Correct Identification means-end abstraction hierarchy by showing a drill-down for the Rectified CR process. In this case, the inspector has a database of existing CRs and must select an appropriate sample for review. The samples fall into three categories: CRs still open but open too long, CR closed, but not in a timely manner, and CRs not properly closed.

These samples, once identified, must then be compared with databases on similar CRs in the plant, and in the industry as a whole. Not depicted but implied is a linkage to the significance component in the previous figure. The requirement for comparison with similar CRs assumes that there are available databases for both plant and industry in which CRs can be sorted according to four criteria: relevant dates, issue categorizations, deficiency classifications, and Corrective Action Program (CAP) if-then statements. The assessment of whether CRs have been open too long, or not closed in a timely manner, as shown in Figure 11, requires access to time histories of similar CRs. The assessment of proper closure requires access to CAP If-Then statement compliance history. Finally, as in the previous figure, NRC documentary materials are available for reference. As a reminder, while not explicitly depicted in this analysis, Figure 7 implies the requirement that sampling of cases for investigation between distributed across the cornerstone areas.

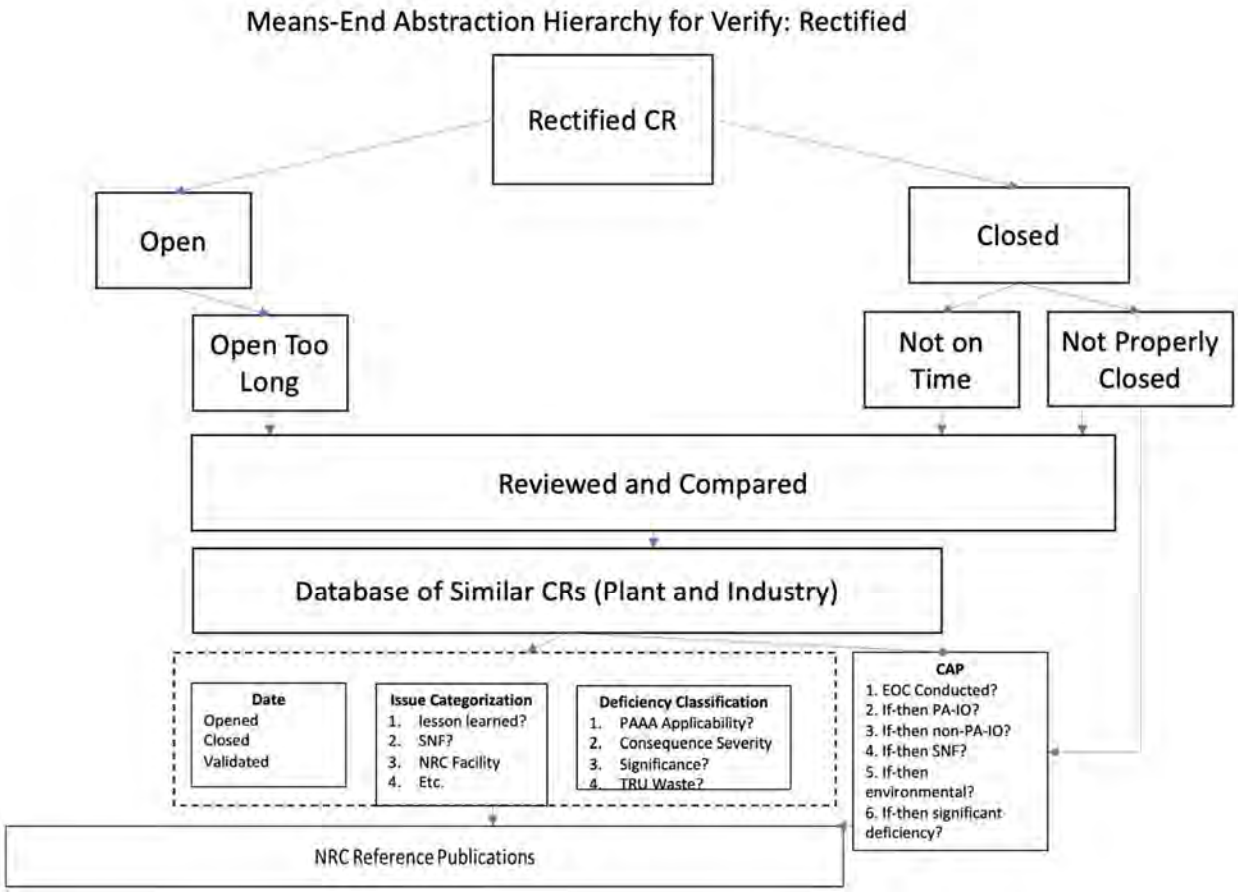

Figure 11. Rectified CR Drill-down of Verify Correct Identification

3.3 STPA: Control Structure

The control structure – more properly safety control structure – is a component of the STPA methodology (Leveson 2011) which itself is a component of a higher-level STAMP framework. As discussed above, STPA grew out of the CWA environment, and the current analysis represents an updating of both methodological frameworks. Simply put, STPA provides the control system logic for potential actions made possible by the structure of the work domain.

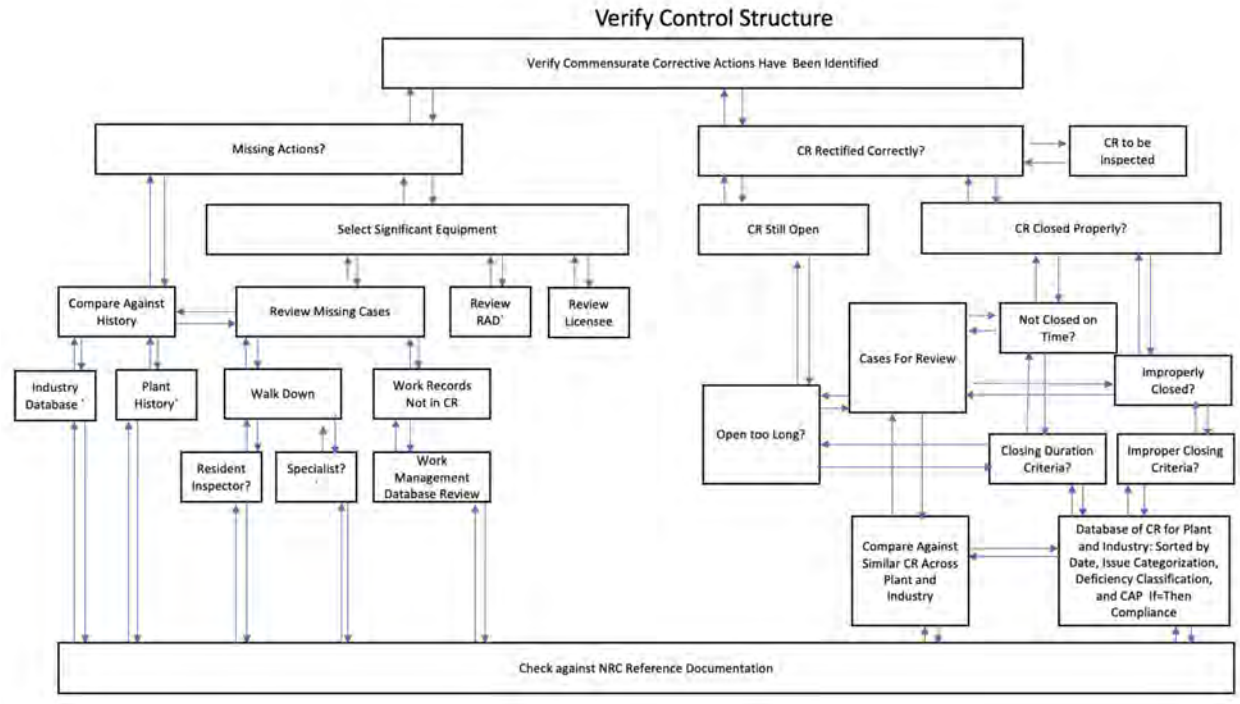

Figure 12. Control Structure for Verify Correct Identification

In this diagram, arrows link controllers and controlled processes. In more detailed analyses, there would be individual labels on arrows, but for this depiction, assume that arrows leaving a box represent either commands, or queries, and arrows entering a box represent responses. It should also be noted that control structures mirror the level of resolution of the part-whole dimension of WDA. Almost any element in Figure 12 could be represented by a more elaborate structure.

This diagram should be within the context of Figure 9 and Figure 10; these figures depict the domain in which these control actions take place. The initial action requires the inspector to verify that corrective actions have been accomplished. To do that he/she needs to both search for cases where CRs should have been created but were not, as well as review existing CRs.

3.3.1 Missing CR

The left-hand part of the diagram starts with a query regarding missing actions. A subtask of this query requires the action of selecting safety significant equipment as potential samples for inspection. This, in turn, may require reviewing RADS documentation as well as the list of licensee safety significant equipment.

Once a candidate set of equipment samples for missing cases has been selected, there are two different options for further selection. Work Records may be reviewed to determine if deficiencies/workarounds were accomplished without being recorded in CRs. This action requires reviewing work management databases. Also, Walk Down Inspections may be carried out. This may be done by the Resident Inspector, or a Specialist Team may be required.

Finally, the results of inspections from both pathways must be compared against prior history. This is accomplished at both the plant and industry levels.

3.3.2 Rectified CRs

The right-hand side of Figure 12 depicts the second process which begins with a different question: Have the CRs which were created rectified correctly? This can be broken down into two sub-tasks:

examine CRs still open and examine CRs which have been closed. From these CRs, cases for review must be selected. As can be seen, there are three potential sources of such cases: CRs which were open too long, CRs, which not closed in time, and CRs which were improperly closed. The first two sources require reviewing existing criteria for appropriate closing durations. These, in turn, may be obtained from existing databases of time histories of CRs. The third source – improper closing – requires examination of the details of the CAP process documented in the CR with particular reference to the required sequence of If-Then statements which are part of that documentation.

Cases selected for review must then be compared with similar CRs in the plant and across industry. Determination of similarity can be determined with reference to CR attributes. These may include, but are not limited to, relevant dates, issue categorization, deficiency determination, and CAP compliance.

Note that, for almost all of these actions, appropriate NRC documentation is available for review.

3.4 STPA: Unsafe Control Actions and Scenarios

3.4.1 Unsafe Control Actions

As discussed in Section 2.3.3.2, this stage of STPA is where the individual decision actions depicted in the control structures in Figure 12 are examined in detail. In this case, in order to demonstrate the operation of the process, an oversimplified example using hypothetical placeholders will be used. The focus will be on the action from Figure 12 in which the inspector must decide if a given CR has been "not closed in time." See Figure 13 for an enhanced view limited to just this portion of the control structure. Note, however, that the single box corresponding to the not closed in time decision has been replaced by a detailed description of the human control process of the inspector. This description has been taken from the top part of Leveson's (2020) Figure 10 (shown as Figure 4 previously in Section 2.3.3.2).

The specific actions related to the decision regarding the timing of the CR is analyzed in terms of the possibility of Unsafe Control Actions (UCA). "Unsafe" in this context refers to those actions that could result in losses. The results are summarized in UCA Table 2 (Leveson and Thomas 2018.)

Table 2. Unsafe Control Actions

Control Action	*Not Provided Causes Loss*	*Provided Causes Loss*
Decision: CR has been open too long	UCA1*:* H1	UCA2: H2

UCA1 results in an unacceptable outcome when the CR under review has, by some external criterion, been open too long but the inspector fails to make this decision. This results in H1: Overlook critical content in inspection leading to loss. UCA2 is an unacceptable outcome when the CR under review is judged by the inspector to have been open too long, but this is an incorrect decision by some external criterion. This results in H2: Devotes unnecessary or excessive time and effort in inspection leading to loss. See Table 1 for original losses and hazards. Note that each UCA is associated with one or more specific hazard, and each hazard, in turn, is associated with one or loss. In this way, the process requires traceability from individual actions to higher level priorities.

3.4.2 Scenarios

Scenarios are constructed once the set of UCAs has been determined. A scenario describes the causal factors that could lead to the UCA and the associated hazard and corresponding losses (Leveson and Thomas 2018). Multiple scenarios can be proposed for any single UCA. When a human controller is involved, the scenario takes into account the modified structure of the human controller model, as described previous in Section 2.3.3.2. Note that the human model has a combined function of generating control functions and mental processing. In addition, as can be seen, four types of mental models may be present.

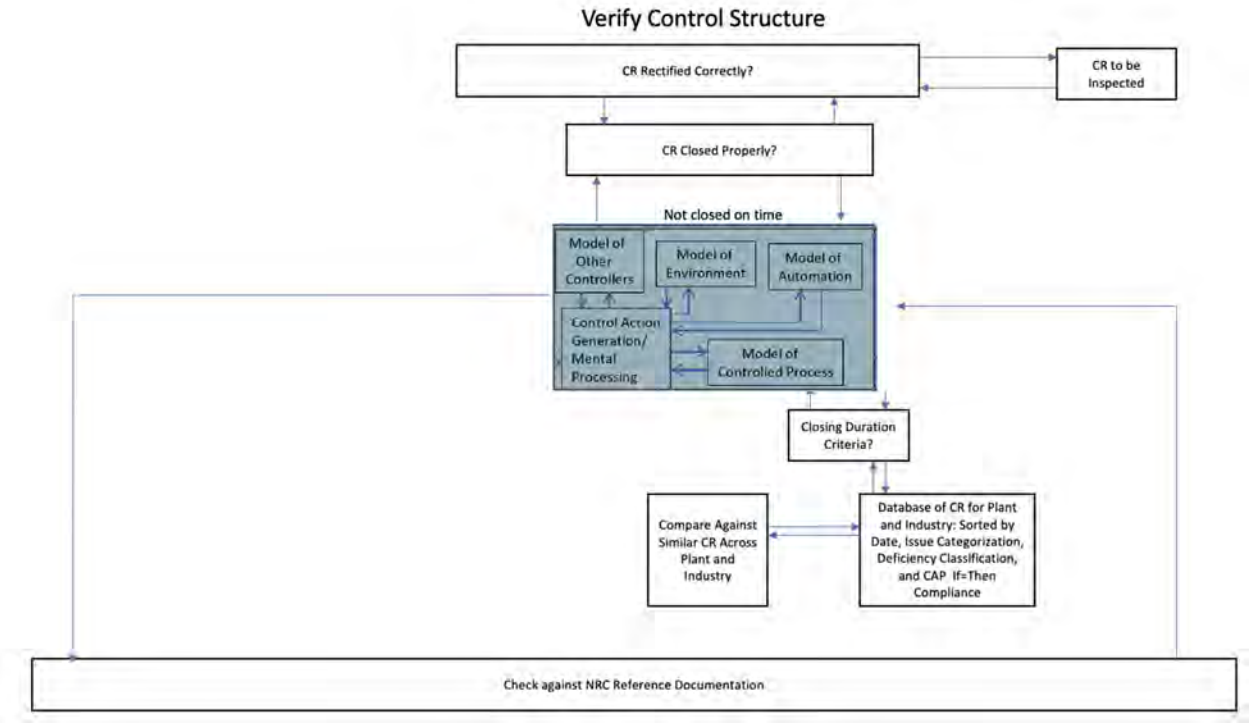

Figure 13. Control structure for closing duration

In constructing scenarios, the human controller model is examined in combination with other elements of the control structure seen in Figure 13. In this simplified example, it is assumed that there is some sort of data store reflecting criteria for CR closing durations. This, in turn, draws from a database of CRs for the plant and industry, as well as a database of closing times for CRs with similar characteristics. Finally, NRC guidelines, standard operating procedures, and training materials are available which are relevant to the decision.

In the human controller model, the model of the controlled system would reflect the inspector's perception of the structure and contents of the CR that is being assessed. The inspector would be using mental processes to examine contents of other mental models so as to generate a control action (i.e., decide whether the CR as either open too long, or not open too long). These other mental models would include the inspector's understanding of the contents of CR closing criteria, reviewing relevant information in the CR database, as well previous training, and understanding of other colleagues' behavior.

UCA1 occurs when an inspector incorrectly fails to recognize that a CR has been open too long. In Scenario 1, a possibility is that the CR was incorrectly identified as one which would normally be opened longer than typical. The incorrect classification was attributed to inconsistent labeling of CR type classified by duration.

UCA2 occurs when an inspector incorrectly judges that a CR has been open too long. In Scenario 2, a possibility is that the CR was again incorrectly identified as was the case in the previous scenario.

In both of these cases, a system constraint has failed to be maintained (SC2.1: Issues must be resolved without inappropriate delay). Moreover, it appears that the same solution for both scenarios is a more effective labeling of distributions of CRs by type and appropriate delay.

3.5 Visualization: Ecological Interface Design

Finally, to complete the loop, the logical practical end result of the enhanced STPA/WDA methodology is to solve the visualization problem by developing user interfaces (i.e., EIDs). EID utilizes the results of STPA/WDA to organize the data into meaningful chunks of information so as to allow the user to be able to form and maintain up-to-date mental models with as little effort and as accurately as possible (Kovesdi et al. 2021b).

Section 2.3.4 discussed the basic perspective of EID. The representation in Figure 14 (a repeat of Figure 5) is offered as an alternative method of representing the methodology and findings thus far presented in order to link them more closely with the requirements of Sections 1.1.3, and 1.1.4.

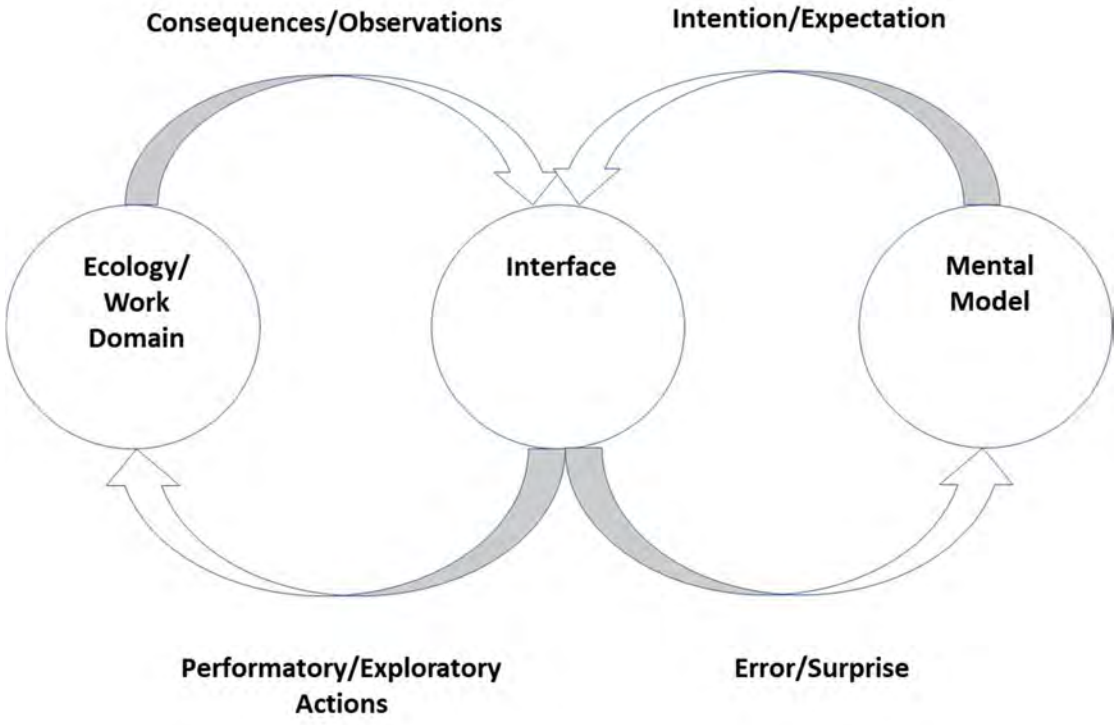

Figure 14. Three-part framework for EID. Modified from Bennett and Flach (2011, Figure 2.3).

The three components allow for the three-way interaction among the work domain, user interface, and the user's mental model. The intervening perception and action links allow for a dynamic depiction of the process of data being transformed to information, then to insight, and then to action. On the right component is the controller mental model, as described earlier in Figure 4 in Section 2.3.3.2. A control action originated by the user is labeled Intention/Expectation and it is a query addressed at the interface. In the current case, it would be the inspector searching for a CR to examine within the repository of CRs. This logically requires a second Performatory/Exploratory link to the work domain and the corresponding appearance of an Observation (i.e., a case record). The feedback signal (Error/Surprise) indicates that he/she has successfully found a CR to investigate. The mental model is updated, and an Intention is sent to the user interface allowing the inspector to explore the electronic version of the CR. As the user's mental model is being modified by new insights, an updated intention is sent to the user interface looking to compare this CR type with others of a similar type in terms of average duration. Assuming that the user interface is so organized, a new exploratory command can be formulated, which will result in the required information appearing in the interface, and the resulting feedback (Error/Surprise link) allows further

updating the mental model. If the required information were not available, an error signal would be received, and a different set of intentions would be generated.

This process would continue until the inspector's assessment is complete. An intention to register the assessment goes to the interface, and a performatory signal registering the decision is sent to the appropriate location in the work domain.

For this process to work systematically, independent of whatever technology is or is not present, requires that the STPA-modified approach to WDA characterized the data infrastructure in functional terms. The Control Structure, with its analysis of USCs and associated scenarios, ensures that the if appropriate inspector intentions are stated, that the data base is correspondingly mapped and organized. The principles of EID assures that the designed information can be visualized in such a way that the inspector's mental models can be appropriately modified allowing for insight and action.

In terms of the automation problem, this initial human analysis would afford a baseline for examining potential candidates for automation. The second component of Figure 4 in Section 2.3.3.2 could be run in parallel with the first to examine not only the replacement of human decision-making with automation but possible synergies between them.

4. SUMMARY OF FINDINGS

4.1 Findings for Objective 1

Objective 1: Provide planning tools and comprehensive guidance on how HTI principles and information automation technologies enable data integration and coordination for full nuclear plant modernization.

In approaching that objective, we examined the data evolution problem as posed in the context of NPP Modernization. As stated in Section 1.1.3, the two attributes of data evolution—mapping and management—must be applied to the three data issues for NPP modernization: acquisition, analysis, and action. HTI principles require that the technological aspects of data evolution be integrated with the needs, capabilities, and limitations of human users of that technology. Our assessment of the literature was that the integration of Work Domain Analysis, STPA, and Ecological Interface Design provide an approach to this requirement. A use case related to the NPP problem of assurance-NRC inspection-was identified, and a feasibility analysis using these integrated methodologies carried out.

4.2 Findings for Objective 2

Objective Two: Develop a conceptual model of information automation within a NPP information and computer architecture ecosystem. The integrated conceptual model is laid out in detail in Section 2.

4.3 Findings for Objective 3

Objective Three: Illustrate potential applicability to a specific use case. The applicability of the approach to the NRC Inspection use case is fully described in Section 3.

4.4 Findings for Objective 4

Objective Four: Identify potential near- and longer-term information automation application areas. The use of the modified Work Domain analysis allows us to specify details of data mapping and management in functional terms. We could trace either an existing or proposed data architecture from acquisition to analysis to its location and form such that it could be utilized for a human operator to develop the appropriate insight so as to perform an appropriate action. As such, the same analysis could be modified to accomplish the same goal for an automatic decision process. Consequently, the procedure is scalable, and generalizable to many other NPP domains. Immediate examples include analysis of the Corrective Action Program procedures, and information support systems for operational forcing function meetings such MRMs.

4.5 Specific Findings (Conceptual Model, Requirements, Unknowns, and Application Areas)

We have demonstrated the use of a conceptual model that, within the specific use case of an NRC inspector performing a Verify Corrective Actions task in conjunction with the Routine Review component of PI&R, addresses the data evolution problem outlined in Section 1.1.3. With respect to the specific functional components of that task, the model allows us, in principle, to identify the data mapping and management attributes of the acquisition, analysis, and action processes. (For example, what are the sources of data that indicate that a given type of CR has been open too long, and how are they organized, and in what form are they available to the inspector?).

The model allows us to analyze the control logic required of the inspector in making his/her decision and identifies potential areas where errors could occur. Moreover, it provides the possibility for development of solutions which might mitigate such errors. This type of analysis would be critical to assess if any aspect of this task were automated.

With regard to the practicality of employment of the model, Naikar (2013) has presented a set of criteria for assessing both the *usefulness* and *feasibility* of applying these kinds of 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 (e.g., schedule, staff, and financial budget).

As discussed in Dainoff et al. (2020), both WDA and STPA have large communities of practice and there are many previous examples of usefulness of these methods. With specific reference to uniqueness, these approaches have a flexibility and scalability that are an appropriate match for the complexity of the NPP modernization problem. In terms of feasibility, the experience within the STPA community of practice is that the time and effort required to conduct such analyses can be orders of magnitude less than traditional hazard analyses. Moreover, both of the methods are derived from the same underlying socio-technical systems perspective. As such, they can be scaled up or down depending on user need. For example, valuable insights can and have been attained by applying the underlying logic at a high level of abstraction—requiring a relatively small amount of resources while affording a global overview of the problem space.

Finally, with respect to uncertainties, we have indicated that, for this use case, practical constraints require the use of placeholders. In an actual analysis, additional subject matter expertise would be required, and the analysis would likely more complicated. This is not a seen a major drawback since WDA/STPA is a mature methodology with ample evidence of implementation with actual information rather than placeholders.

4.6 HTI-relevant findings (what role did HTI principles play in the current effort, what role should they play going forward, what sorts of HTI-relevant issues/findings were uncovered?).

The WDA/STPA methodology utilized in this use case can and has been used for strictly automatic processes with no human operators. However, for the foreseeable future, humans will be involved in the design, operation, and management of complex systems like NPPs. At a very general level, all of these human roles deserve the same kind of information support and visualization capability that is currently devoted to control room operators. Consequently, HTI is an integral component of this method.

Specifically, HTI is the third of four components within the Plant Modernization Research Pathway (See Section 1.1.1)—receiving the outputs of the Digital Infrastructure and Data Architecture research areas. Within the data evolution framework (Section 1.1.2), HTI is explicitly involved in the third component—developing appropriate action based on analysis (including visualization). In the present use case, the WDA/STPA model is the mechanism by which HTI receives the outputs of Digital Infrastructure and Data Architecture. These outputs are used within the model to (a) ensure that the human operator/controller has adequate information resources to develop appropriate actions; and (b) that such information is effectively organized to allow the operator/controller to visualize those information resources.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Implications of Findings for ION

WDA-STPA is a high-level socio-technical method for achieving joint optimization of complex work systems, where joint-optimization is defined in terms of the balance among efficiency (cost)-effectiveness (functionality) and safety (minimization of loss). Joint optimization would seem to be key to the basic goals of ION; seeking to reduce costs and inefficiency while maintaining effectiveness and safety.

Redundancy provided by human operators in traditional NPPs—affording multiple opportunities to catch errors—is replaced by automation. It is essential, therefore, that the remaining humans are provided proper information support/visualization to replace the lost redundancy.

The WDA/STPA methodology can provide that support. In particular, the application of the Means-End Abstraction Hierarchy poses the question: In what sense does a given set of data constitute a means to a higher-level functional end (goal)? If the answer is positive, this means-end linkage is inherent in the system design logic insofar as this logic satisfies the original intentions of the coordinated decision-making of the designer and the customer.

In Levison's (2020) conceptual architecture concept, these high-level intentions, along with potential losses, hazards, and required safety constraints, are specified early in the design process, before any specific engineering design decisions are made. Moreover, the formative nature of the process provides opportunities to ensure that critical safety constraints are maintained while reducing unnecessary persons/procedures.

5.2 Recommendations

5.2.1 Near-Term ION Design, Development, and Implementation Recommendations

5.2.1.1 Expand NRC Use Case

The first recommendation is to expand the current NRC use case by replacing placeholders with actual data sources. Expanding this use case would allow researchers to explore automation possibilities. As mentioned previously, compliance activities are estimated to account for as much as 50% of non-fuel and non-capital costs of plant operation. How much the licensee's costs associated with complying with the NRC PI&R could be reduced by automating certain aspects of the process is a topic is the next obvious question that should be researched.

5.2.1.2 Expand Dashboard Use Case

The second recommendation is to expand the dashboard collaboration project initiated in FY21 (see Kovesdi et al., 2021b) to develop working prototypes of a dashboard to enable better situation awareness in the NPP as an organization. In the same way that Joyce and Lapinsky (1983) describe the development of the SPDS for the NPP main control room to help the licensed operators formulate a common and correct mental model of the plant's state, we envision the development of various dashboards that will help staff at an NPP (i.e., compliance specialists, engineering, auxiliary operators, maintenance technicians, radiation protection technicians, business support staff, supervisors and line management) formulate a common and correct mental model of the ways in which each person's job interacts with other people's jobs. This organizational situation awareness[a] is a key first step in achieving one of ION's primary goals of joint optimization.

[a] See also the notion of "Interpredictabilily" and other teaming constructs in Klein, Feltovich, Bradshaw, and Woods (2015). Common Ground and Coordination in Joint Activity.

5.2.2 Longer-Term ION Design Development, and Implementation Recommendations

The third recommendation based on the content of this report is to explore additional collaboration possibilities for generalizing the WDA/STPA methodology to broader examination of the data evolution problem. Along with the many different kinds of SMEs at an NPP (e.g., specialists and technicians), there are many different departments or organizational entities, including:

- Operations
- CAP Management
- Engineering (e.g., Design and Project Engineering)
- Outage Management
- Line Management (e.g., Oversight, Compliance, and Performance)
- Radiation Protection and Chemistry
- Security
- Maintenance (e.g., System Health and Equipment Reliability)
- Training

As this research demonstrates its feasibility in reducing operations and maintenance costs in the specific use cases described above, there ever-expanding opportunities to apply its findings to other parts of the NPP organization where improved situation awareness is needed to enable joint optimization of cost, performance, and safety.

6. REFERENCES

Al Rashdan, A., Browning, J., and Ritter, C. 2019. "Data Integration Aggregated Model and Ontology for Nuclear Deployment (DIAMOND): Preliminary Model and Ontology." INL/EXT-19-55610. Idaho National Laboratory.

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

Burns, C. and Hajdukiewicz, J. 2004. *Ecological Interface Design*. Boca Raton: CRC Press.

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

Flach, J., and Dominguez, C. 1995. "Use-Centered Design: Integrating the User, Instrument, and Goal." Ergonomics in Design 3(3): 19–24.

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

Joe, J., Miyake, T., and Hall, A. 2021. "Guidance on Transforming Existing Light Water Reactors into Fully Modernized Nuclear Power Plants: The Role of Plant Modernization R&D." INL/LTD-21-64369, Idaho National Laboratory.

Joyce, J. and Lapinsky, G. 1983. "A history and overview of the safety parameter display system concept." IEEE Transactions on Nuclear Science 30(1): 744–749.

Kovesdi, C., Spielman, Z., Hill, R., Mohon, J., Miyake, T., and Pederson, C. 2021a. "Development of an Assessment Methodology That Enables the Nuclear Industry to Evaluate Adoption of Advanced Automation." INL/EXT-21-64320, Idaho National Laboratory.

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

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

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

Little, E. 2009. On an Ontological Foundation for Work Domain Analysis. In Applications of Cognitive Work Analysis edited by A. Bisantz and C. Burns, 301–319. Boca Raton: CRC Press.

Naikar, N. 2013. *Work domain analysis: Concepts, guidelines, and cases*. Boca Raton: CRC Press.

Poh, J. 2022. *A Top-Down, Safety-Driven Approach to Architecture Development for Complex Systems*. Cambridge: Massachusetts Institute of Technology.

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