BNL-91047-2010

The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance: HFE Review Guidance and Technical Basis

John O'Hara, Bill Gunther, and Gerardo Martinez-Guridi

February 2010

Energy Sciences and Technology Department

Brookhaven National Laboratory
P.O. Box 5000
Upton, NY 11973-5000
www.bnl.gov

DISCLAIMER

Human Factors Aspects of Operations Under Conditions of Degraded I&C (NRC JCN N-6526)
Technical Report BNL-91047-2010

The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance: HFE Review Guidance and Technical Basis

Prepared for

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Prepared by

John O'Hara, Bill Gunther, and Gerardo Martinez-Guridi
Brookhaven National Laboratory
Energy Science and Technology Department
Environmental and Systems Engineering Division
Upton, New York 11973

February 26, 2010

ABSTRACT

Integrated digital instrumentation and control (I&C) systems in new and advanced reactors will support operators in monitoring and controlling the plants. Even though digital systems typically are highly reliable, their potential for degradation or failure significantly could affect the operators' performance and, consequently, jeopardize plant safety. The U.S. Nuclear Regulatory Commission (NRC) supported this research project to investigate the effects of degraded I&C systems on human performance and on plant operations. The objective was to develop guidance for human factors engineering (HFE) reviews addressing the operator's ability to detect and manage degraded digital I&C conditions. We reviewed pertinent standards and guidelines, empirical studies, and plant operating experience. In addition, we evaluated the potential effects of selected failure modes of the digital feedwater-system on human-system interfaces (HSIs) and the operators' performance. Our findings indicated that I&C degradations are prevalent in plants employing digital systems, and the overall effects on the plant's behavior can be significant, such as causing a reactor trip or equipment to operate unexpectedly. I&C degradations may affect the HSIs used by operators to monitor and control the plant. For example, deterioration of the sensors can complicate the operators' interpretation of displays, and sometimes may mislead them by making it appear that a process disturbance has occurred. We used the information obtained as the technical basis upon which to develop HFE review guidance. The guidance addresses the treatment of degraded I&C conditions as part of the design process, and the HSI features and functions that support operators in monitoring the performance of the I&C system and managing any degradations that occur. In addition, we identified topics for future research.

ACKNOWLEDGMENTS

This research was sponsored by the U.S. Nuclear Regulatory Commission. The views presented represent those of the authors alone and are not necessarily those of the NRC. The authors wish to thank NRC Project Manager Jing Xing for her careful review, recommendations, and suggestions throughout the project, and Michael Boggi, former NRC Project Manager, for his guidance and input during the development stages of this research. We are grateful to Val Barnes of the NRC, and Jim Higgins of BNL for their insights and helpful comments. We also thank Avril Woodhead for her technical editing of this report and Maryann Julian for preparing the manuscript.

CONTENTS

Part 2: HFE Guidelines for the Review of The Effects of Degraded I&C Conditions on HSIs and Operator Performance

FIGURES

TABLES

ABBREVIATIONS

Abbreviations	Definition
A/M	auto/manual
AEOD	Analysis and Evaluation of Operational Data
ANSI	American National Standards Institute
ATHEANA	A Technique for Human Event Analysis
B/U	bypass unit
BCPU	backup central processing unit
BFRV	bypass feedwater regulating valve
BFV	bypass feedwater valve
BIT	boron injection tank
BNL	Brookhaven National Laboratory
BTP	branch technical position
CBP	computer-based procedure
CCF	common cause failures
CFR	U.S. Code of Federal Regulations
CPB	computer-based procedure
CPU	central processing unit
D3	diversity and defense-in-depth
DCS	distributed control system
DEV	deviation alarm
DFWCS	digital feedwater control system
DI&C	digital instrumentation and control
DOE	Department of Energy
DPCS	digital plant control system
DPI	direct perception interface
DURESS	DUal REservoir System Simulation
EDG	emergency diesel generator
EHC	electrical and hydraulic controller
EID	ecological interface design
EOP	emergency operating procedures
EPRI	Electric Power Research Institute
EQ	equipment qualification
ERDADS	emergency response data acquisition and display system
ERFDS	emergency response facility data system
FMEA	failure modes and effects analysis
FWP	feedwater pump
FWS	feedwater system
HFE	human factors engineering
HPCS	high pressure core spray
HRA	human reliability analysis
HSI	human-system interface
I&C	instrumentation and control
I/O	input and output
IAEA	International Atomic Energy Agency
IE	initiating event
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute for Nuclear Power Operations
ISG	interim staff guidance
LER	licensee event report

Abbreviations	Definition
LOCA	loss of coolant accident
M/A	manual/automatic
MCPU	main central processing unit
MCR	main control room
MFRV	main feedwater regulating valve
MFV	main feedwater valve
MUX	multiplexer
NEI	Nuclear Energy Institute
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OHA	overhead annunciator
ORE	operator reliability experiment
PC	plant computer
PDI	pressure differential indication
PDU	plasma display unit
PID	piping and instrumentation display
PORV	power operated relief valve
PRA	probabilistic risk assessment
PWR	pressurized water reactor
RCIC	reactor core isolation cooling
RCS	reactor coolant system
RG	regulatory guides
RIS	regulatory issue summary
RMU	remote multiplexing units
RV	reactor vessel
S/G	steam generator
SI	safety injection
SRP	Standard Review Plan
SSPS	solid state protection system
TCT	trial completion time
TEST	to ensure safe testing
TR	technical report
U.S.	United States
VFD	variable frequency drive

Part 1:

Technical Basis and Guidance Development

1 INTRODUCTION

1.1 Background

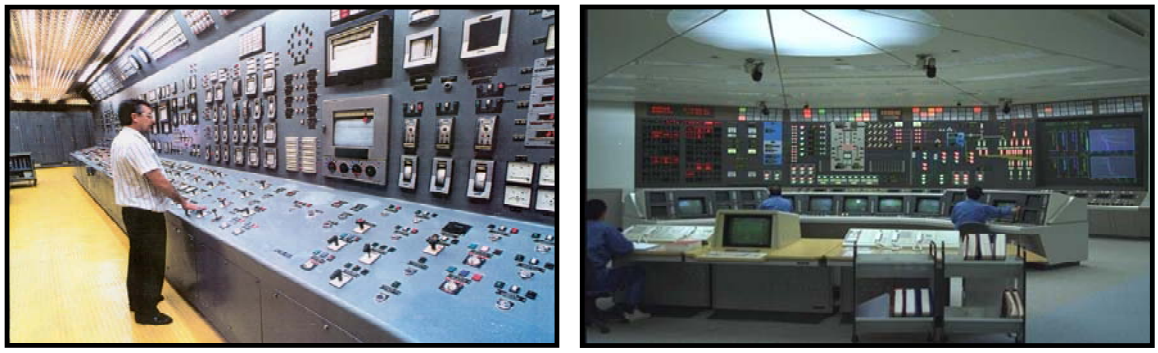
The design of new nuclear power plants (NPPs) differs in several important respects from those currently operating in the United States (U.S.), including their instrumentation and control (I&C) systems and human-system interfaces (HSIs). Current plants employ predominantly analog I&C technology, while new plants are designed to use digital I&C technology. The latter systems expectedly will offer functions and capabilities that are vital for performance and plant safety. Together with the plant's personnel, the I&C system might be considered as the plant's "central nervous system". It senses basic parameters, monitors the plant's processes, performance, and various barriers that prevent release of radioactive material, and adjusts operations as needed. It also responds to transients, accidents, and other failures. Modern digital systems undertake sophisticated monitoring of the equipment's condition and contain diagnostic- and prognostic-functions. They also are able to implement control algorithms that are more advanced than used in plants to date, e.g., techniques for optimal control, nonlinear control methods, fuzzy logic, neural networks, state-based control, and adaptive control (a control that modifies its behavior based on the plant's dynamics)(O'Hara et al., 2008b). Employing these advanced techniques will assure more intricate and more complex control of plant systems and processes.[1] Digital I&C systems also support increased automation and new forms of automation that make greater use of interactions between personnel and automatic functions.

Another difference between the designs of current and new plants lies in their HSIs. The analog HSIs in most plants now operating in the U.S. have hardwired controls (e.g., switches, knobs, and handles) and displays (e.g., alarm tiles, meters, linear scales, and indicator lights), arranged on control boards. Operators walk the boards, and accomplish their tasks via paper procedures. New NPPs have computer-based HSIs organized into sit-down workstations (Figure 1-1) from which personnel monitor the plant through screen-based displays. Soft controls, accessed through computer workstations, control the plant's equipment. In many new control room designs the procedures will be computer-based, offering the potential to take control actions directly from the procedure display, including semi-automated control with the operator authorizing the procedure to perform a series of actions.

We note that digital I&C and HSI technology can be retrofitted into current plants. In fact, many operating U.S. plants are planning modernization projects to replace their analog I&C systems and HSIs with new digital systems (O'Hara, 1998, 2000, & 2004).

Although digital technology potentially can improve operational performance, there are challenges to using this technology in NPPs. One of these challenges concerns the impact of I&C degradations on personnel's performance.

[1] Increases in sensing capabilities, information-processing support, intelligent agents, automation, and software-mediated interfaces extends the "distance" between personnel and the physical plant. Although these technologies potentially are beneficial, sometimes they add to complexity for personnel operating and maintaining the plant.



Control Room with Analog HSIs Control Room with Computer-based HSIs

Figure 1-1 Typical HSIs in many current plants (left) and new plants (right)

The subject of degraded I&C systems was identified in earlier research sponsored by the U.S. Nuclear Regulatory Commission (NRC) to identify potential human-performance issues related to introducing emerging technologies in NPPs (O'Hara et al., 2008a, 2008b). The authors identified 64 issues that subject-matter experts then prioritized. Twenty issues ranked as top priorities included "Operations under conditions of degraded instrumentation and controls." The importance of such conditions stems from the I&C system's function. As described above, the I&C system, together with plant personnel, monitor performance, take control actions, and respond to failures and off-normal events, thus ensuring the goals of efficiently and safely producing power. Through the control room's HSIs, the I&C system provides information to plant operators and the means to control plant's equipment (Figure 1-2).

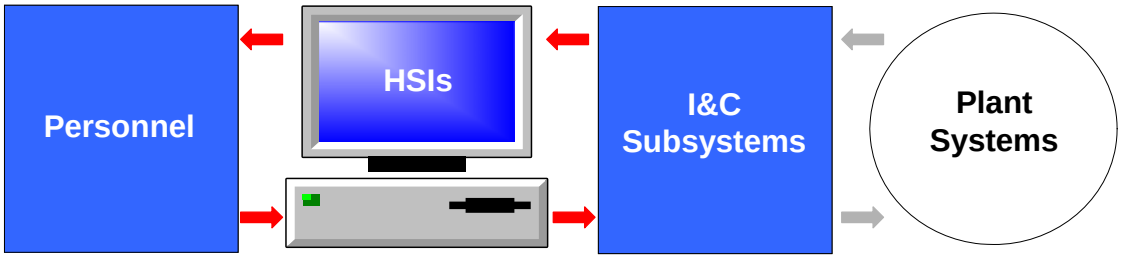


Figure 1-2 Three main levels of personnel interaction with the I&C system

Thus, I&C degradation may significantly lower the operator's ability to monitor the systems and control tasks. Failure or degradation of I&C systems can pose additional problems by causing abnormal operating conditions due to erroneous automatic action. Some human-performance considerations in dealing with operations under degraded conditions included detecting the failure of the digital system, and the ability to transition to back-up systems when failures occur.

The Electric Power Research Institute (EPRI) and the Nuclear Energy Institute (NEI) similarly highlighted degraded I&C systems as a technical issue facing new plant development (Torok et al., 2006). Specifically, "Failure management for new HSIs" was defined as

> Practical criteria and methods are needed for addressing partial or large-scale failures of the HSIs normally used by the operators. This is especially applicable to new plant control rooms, which will be

more integrated and digital than operating plant control rooms. Specific issues include appropriate operation under degraded I&C and HSI conditions, what backups should be provided, when to switch to backups, and the human factors engineering (HFE) issues associated with switching to backups, as well as integration of backups into the overall control room design.

1.2 Research Objectives

The objectives of this NRC research project are to (1) identify the effects of degraded I&C conditions on the operator's performance, and (2) develop HFE review guidance that NRC's staff can follow to address the detection and management of degraded I&C conditions by personnel. For the purposes of this study, "degraded" refers to a full range conditions, from relatively minor loss of functionality to the complete failure of a digital I&C system.

The scope of this research is limited as follows:

- The focus is on control room operations, even though we recognize that maintaining digital systems also is a very significant consideration (O'Hara et al., 1996)
- Assessment of degraded conditions is limited to typical situations wherein I&C systems may degrade, and not those due to intentional actions, such as sabotage or cyber attacks.

The guidance resulting from this research will be integrated into the appropriate HFE review guidance documents, such as the *Standard Review Plan*, Chapter 18, Human Factors Engineering (NRC, 2007), the *Human Factors Engineering Program Review Model* (NUREG-0711; O'Hara et al., 2002), and the *Human System Interface Design Review Guidelines* (NUREG-0700; O'Hara et al., 2004). The guidance will support the NRC staff's review of new plants, and of digital I&C upgrades to existing plants.

1.3 Organization of the Document

This report is divided into two parts. Part 1 describes the technical basis and the process for guidance development. Part 2 contains the guidance for reviewing the HFE aspects of degraded I&C conditions.

In Part 1, Section 2 describes the methodology we used to develop the HFE review guidance. Section 3 characterizes the I&C system, HSI, and human performance. Section 4 details the results of our analyses of the technical basis for determining the effects of degraded I&C conditions on human performance, and mitigating those effects. Section 4 also includes topics for possible future research. Section 5 presents our overall conclusions, and Section 6 gives references to cited works.

In Part 2, Section 8 has guidance for reviewing an applicant's design process and for reviewing the HSIs used to monitor the I&C system and manage its degraded conditions.

The Appendix to this report gives additional details about the analysis described in Section 4.4 of the impact on HSIs and operators of the degradation of a digital I&C in a feedwater system.

2 METHODOLOGY

The NRC established a methodology to develop HFE review guidance to address safety review needs (O'Hara et al., 2008a). Figure 2-1 is an overview of the main steps in the process. A central tenet of the method is establishing the guidelines' validity. Validity is defined along two dimensions: Internal and external validity. Internal validity is the degree to which individual guidelines are linked to a clear, well-founded, and traceable technical basis. External validity is the degree to which independent peer review supports the guidelines. Peer review is a good method of evaluating guidelines for conformance to generally accepted HFE practices and to industry-specific considerations, i.e., for ensuring that the guidelines are appropriate with respect to practical operational experience of actual systems.

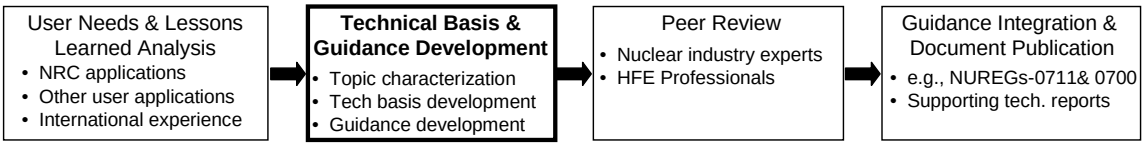


Figure 2-1 Major steps in developing NRC HFE guidance

Of the four steps shown, this research project addresses the second, viz., technical basis and guidance development. The first step of the methodology was researched earlier (O'Hara et al., 2008a, & 2008b) when "Operations under conditions of degraded I&C" was identified as a top-priority issue. The last two steps will be conducted in a future research project to update the NRC's HFE-review guidance.

Technical basis and guidance development involves several phases including topic characterization, technical-basis development, and guidance development and documentation. We discuss each in this section (see Figure 2-2).

2.1 Topic Characterization

The first step in developing guidance for any topic is to characterize it, that is, describe the topic's key elements. The characterization serves several purposes:

- it provides a way of organizing the analysis of research studies, operational events, and the like into a standardized language to support formulating more general insights
- it offers a structure for developing and organizing the guidance
- it gives reviewers a process for requesting information from applicants and licensees during a review

In the present context, a characterization is needed describing how the degraded I&C conditions impact the performance of operators. The three essential levels must be discussed to establish such a linkage: The I&C system, the HSI, and human performance (see Figure 1-2). The topic characterization is detailed in Section 3.

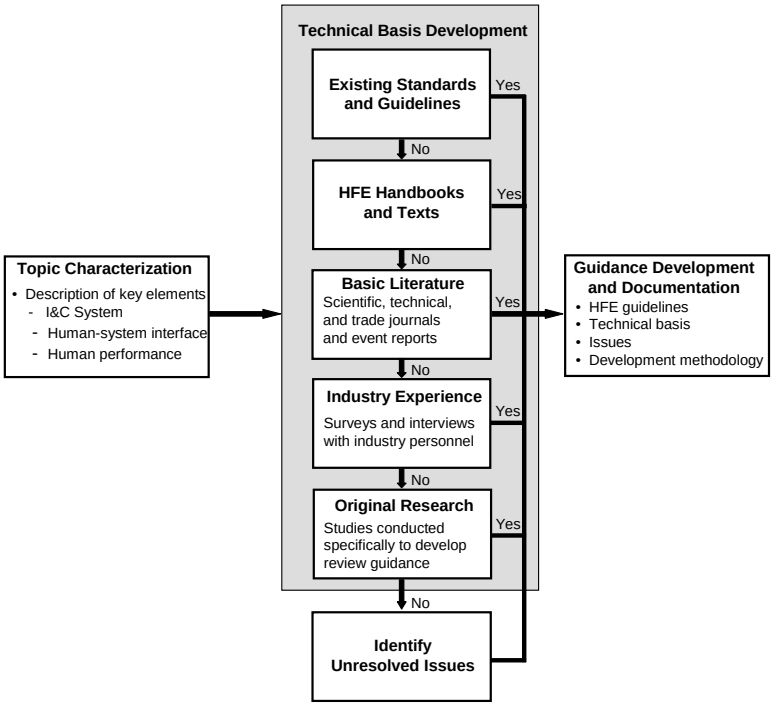


Figure 2-2 Technical basis and guidance development phases

2.2 Technical Basis Development

Our next step was to develop the technical basis upon which guidance can be developed and justified. For our project, the technical basis was reviewing information from a variety of sources, as discussed below, on the effects of degraded conditions on HSIs and operators' performances. The technical basis also includes strategies and approaches for resolving those indentified effects.

Figure 2-2 illustrates our usage of several sources of information in order of preference for developing guidance. Proceeding down the flow chart, the technical basis sources change in three ways. First, the sources of information near the top are already in or close to HFE guidance format. Toward the bottom, individual research studies must be synthesized and HFE guidelines abstracted. Second, the information at the top already possesses a degree of validity (as discussed earlier), while towards the bottom, validity must be completely established when formulating the guidance. Third, the cost of using the information generally increases y toward the bottom of the flow chart. Thus, the preference is to use sources higher in the figure.

We consider existing HFE standards and guidance documents first. They are those developed by standards organizations, such as the American National Standards Institute (ANSI) and other organizations that develop standards, such as the U.S. military. Generally, these documents are based on the research, operational experience, and subject-matter expertise. In addition, most existing standards and guidance documents have been peer-reviewed. Thus, they may have internal validity or external validity, or both. Since the information already is in guideline form, it generally is easier to use than data from other sources. We found in several standards and guideline documents with guidance related to degraded I&C systems; for example, documents published by the NRC and the IEEE. Section 4.1 summarizes the information.

While standards and guidelines documents provide a valuable starting place, some aspects of a topic extend beyond the considerations of technology and human performance in these documents. Thus, we utilized additional sources of information. We sought documents providing good analysis and syntheses of existing literature, such as handbooks and textbooks written by knowledgeable experts who have reviewed the research and operational literature. An example that was applicable to our current research is Wickens' (1986) chapter "The effects of control dynamics on performance" in the *Handbook of perception and human performance*. The information usually is not expressed as guidance, so that it has to be developed from these documents; however, the establishment of a technical basis usually is expedited by the information given in the handbook.

For topics reflecting new technology, the sources discussed above frequently are insufficient to support the establishment of guidance. Then, basic literature was reviewed. It encompasses papers from research journals, industry conferences, and technical reports from which we can derive a theoretical basis for understanding human performance concerns related to complex human-machine systems. It also provides a general theory of human-machine interaction relevant to the design of the user interface, human error, and usability. Empirical studies of human-machine interactions address a broad range of technologies and user tasks. However, greater effort is needed to develop such information into design review guidance. Thus, engineering judgment is required to generalize from the unique aspects of individual experiments and studies that have their particular constraints to actual applications in the workplace. The generalizability of individual experiments is limited by factors such as their unique participants, types of tasks performed, and types of equipment used. For example, laboratory experiments often do not involve tasks as complex as operating a nuclear power plant. Most experiments do not examine tasks under the same performance-shaping factors (such as rotating shifts, stress, and fatigue) that exist in the nuclear industry's work environments. While information from research is a valuable part of developing guidance, the findings must be interpreted in the context of real-world tasks and systems that involves judgment based on professional- and operational-experience. Event reports also may have some of the same issues of generalization. We found a few studies addressing the effects of I&C degradations on HSIs and human performance and review them in Section 4.2.

Industrial experience is a valuable source of information. It includes reports and surveys of plant personnel, designers, and regulators. Operational experience can be garnered from interviews, knowledge-elicitation sessions, and walk-through exercises using the actual HSI or a high-fidelity training simulator. While this information can be difficult and costly to obtain, it is usually more directly applicable to the NPP domain than basic literature. Like the latter, the information needs to be critically analyzed and synthesized to develop review guidance. For our study, we assessed published events and operating experience pertaining to degraded I&C wherein impacts on human performance were identified; it is discussed in Section 4.3.

Finally, information for the technical basis is gained from original research that advantageously focuses on the specific issues that must be addressed in writing guidance. For this project, we analyzed the failure modes of a portion of the digital feedwater system of an operating pressurized water reactor (PWR) to assess the impact on operator's performance. We describe our analysis in Section 4.4.

During these analyses, we identified several issues for which there is an insufficient technical basis with which to develop review guidance. The future research topics we outline in Section 4.5 can resolve these problems.

2.3 Guidance Development

We formulated HFE review guidance from the technical basis discussed in Section 4. We note in advance that the technical basis for it was quite limited. As we will discuss in Section 4, few studies specifically evaluated the effects of various types of I&C degradations on human performance, rather most research focused on sensor issues and automation. Furthermore, generalizations extrapolated from the sensor research are circumscribed for the reasons discussed in Section 4.2.1. As described in Section 2.2, we supplemented this information by reviewing operating experience and through our own analysis of degradations to a digital feedwater control system, but the net result remains; the technical basis is restricted and so we made many recommendations for additional research.

Having acknowledged this limitation, our guidance development focused on reviewing (1) an applicant's design process, and (2) the HSIs used for monitoring the I&C system and managing its degraded conditions. Considering its narrow technical basis, the guidance necessarily is fairly high-level and does not individually address all of the subsystems identified in the I&C system characterization (Section 3). It is typical in our developmental process to structure review guidelines using the characterization, but the information evaluated did not support it.

The review guidance for an applicant's design process is structured on the format used in NUREG-0711. Each individual guideline contains a review criterion, followed a brief summary of the pertinent literature. The discussion sections will be removed when the guidance is integrated into NUREG-0711. Section 7 contains our guidance on reviewing the design process.

The HSI review guidance is structured in the format of NUREG-0700 (Figure 2-3 gives an example):

- *Guideline Number* – Within sections/subsections, individual guidelines are numbered consecutively from 1 to n. Each guideline's unique number indicates its section/subsection location, followed by a dash, and then its serial number.
- *Guideline Title* – Each guideline has a unique, descriptive title.
- *Review Criterion* – Each guideline contains a statement of an HSI characteristic with which the reviewer may judge the HSI's acceptability. The criterion is not a requirement, and characteristics incompatible with the review criterion may be judged acceptable as per the procedures in the review process (see NUREG-0711, Section 11.4.2.3.2, HFE Design Verification Review Criteria, Criterion 2).
- *Additional Information* – For many guidelines, there is additional information that may address clarifications, examples, exceptions, figures, or tables. This information is intended to assist the reviewer in interpreting or applying the guideline.
- *Source* - The source document(s) from which the guideline was developed is shown in the superscript. Typically, this is the NUREG/CR or technical-report number. In the example in Figure 2-3, the number "91047" is used, indicating this document.

Section 8 contains the HSI review guidelines.

8.1-3 Indicate Important Status and Performance Parameters
The HSI should provide information about each I&C subsystem's status and performance parameters necessary to monitor the HFE-significant aspects of the system and detect I&C degradations.
Additional Information:
The intent of this guideline is give operators knowledge about how well the HFE-significant aspects of the I&C system are performing. If the HSI includes performance measures for I&C subsystems, operators can monitor that performance. Comparing current performance with typical performance will support operators in detecting changes in the system. [91047]

Figure 2-3 Format of HFE design review guideline

3 Topic Characterization

As discussed in Section 2.1, the first step in developing guidance for any topic is to characterize the topic (see Figure 2-2), that is, describe the topic's key elements. In this Section, we describe the characterization of the I&C system, the HSI, and human performance.

3.1 Instrumentation and Control System Characterization

Modern complex digital I&C systems afford a great deal of functionality that is vital to the plant's performance and safety. New reactor designs use a diversity of digital I&C architectures. Figure 3-1 is a generic block-diagram of a representative I&C system identifying the generic components that it encompasses. The blocks represent the types of digital instrumentation component types required to process a signal from the system to its end use. The arrows represent the communication links between each component. The signals are processed through a "data processing and error checking unit" (sometimes termed an I/O unit), and transformed to an appropriate format that might include some high- level calculated parameters. These input parameters then pass through a communication link to a computerized logic unit, often containing internal software that processes the parameters, and compares them to a set of criteria to decide if a series of systems and components must be actuated. Thereafter, the actuation signal is transmitted to actuator devices that complete the desired operation. The communication links can be provided from both the data- processing and actuation-signal logic units through a separate communication bus to generate information displays in the control room. Displays for the operators can be fed from any of these components, although the logic units and signal processors are the commonest links to the control room displays.

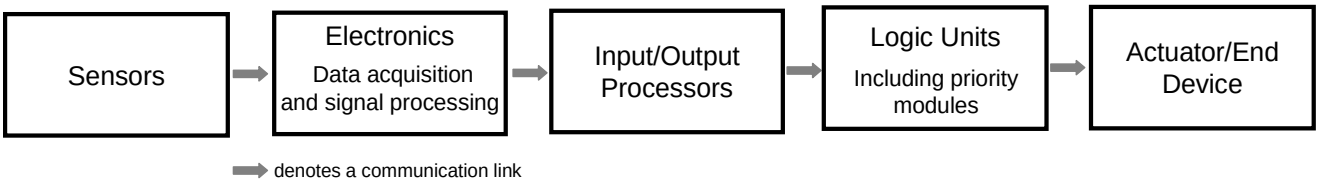


Figure 3-1 Digital I&C system components

We wanted the I&C characterization to be generic, simple, fairly high-level, and independent of the system's architecture. We felt this would be our best approach to formulating insights about the effects of I&C degradations on the HSIs and operators' performance that are generalizable beyond specific I&C systems. Future research can address a more fine-grained characterization of the I&C system if warranted. To identify a suitable means of doing this, we reviewed recent publications on characterizing modern, digital I&C systems.

A limitation of a simple component characterization, such as that shown in Figure 3-1, is that it fails to address the functions of the I&C system. The I&C roadmap for the U.S. Department of Energy's (DOE's) advanced nuclear-power-plant programs (Dudenhoeffer et al., 2006) offers an alternative approach. It is shown in Figure 3-2.

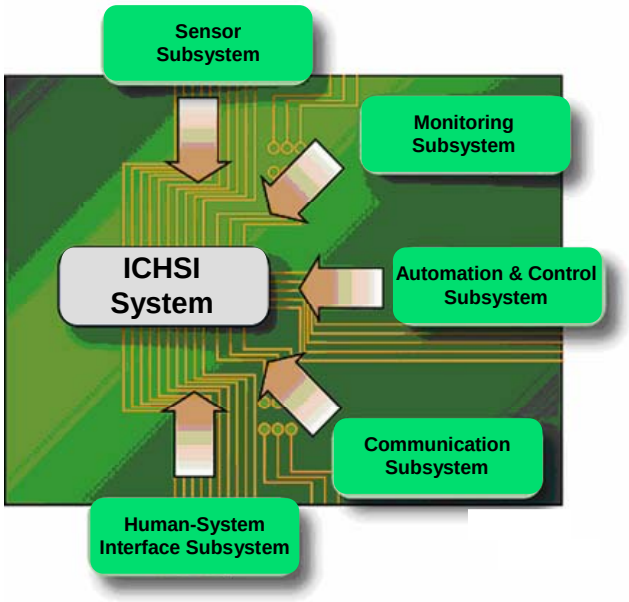


Figure 3-2 I&C subsystem representation employed by the DOE for advanced NPPs
(Source: Dudenhoeffer et al., 2006)

The subsystems are described as follows:

- *Sensor subsystem* – Nearly every plant process uses some form of physical measurement taken by sensors that detect parameters in the plant, such as neutron flux, temperatures, pressures, flow, valve positions, electrical current levels, and radiation levels. Some new nuclear-energy production technologies employ new, different types of sensors and instruments to measure physical processes. In some reactor designs, they include electronic sensors with imbedded software that are required to work in high-temperature environments and measure and analyze process parameters quite different from those in today's operating LWRs.
- *Monitoring subsystem* – These subsystems monitor the signals and other information produced by sensors and evaluate that information to determine whether and what type of response is needed. They can contain sophisticated diagnostic- and prognostic-functions. Diagnostics refers to techniques for identifying and determining the causes of deviations or faults in the plant's systems or processes. Prognostics refers to methods for using sensor data to estimate the rate of physical degradation and the remaining useful life of systems, predicting time to failure, and applying this information to more effectively control processes.
- *Automation and Control subsystem* – Digital control systems offer the ability to implement more advanced control-algorithms than those presently used in U.S. NPPs that rely primarily on single-input, single-output, classical control schemes to automate individual control loops. Advanced control schemes include matrix techniques for optimal control, nonlinear control methods, fuzzy logic, neural networks, adaptive control (a control that modifies its behavior based on plant dynamics), expert systems, state-based control schemes, and other schemes combining multiple control methods. Applying these advanced techniques will assure a more integrated control of plant systems and processes (versus separate, non-interacting control loops) and greater complexity. More modern control systems support closer interaction and cooperation between automation

and personnel, which essentially makes “human and machine” team players in controlling plant functions (O’Hara & Higgins, 2010).

- *Communications subsystem* – A variety of communication systems assure information flow throughout the I&C system and to devices being monitored and controlled; they may include wireless technology. A classical I&C architecture provides point-to-point wiring of measured variables to the monitoring and control systems. The communications subsystems for a modern I&C system are configured into a flexible network architecture’ their greatly expanded functionality enables “smart” transducers to signal their service condition to the engineering staff.

While either schematization could simplify the representation of complex digital I&C systems, we chose the subsystem one. It provides a simple generic characterization, independent of the architecture. Thus, it is suitable for our research and will serve for characterizing the I&C system.

Each subsystem of our generic I&C characterization might experience degraded conditions that could impact HSIs and the operators’ performance. For example, Kisner et al. (2007) found that deterioration in communication links can resulting in the same loss of information as caused by degraded or failed sensors or other processing modules. Communication between components and between components and personnel is a vital function throughout the plant infrastructure. In Section 4, we analyze the impact of these degraded conditions.

3.2 Human-system Interface Characterization

Next we addressed the characterization of the HSI level. This work was needed because operations personnel perform their tasks associated with I&C systems via the HSIs in the control room and local control stations. Furthermore, it is also through the HSIs that operator’s actions affect plant systems and ultimately higher-level plant functions, including safety functions. The HSIs mediate any impact on the operator’s performance of a degraded I&C system. HSIs comprise hardware- and software- components with physical- and functional-characteristics. The NRC’s HSI review guidance in NUREG-0700 gives a detailed characterization of NPP HSIs (Figure 3-3).

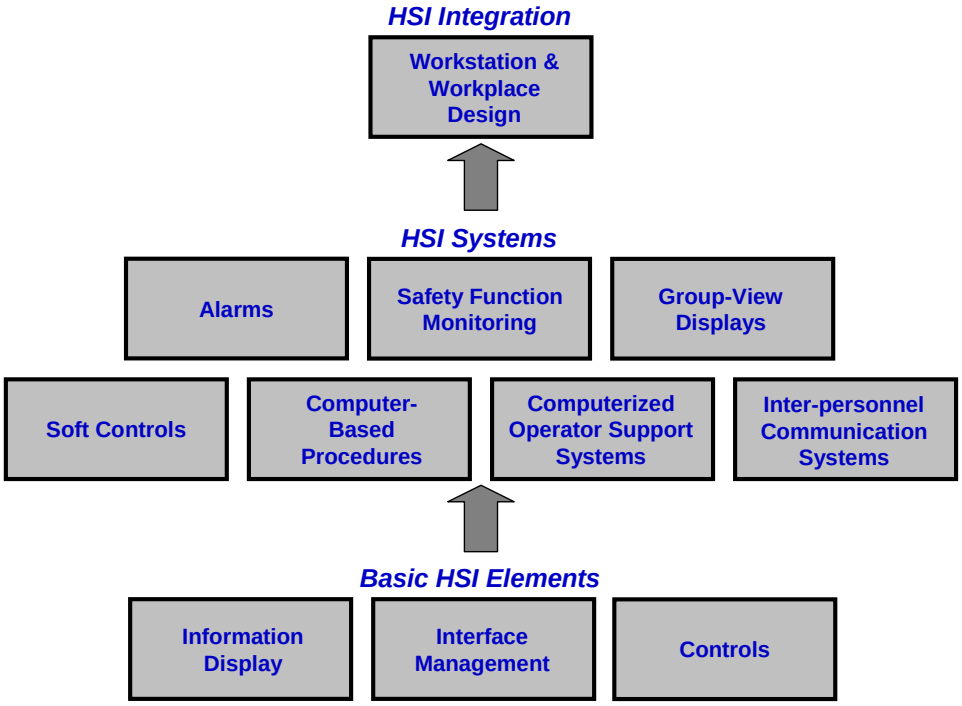


Figure 3-3 NUREG-0700's HSI characterization

The following basic elements are used as building blocks to develop HSI systems that serve specific functions;

- *Information Display* – Information display refers to the design of the visual- and auditory-displays used in the main control room and at remote locations throughout the plant. Displays can be conceptualized in a top-down fashion, beginning with the display's function (the purpose of the information being presented), the display's formats (such as mimic displays and trend graphs), its format elements (such as labels, icons, symbols, color, text, and coding), data quality and update rate, and display devices (such as video display terminals and large-panel displays).
- *User-interface Interaction and Management* – The user-interface interaction and management element refers to the modes of interaction between personnel and the HSIs. Topics include dialogue formats (such as menus, direct manipulation, and command language), navigation, display controls, entering information, system messages, and prompts. It also covers methods for ensuring the integrity of data accessed through the user interface. Guidelines address preventing inadvertent changes in or deletion of data, minimization of data loss due to computer failure, and protecting data from unauthorized access, via setpoints.
- *Controls* – Controls refers to HSI elements that enable operators to interact with the plant including conventional control devices, such as pushbuttons and various types of rotary controls. Considerations of the system's response time and display control integration are addressed. We note NUREG-0700's organizational structure deems soft controls a separate system (described below).

These three basic HSI elements constitute building blocks of seven systems, each of which performs a specific function:

- *Alarm System* – The design of the alarm system includes selecting alarm conditions, choosing setpoints, considering alarm processing and alarm availability (such as filtering and suppressing alarms), along with the unique aspects of displaying alarm information (such as organization, coding, and alarm message content), and alarm controls.
- *Safety Function and Parameter Monitoring System* – The safety function and parameter monitoring system includes the displays for monitoring critical safety functions and safety parameters.
- *Group-View Display System* – Group-view displays are those designed to be viewed from anywhere in the control room. Design considerations address their functional characteristics and user-system interaction aspects, as well as their physical characteristics.
- *Soft Control System* – Soft controls are those mediated by software rather than direct physical connections, for example, on-screen control of pumps and valves. Because software mediates soft control, its functions may be variable and context-dependent. Also, the location of a soft control may be virtual (e.g., within the display system structure) rather than spatially dedicated.
- *Computer-based Procedure System* – The computer-based procedure (CPB) system includes the representation of procedure information, its functional capabilities, user interaction features, backup provisions, and the integration of the CBP system with other HSI elements.
- *Computerized Operator Support System* – Computerized operator support systems assist personnel in situation analysis and decision-making. Design considerations encompass functional requirements, such as explanation and simulation facilities, and the desirable characteristics of their user interfaces.
- *Inter-personnel Communication Systems* – The inter-personnel communication systems are the means whereby plant personnel speak with each other and communicate electronically.

The HSI characterization in NUREG-0700 also includes workstations and workplaces.

- *Workstations* – These are the locations wherein HSIs are integrated giving an area where plant personnel can perform their tasks. Workstations include consoles and panels, along with sit-down desk-type configurations.

- *Workplaces* – Workplaces are locations were the workstations are located in the plant, such as the main control room and remote-shutdown facilities.

3.3 Human-Performance Characterization

NPP operators are essential to the safe, efficient generation of electric power in monitoring and controlling plant systems and components to ensure their proper functioning. Test and maintenance personnel ensure that the equipment is functioning properly, and restore malfunctioning components. Human actions that fail to achieve what the needed outcome in a given situation can be important contributors to the risks in operating nuclear power plants. Both

risk analyses and operating experience establish the important links between human performance and plant risk, but do not identify the mechanisms whereby human performance is affected adversely.

Operators contribute to a plant's defense-in-depth approach to safety, and serve a vital function in ensuring its safe operation. They can negatively impact safety by making errors. For instance, an error of omission occurs when personnel do not complete a safety-related action within the time required. An error of commission may occur because personnel incorrectly interpret conditions and take the wrong action. To understand how I&C technology can impact plant safety, we must know how human errors are caused and how technology impacts human performance. Thus, a characterization of human performance is needed.

The NRC initiated the development of this characterization when they first began to focus research on advanced control room technology and on developing guidance for reviewing it (O'Hara, 1994). Since then, the characterization has been developed further, and was used as part of the technical basis in numerous research projects (O'Hara et al., 2008). In addition, other nuclear-industry researchers and designers adopted the NRC's characterization. Similarly, we used ii in our research, as described below.

Figure 3-4 illustrates the causal chain that mediates the impact of operators on the plant. The point of the human-system interaction occurs when operations personnel use the HSIs to perform their tasks. Here, the operator physiological- and cognitive-processes are involved closely. As we noted previously, it is through the HSIs that operators interact with the plant's systems and components, and ultimately high-level plant functions, including safety functions.

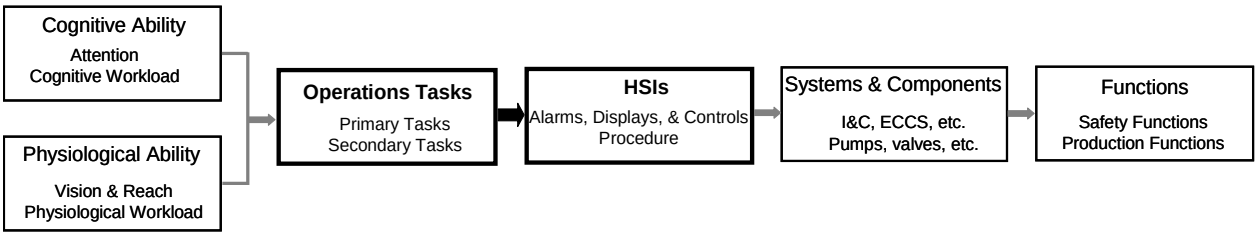


Figure 3-4 Operator impact on plant safety

In fulfilling their roles and responsibilities, nuclear-plant operators perform primary tasks and secondary tasks. Primary tasks include activities such as monitoring plant parameters, following procedures, responding to alarms, starting pumps, and aligning valves. Secondary tasks are mainly "interface management tasks." Primary tasks have several common cognitive elements: monitoring and detection, situation assessment, response planning, and response implementation. Breakdowns in any of these generic primary tasks can entail a human error.

The first primary task is *monitoring and detection* and involves extracting information from the environment, such as checking the parameters on a control panel, monitoring parameters displayed on a computer screen, obtaining verbal reports from other personnel, and sending operators to areas of the plant to check on system components. From this information they determine if the plant is operating as expected. In a highly automated plant, much of what operators do involves monitoring. Detection is the operator's recognition that something has changed, e.g., a component is not operating correctly, or the value of a parameter has increased or decreased.

In any complex system, the monitoring and detection tasks easily can be overwhelming due to the many individual functions, systems, components, and parameters encompassed. Therefore, support generally is provided by an alarm system. The alarm system is one of the primary means by which abnormalities and failures come to the attention of plant personnel.

The second primary task is *situation assessment*, that is, the evaluation of current conditions to determine if they are within acceptable limits, or to identify the underlying causes of any abnormalities. Operators actively try to construct a coherent, logical explanation to account for their observations. This cognitive activity involves two related concepts: The situational model and the mental model. The latter consists of the operator's internal representation of the plant's physical- and functional-characteristics of the plant and its operation, as they understand it should be. The mental model rests upon formal education, training, and experience. Situation assessment occurs when operators use their mental model to understand information they obtain from the HSIs and other sources. The cognitive representation resulting from situation assessment is termed the "situation model," i.e., the person's understanding of the specific current situation. The term "situation awareness" refers to the understanding that personnel have of the plant's current situation; that is, their current situation model. The alarms and displays serve to generate information supporting situation assessment. The HSIs may provide additional support to situation assessment in the form of operator-support systems.

To construct a situation model, operators use their general knowledge and understanding about the plant and its operation to interpret their observations and to extract its implications. Limitations in knowledge or in current information may entail incomplete or inaccurate situation models. General knowledge about human performance, the so-called "mental model" consists of the operator's internal representation of the physical- and functional-characteristics of the plant and its operation as they understand it should be. The mental model rests on formal education, training, and experience.

Situation assessment is critical to taking proper human action. Thus, an IAEA report (1988) noted about events involving incorrect human actions: "Frequently such events have occurred when plant personnel did not recognize the safety significance of their actions, when they violated procedures, when they were unaware of conditions of the plant, were misled by incomplete data or incorrect mindset, or did not fully understand the plant in their charge" (p. 19). Further, Roth et al. (1991) identified situation assessment and response planning as important factors in simulator experiments involving cognitively demanding situations (i.e., situations not fully covered by procedures or training because those conditions for the specific, simulated event differed from the nominal). Also, in the Operator Reliability Experiment (ORE) program, 70% of the operating crews' errors or near-misses observed in the simulator experiments, regardless of plant type, were categorized as situation assessment errors (diagnosis) (Beare et al., 1991).

If operators have an accurate situation model, but mistakenly take a wrong action, they have a good chance of detecting it when the plant does not respond as expected. However, with a poor situation model, operators may take many "wrong" actions because their actions conform with their current understanding of the plant's state, but are wrong for it.

The third primary task is *response planning* that refers to deciding upon actions to resolve the current situation. In general, it involves operators using their situation model to identify goal states and the transformations required to achieve them. The goal state may vary, such as identifying the proper procedure, assessing the status of back-up systems, or diagnosing a

problem. To meet their goals, operators generate alternative response-plans, evaluate them, and select the one most appropriate to the current situation model. Response planning can be as simple as selecting an alarm response or it may involve developing a detailed plan when existing procedures proved incomplete or ineffective.

In a NPP, procedures usually aid response planning. The need to generate a response plan in real time largely might be eliminated when operators trust that the procedures are suitable to meet the current problem. However, even with good procedures, operators will undertake some aspects of response planning. For example, they still need to (1) identify goals based on their own situation assessment, (2) select the appropriate procedure(s), (3) evaluate whether the procedure-defined actions are sufficient to achieve those goals, and (4) adapt the procedure to the situation, if necessary.

The fourth primary task is *response implementation*. It is performing the actions specified by response planning that might actions include selecting a control, providing control input, and monitoring the responses of the system and processes. Several types of errors are associated with controls. One good example is mode errors, a new type associated with digital technology. A mode error occurs when operators take an action thinking the control system is in one mode when actually it is in another one. Consequently, the system's response to the action is not what the operator intended.

Performing these generic primary tasks well constitutes a moderate level of workload. If workload is too low, vigilance suffers and the ability of personnel to develop accurate situation- assessment diminishes. As the demands of performing the task rise, a greater workload is experienced, and ultimately, if the workload gets high enough, the ability to perform tasks declines.

To understand human performance, it is also important to consider the secondary tasks. In a computer-based control room, personnel must successfully perform secondary tasks or "interface management tasks" so that they can complete their primary tasks. Under these conditions, those secondary tasks include navigating or accessing information at workstations, and arranging various pieces of information on the screen. In part, these tasks are necessary because operators view only a small amount of information at any one time through the workstation displays. Therefore, they must undertake interface management to retrieve and arrange the information. These tasks are termed secondary because they are not directly associated with monitoring and controlling the plant.

The distinction between primary and secondary tasks is important because of the ways they can interact. For example, secondary tasks create workload and may divert attention away from primary tasks, making them difficult to complete (O'Hara & Brown, 2002). Thus, secondary tasks, must be addressed carefully in design reviews, particularly interface-management tasks. Degraded I&Cs increase interface management, such as when information on their current display is corrupted, so that operators must navigate additional displays.

Our discussion above focuses on the primary and secondary tasks that operators perform. In actuality, individual operators typically do not undertake these tasks alone; they are accomplished by the coordinated activity of multi-person teams. Operators share information and work in a coordinated fashion to maintain the plant's safe operation as well as to restore it to a safe state should a process disturbance arise. Crew members may perform a task cooperatively from one location, such as the main control room, while in other cases a control room operator may have to coordinate tasks with personnel in a remote location, such as at a local control station. Important

HFE aspects of teamwork include having common, coordinated goals, maintaining shared situation awareness, engaging in open communication, and cooperative planning. Successful teams monitor each other's status, back each other up, actively identify errors, and question improper procedures.

As new technology was introduced into control rooms and throughout nuclear power plants, there has been growing recognition that the design of technology must consider team performance as well as y individual performance (O'Hara & Roth, 2005). Compared to conventional control rooms, computer-based control rooms can impact teamwork in at least two ways: Changes to the physical layout and characteristics of the workplace; and, changes to the functionality of the I&C system and HSIs such that the HSI now undertakes activities previously performed by a crew member. Thus, new technology impacts teamwork; it is important to understand how this might affect the team's performance and safety.

Thus, the effect of human performance on plant safety can be understood by considering the effects of technology, including degraded or failed I&C, on the factors that support human performance in operations: Primary tasks, interface management tasks, and teamwork. To the extent that technology is implemented to support these factors, human performance and safety also should be supported. To the degree that technology is established in a way that undermines or disrupts these factors, human performance will be negatively impacted and may lead to error. Under the right circumstances, human errors undermine plant safety as we earlier demonstrated in various analyses of operational experience and risk (O'Hara et al., 2008).

Thus, for the purposes of our study, we characterize human performance under the following dimensions:

- Monitoring and Detection
- Situation Assessment
- Response Planning
- Response Implementation
- Interface Management
- Team Processes

3.5 Summary

We developed a characterization representing the I&C system, HSIs, and human performance, as illustrated in Figure 3-5, and identified the key constituent elements of each level.

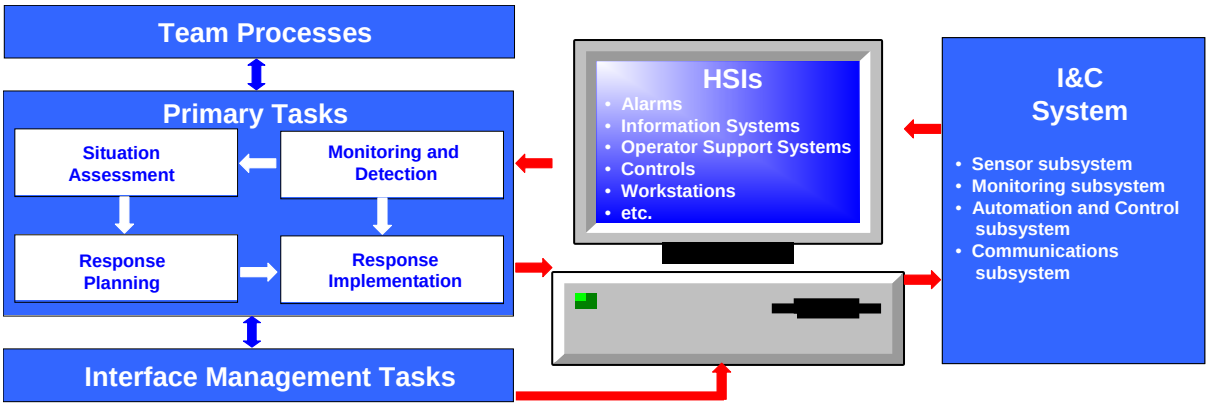


Figure 3-5 Characterization of the I&C system, the HSI, and human performance

Our characterization provides a way of organizing the evaluation of other research, and events into a standardized language for developing general insights (Section 4). Figure 3-6 illustrates the way we used the process in this study.

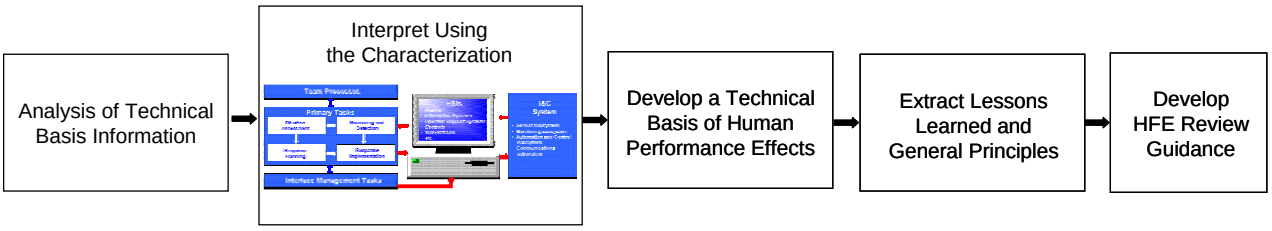
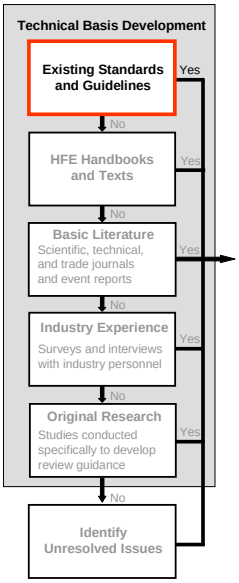


Figure 3-6 Use of the process in developing guidance

4 TECHNICAL BASIS DEVELOPMENT

The second step in formulating guidance is to develop a technical basis (Figure 2-2). In this section, we address the steps upon which the HFE review guidance was refined and justified. In Section 2.2, the methodology to develop the technical basis was discussed; it uses a variety of sources of information, as illustrated in Figure 2-4.

4.1 Existing Standards and Guidelines



As shown in Figure 2-4, the first source of information evaluated for the technical basis was existing standards and guidelines, both of which are discussed in this section.

Over the years, the nuclear industry expended much effort to help ensure that the quality and reliability of I&C systems and HSIs used in NPPs will support safe operations. In the United States, this goal was met through the implementation of industry standards (i.e., IEEE), and through the NRC's detailed regulations and design review guidance. The NRC documented its analyses and regulatory positions in standard review plans, regulatory guides (RGs) and regulatory issue summary (RIS) reports, along with interim guidance documents (ISGs) and branch technical positions (BTPs).

The nuclear industry, through EPRI and INPO, established high standards of performance for operations and safety of which the instrumentation and controls systems are a vital component. They also published documents (i.e., EPRI Topical Reports) to assist licensees and license applicants with the design, licensing, and operation of digital I&C systems and associated HFE. Some regulatory guidance endorses or references industrial standards. For instance, RIS 2002-22 was issued by the NRC endorsing the use of an EPRI report (TR-102348) (EPRI, 2002) as guidance in designing and implementing digital upgrades to I&C systems.

We culled guidelines on the relationship between digital I&C system degradation, HSI, and operator performance from the existing documents described below.

4.1.1 NRC Documents

4.1.1.1 HFE Review Guidance

In this section, we review the following NRC's HFE review guidance documents:

- Standard Review Plan (NUREG-0800), Chapter 18, Human Factors Engineering (NRC, 2007a)
- HFE Program Review Model (NUREG-0711, Rev 2) (O'Hara et al., 2004)
- HSI Design Review Guidelines (NUREG-0700, Rev 2) (O'Hara et al., 2002)
- Digital I&C: Highly-integrated Control Room-Human Factors Issues (DI&C-ISG-05, Rev 1) (NRC, 2008b)

- Human-system Interfaces to Automatic Systems: Review Guidance and Technical Basis (Technical Report BNL-91017-2010) (O'Hara & Higgins, 2010)

The review guidance that we deemed applicable to our objectives in the guidance development process is cited in Sections 7 and 8.

NUREG-0800 and NUREG-0711

The NRC addresses human performance, in part, by conducting HFE safety reviews. In accordance with 10 CFR 52, the NRC's staff reviews the HFE programs of applicants for construction permits, operating licenses, standard design certifications, and combined operating licenses. The purpose of these reviews is to help ensure safety by verifying that the applicant's HFE program incorporates acceptable practices and guidelines, thereby assuring that personnel performance and reliability are supported appropriately.

The *Standard Review Plan* (NUREG-0800) contains high-level guidance for conducting the HFE reviews in *Chapter 18, Human Factors Engineering* (NRC, 2007). Detailed review criteria are given in the *Human Factors Engineering Program Review Model* (NUREG-0711) (O'Hara et al., 2004). The approach rests on the concept that the HFE aspects of NPPs should be developed, designed, and evaluated on the basis of a structured systems analysis, using accepted HFE principles. Figure 4-1 shows the twelve elements of an HFE program review.

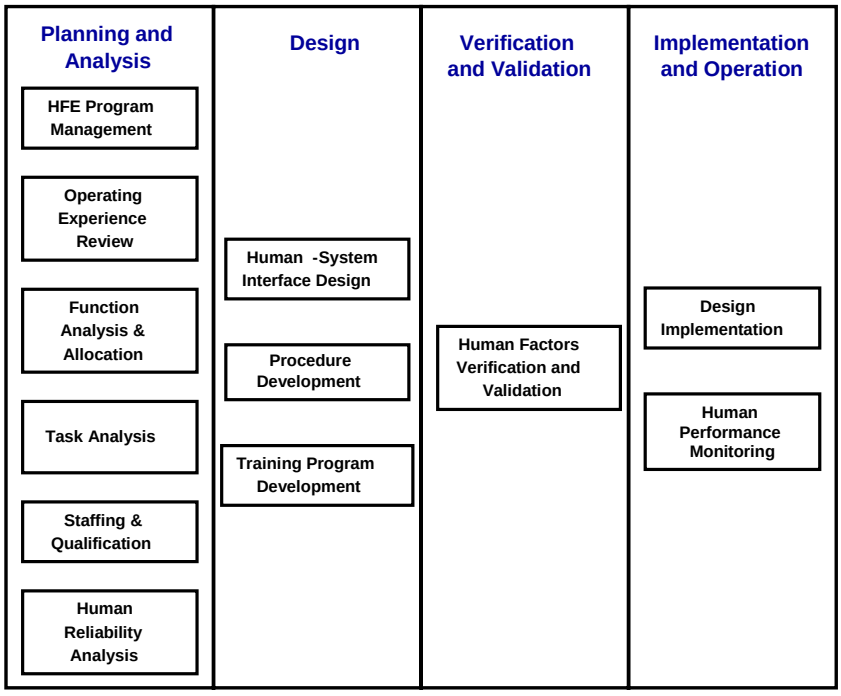


Figure 4-1 NUREG-0711 review topics

NUREG-0700

The *Human-system Interface Design Review Guidelines* (NUREG—0700, Rev 2) (O'Hara et al., 2002) has guidance for reviewing the physical- and functional-characteristics of HSIs. We described it in Section 3.2 of this report because we employed it to help define the elements of the HSI level of the process. Figure 3-7 illustrates the NUREG-0700's HSI characterization; guidelines addressing the maintainability of digital systems are not included (in NUREG-0700, Part IV).

In addition, Appendix B of NUREG-0700 contains HSI-specific guidance on the HFE design process that covers the human performance problems associated with particular HSI technologies. The format of the guidelines in Appendix B corresponds to that used in NUREG-0711. Guidance is given on for information display, computer-based procedures, and interface management.

Many of the sections in NUREG-0700 have review criteria addressing degraded conditions in general.

Interim Staff Guidance on Digital I&C; Highly-integrated Control Room, Human Factors Issues

The purpose of this ISG (NRC, 2008b) is to offer acceptable methods for resolving several human factors problems related to highly-integrated control rooms, encompassing the following:

- Computer-based procedure systems
- Minimum inventory of alarms, controls, and displays
- Crediting manual actions in analyses of diversity and defense-in-depth (D3) as a diverse means of coping with "…anticipated operational occurrences and postulated accidents" that are concurrent with a software common-cause failure of the digital I&C protection system

The issues of CBP systems and manual operator actions address degraded I&C conditions.

Technical Report BNL-91017-2010: Human-system Interfaces to Automatic Systems: Review Guidance and Technical Basis

Part 2 of the report (O'Hara & Higgins, 2010) has guidelines for reviewing HSIs to automatic systems including their degradation, and their implications for the design process and operator training.

4.1.1.2 I&C Review Criteria

NUREG-0800 and Associate Branch Technical Positions

Appendix 7.0A - Review Process for Digital I&C Systems

This appendix affords an overview of the process for reviewing digital I&C systems. "It shows how the review activities interact with each other and with the overall I&C review process described in SRP Sections 7.2 through 7.9." It notes in Section 7.0-A-4(1) that "Digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and

implementation can cause them to exhibit unexpected behavior." Operators' awareness of this potential, and their having a plan for responding to these behaviors would be beneficial. Appendix A of NUREG-0800 notes that the reviews of control systems and data-communication systems are limited.

Section 7.5 - Information Systems Important to Safety

The objective of this area of the review is to confirm that the information systems vital to plant safety provide the information needed to ensure it under all conditions. One link between the digital I&C system and the operator that this section covers is the need to give the operators timely information and status reports, including system-bypass conditions, so they can mitigate the effects of unexpected system unavailability.

Section 7.7 - Control Systems

"The control systems covered by this SRP section include those control systems that control plant processes having a significant impact on plant safety. These control systems are those systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions." This section of the SRP requires the inclusion of the impact of failures of the control system in analyses of design basis accidents.

Branch Technical Position (BTP) 8.5 - Supplemental Guidance for Bypass and Inoperable Status Indication for Engineered Safety Features Systems

This BTP supplements the criteria for the indication of bypass and inoperable status described in IEEE 603 and endorsed by RG 1.153. It states that the design criteria for bypass and inoperable indication systems for ESFs should reflect the importance of accurately informing the operator. It provides guidance to the reviewer on how bypass conditions should be indicated and procedurally managed.

Interim Staff Guidance on Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments:

The purpose of this ISG (NRC, 2008c) is to offer interim guidance on how reviewers should evaluate digital I&C system PRAs, including common-cause failures and uncertainty analysis associated with new reactor digital systems. "DI&C systems are combinations of hardware components and software (i.e., computer programs). This combination of hardware and software can result in the presence of faults and failure modes unique to DI&C systems."

Interim Staff Guidance on Digital I&C: Highly-integrated Control Rooms - Communications Issues

This ISG (NRC, 2009) describes how to combine controls and indications into a single integrated workstation while maintaining separation, isolation, and independence. A digital workstation is one such device, according to this definition. Appendix B contains some operational considerations.

Reg Guide on Bypassed and Inoperable Status Indication for NPP Safety Systems

This RG (NRC, 1973) describes an acceptable way of aiding the operator's knowledge of plant status by supplementing administrative procedures with automatic indications of the bypass or

inoperability of each redundant portion of a system that performs a safety function. One criterion for implementing such indications is if the inoperable condition reasonably can be expected to occur more often than once a year.

Reg Guide on Criteria for Accident Monitoring Instrumentation for NPPs

With some restrictions, this RG (NRC, 2006a) endorses IEEE 497-2002 that establishes flexible, performance-based criteria for the display of accident-monitoring information. Revision 4 of RG 1.97 is intended for new plants. The IEEE standard has guidance on computer-generated control room displays and calculated values, without limiting the types of displays that might be made available.

Reg Guide on Criteria for use of Computers in Safety Systems of NPPs

This RG (NRC, 2006b) describes a method for promoting high functional reliability for employing digital computers in safety systems. "In this context, the term 'computer' identifies a system that includes computer hardware, software, firmware, and interfaces." It references IEEE Std. 7-4.3.2-2003.

Reg Guide on Guidelines for of Computer-based I&C Systems in NPPs

Safety-related computer-based I&C systems are discussed in this RG (NRC, 2007c) that endorses certain practices and incorporates guidance to address specific issues posed by the applying microprocessor-based technology. This guide complements RG 1.89 that is associated with environmental qualification (EQ) equipment in harsh environments. The regulatory analysis section states that "Because of expanding single-chip capabilities, many safety-related implementations involve replacing multiple functional modules with a multifunction microprocessor-based module. Therefore, failure of a single module for a computer-based I&C system can affect numerous functions." The RG endorses IEEE Std. 323-2003.

4.1.2 Industry Documents

The IEEE's Nuclear Power Engineering Committee developed many industrial standards and technical reports on digital I&C systems to which the NRC documents refer. In the following, we summarize the documents we felt to be of most relevance to our project. The regulatory guide associated with the standard also is identified where appropriate.

IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations

This standard (IEEE, 2003) in conjunction with IEEE Std. 603, establishes the minimum functional and design requirements for computers used as components of a safety system. It defines failure as "The inability of a system or component to perform its required function within specified performance requirements", and hazard analysis as "A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analyses focuses on system failure mechanisms rather than verifying correct system operation."

Paragraph 5.14 states that that no human factors considerations are necessary beyond IEEE-603-1998 (IEEE, 1998).

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

This standard (IEEE, 1998) establishes the minimum functional design criteria for the power, instrumentation, and control portions of nuclear-power-plant safety systems. The latest revision clarified the application of this standard to computer-based safety systems and to advanced NPP plant designs. This standard includes the requirements for displaying information, and human-factors considerations.

IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

This standard (IEEE, 2002) provides a consolidated source of post-accident monitoring requirements and bases for advanced nuclear-plant designs. It also contains guidance on upgrading digital I&C at operating plants. It brings together the requirements from 497-1981, ANSI/ANS Std 4.5-1980, and Reg. Guide 1.97. It also covers information about control room displays, and other information that must be available to the control room operator.

IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities

This standard (IEEE, 2004 provides recommended practices to integrate HFE into the design, operations, and maintenance of NPPs. It discusses how the operator detects and responds to abnormalities.

IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

The principles in this guidance document (ANSI/IEEE, 1987) are applicable to analyzing the effects of component failures on the safety system's reliability. It defines failures related to operator awareness: "…a failure is the termination of the ability to perform a required function. Failures may be unannounced and not detected until the next test (unannounced failure) or they may be announced and detected by any number of methods at the instant of occurrence (announced failure)".

EPRI TR-102348[2] (EPRI, 2002) was written "…to help nuclear plant operators implement and license digital upgrades in a consistent, comprehensive, and predictable manner." The NRC endorsed this document, as described in NRC RIS 2002-22. The NRC staff's position is that since there are no established consensus methods for accurately quantifying the reliability and dependability of digital equipment, it supports the need for a failure analysis with an appropriate level of detail to properly assess the potential for, and impact of, failures. Human factors issues associated with replacing digital I&C systems are covered in Section 5.3.4.2 of the TR. Appendix B offers the relevant guidance. This TR uses the concept of "failure management" as the ability to identify failures, and to alarm them, stating that "…good failure management will result if the design includes consideration of plausible failures and defects and provides appropriate features to detect the results of such events."

[2] This document also is identified as *Guideline on Licensing Digital Upgrades* (NEI 01-01), March 2002.

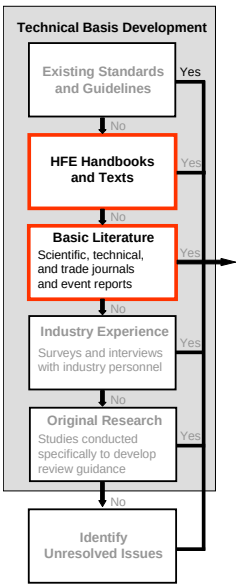
IEEE Standard Application to the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

This standard (IEEE, 2000) provides guidance for applying the single-failure criterion. NRC Regulatory Guide 1.53 endorses this standard. Also, it defines a non-detectable failure thus; “a failure that cannot be detected through periodic testing, or revealed by an alarm or anomalous indication”. There is no additional guidance.

4.1.3 Summary

Our review of existing regulatory and industry standards, guidelines, and related documents identified a substantive amount of information on the impact of degraded digital I&C systems on the HSIs and operators’ performance.

4.2 Analysis of Handbooks, Texts, and Basic Literature



As we depicted in Figure 2-4, the next sources of information we consulted were HFE textbooks, texts, and basic literature. We discuss these together because of the paucity of such information. In this section, we examine this literature describing research on the effects of degraded I&C conditions on HSIs and human performance. We note in advance that very few studies examined these effects; most of them focused on degradations of the sensors. The work on the deterioration of sensors and monitoring subsystem appears in Section 4.2.1 below.

Some research in related areas that, while not specifically directed at I&C degradation, provides insights that can be extrapolated to it. Specifically, research on automation provides an understanding of the degradation of the automation and control subsystem. While that on time delays offers clues about the degradation of the communication system; Section 4.2.2 briefly describes both. The literature we researched also addressed methods and design features to minimize these effects; it is discussed in Section 4.2.3, where we also summarize the findings.

Thus, the limited scope of the research carried out limits the insights that can be derived from it. It does not address the diversity of degradations, HIS performance, and the failure modes of the I&C system. Additional, robust research is needed to clarify these relationships. .

4.2.1 Degraded Sensor and Monitoring Subsystems

Several studies examined the effects of sensor degradations on graphical HSIs and human performance. Vicente and Rasmussen (1992) identified sensor noise[3] as one potential limitation to implementing graphical user interfaces and called for empirical research on the issue. This led to a series of studies examining this relationship.

Thus, Moray and his colleagues (Moray et al., 1993; Moray et al., 1995; Vicente et al., 1996) undertook a study for the NRC comparing performance using a graphic display with the use of two types of "traditional" displays. The graphic display, a configural one, with inputs from 35 sensors, was based on a plant's Rankine cycle,[4] and was referred to as a direct perception interface (DPI). An emergent feature was a curve connecting sensor values (Figure 4.2-5). The two traditional displays were (1) analog linear gauges, and (2) analog linear gauges with a pressure-temperature plot.

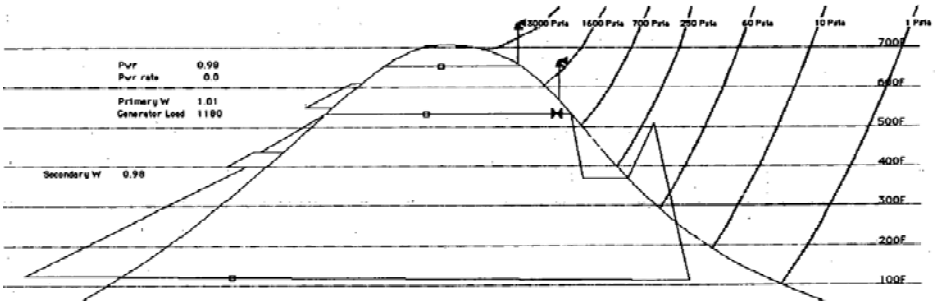
Three groups participated in the study: Novices (upper class undergraduates), experts (graduate students), and professional NPP operators. Nine transient scenarios, such as a loss of coolant accident (LOCA), were presented on a desktop computer. No actual simulation was used during the study, but the displays were based on data collected during actual simulation trials with a simplified PWR model. Two scenarios were a failed instrument (steam generator pressure failed to zero) and a drifting instrument (steam generator level drifted from normal to zero). Measures

[3] Noise is irrelevant data that hampers the recognition and interpretation of data of interest (IEEE, 1990).

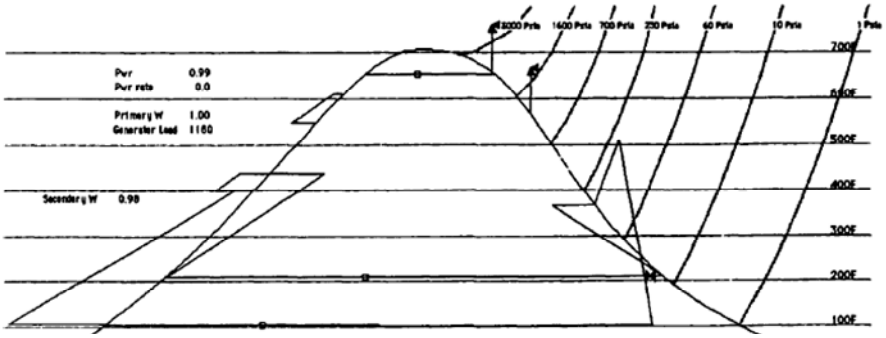
[4] O'Hara et al., 2002 give a detailed explanation of the Rankine Cycle display.

of performance were the quantitative recall of parameter values, the qualitative recall of plant states, fault detection, and fault diagnosis.

Overall, the study supported the groups' improved detection and diagnostic performance with the DPI display. Unfortunately, in their data analysis, the authors did not address the specific effects of sensor failures on performance. However, they noted that these failures affected the participants' behavior and their understanding of the display. Moray (1994) observed that that when only one of the thirty-five instrument sensors failed, the display was very difficult to interpret, see Figure 4-2. We include this figure simply to illustrate the considerable deviation in the graphic from normal when only a single sensor failed.



Display of Normal Conditions



Display Resulting from a Failed Sensor

Figure 4-2 Effect of failed sensor on the direct perception interface
(Source is Moray et al., 1993)

Moray commented that

> … the failed sensor makes the geometry of the Rankine cycle display become physically meaningless, and leads to a display which is extremely hard to interpret, although only a single variable is faulty. In this situation the loss of a single variable in the analog display left 34 variables displayed in a way which allowed them to be used for assessing plant state, but the DPI collapsed into a format which would have been extremely difficult to use, even though the plant state was in fact normal.
>
> The calculations involved in coupling information from many sources to produce the DPIs are extremely vulnerable to certain classes of failures. Little or no research exists in this aspect of DPIs,

> and is urgently needed. The real advantages of such displays during normal operation and during many classes of transients may be more than offset if they collapse under other classes of abnormalities.
>
> An understanding of the failure modes of DPIs (as distinct from the failure modes of the plant itself) is as necessary as an understanding of their design for normal conditions. Existence proofs of interface designs are no substitute for full empirical evaluations, and yet very few advanced DPIs have been exhaustively evaluated over a wide range of abnormal conditions. It is clear from our results that DPIs and/or ecological interfaces can fail in catastrophic ways, and it is probable that such failures may be particularly dangerous in large richly coupled systems. (p. 485)

Vicente et al. (1996) commented that it is essential to evaluate displays under these types of failure modes to ensure that they are comprehensible, and do not mislead operators or confuse them in thinking another process failure has occurred. Further, Vicente (2002) listed sensor noise and failure as one of the unaddressed, potentially worrisome challenges to using graphic displays. He indicated the need for work to resolve this high-priority issue.

Reising and Sanderson (2000, 2004) sought quantitatively to assess the ability of operators to distinguish sensor failures from process failures. Four groups of college students, in one of four test groups, performed a process-control task using a simple pasteurizer simulation, Pasteurizer II (an interactive microworld depiction of a pasteurization process). To monitor and control the process, participants used either an "Ecological Interface Design" (EID) display[5] or a "piping and instrumentation" display (PID). Information in the displays was supplied by either a maximum sensor configuration or a minimum one. In the following example, adapted from Reising and Sanderson (2002a), we illustrate the concept of both sensor configurations. Figure 4-3 presents a display of a simple reservoir system consisting of a tank with an input pipe and an output pipe. The display offers the operator with information about the value of each of these three parameters. The information can be obtained for three sensors, one for each parameter (a level transducer in the tank, and flow transducers in the input and output pipes), viz., the maximum sensor configuration. Alternatively, the information can be obtained from only two sensors, e.g., the Tank Level, and Flow Out sensors, so that the value of Flow In is calculated or derived from the other two (the change in tank level per unit of time). Flow In is needed to display the emergent feature (the line connecting Flow In and Flow Out displaying rate of change) commonly used in EID displays.[6]

The combination of the two display types and two sensor configurations gave four groups, each with 11 participants. Faults, either process- or sensor-failures were introduced during selected trials. The dependent measure was correctly diagnosing the fault. A significant crossover interaction was observed; i.e., performance was best in the EID display with the maximum sensor configuration and worst with the EID display in the minimum sensor configuration. Performance in the two PID display conditions fell in between. However, they were below 50% correct diagnoses in all but the EID display with the maximum sensor configuration. These results indicate that participants had difficulty distinguishing between failures of processes and sensors. Performance improved under the maximum sensor configuration where there were the greatest

[5] EID refers to an approach to display design that focuses on presenting information at various "levels of abstraction" (from low-level parameter information about a component to high-level plant functions, such as critical safety-function status). EID principles seek to maximize the value of the display of this information by fully using graphical features to present it. O'Hara et al. (2000) give more information.

[6] NUREG-0700 defines an "emergent feature" as a high-level, global perceptual feature produced by the interactions among individual parts or graphical elements of a display (e.g., lines, contours, and shapes) to convey relationships between the information.

opportunities for comparisons to related performance parameters. Further, the EID display was more affected than the PID displays by the sensors' configuration; thus, diagnostic performance was worse with the minimal number of sensors. We discuss the reason for this below.

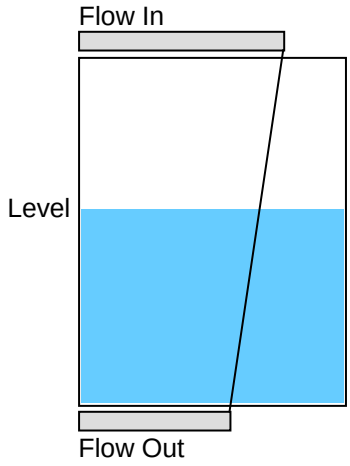


Figure 4-3 Display showing the tank level, flow in, and flow out

To illustrate how the maximum sensor configuration is beneficial, consider the displays in Figure 4-4. The upper and lower sets of displays, respectively, represent the minimum and maximum sensor configurations (as defined above). Each set shows the display at three time points after a sensor failure (at Time 1); it is a degraded level transmitter that drifts upward.

In the minimum sensor configuration (upper set of displays in Figure 4-4), when the sensor fails, the display depicts an increase in Tank Level *and* a corresponding increase in Flow In (that is derived from Tank Level) relative to Flow Out. This will make sense to an operator since the level is increasing; more fluid is coming into the tank than is leaving. However, the display is ambiguous, and operators cannot distinguish the possibility of a sensor failure from an actual change in level. Since operators are taught to "trust their instrumentation," it is unlikely an operator will consider that a sensor failure occurred.

In the maximum sensor configuration (lower set of displays in Figure 4-4), when the level transmitter fails, the display shows the rising level in the tank. However, Flow In and Flow Out are the same. Thus, the operator can determine that something is wrong; that is Flow In and Out are equal, yet the level in the tank is rising. The possibility of a degraded sensor is likely.

Thus, in some circumstances improved instrumentation can help operators distinguish between sensor issues and process disturbances. Reising and Sanderson (2002b) give additional examples.

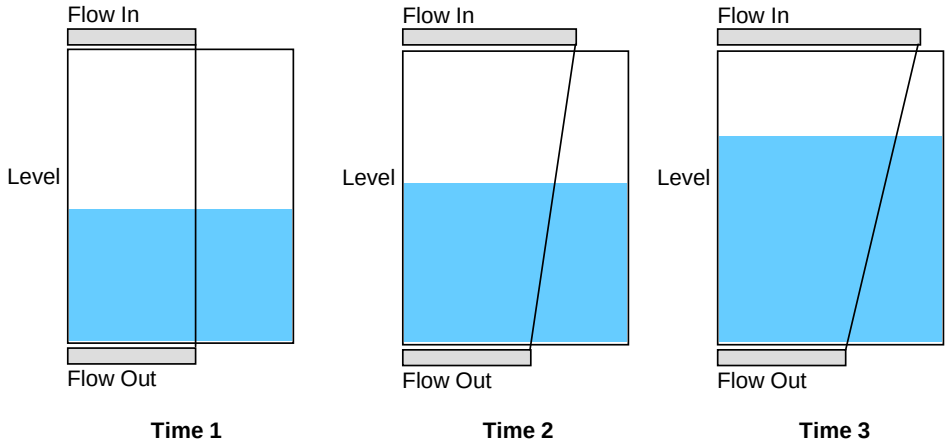


Figure 4-4 Effect of sensor configuration on a display
(adapted from Reising & Sanderson, 2002a)

Vicente and St-Cyr extended the work of Reising and Sanderson, specifically examining the effects of sensor noise on the operator's performance while controlling a simulated thermal-hydraulic process (St-Cyr & Vicente, 2004; St-Cyr & Vicente, 2005; St-Cyr, 2006). The first study (St-Cyr & Vicente, 2004) examined the effects of the magnitude of the sensor's noise on the performance and control strategies of the participants, 20 engineering undergraduate students. DURESS II (DUal REservoir System Simulation), a dynamic simulation of a simple thermal-hydraulic process, was used. It has two redundant feedwater streams, which feed two reservoirs under various configurations, and with time lags on control variables. The operators try to keep each reservoir at a specific temperature and to maintain water levels as needed, based on flow rates. They accomplish this task by controlling valves, pumps, and heaters. Improperly operating the equipment can damage it, such as allowing the water level to get too low in a reservoir while it is being heated. Experimenters also can introduce faults into the system.

Participants controlled the simulation using one of two interfaces: A basic physical representation of the process (P interface), or a physical plus a functional display (P+F interface). The P interface was a mimic-type display showing information about the two feedwater systems. The

P+F display contained the same information plus along with information about system functions displayed using emergent features similar to rate of change line in Figure 4-3.

The magnitude of sensor noise used in the study was based on industrial standards (by averaging accuracy ranges for different types of sensors from different vendors). The magnitude of noise was varied randomly across trials.

Performance measures included (1) trial completion time (TCT), i.e., the time needed to achieve a steady state condition, (2) control stability, measured as the number of oscillations around four goal variables, and, (3) control recipes that were instructions each participant prepared to describe how the steady-state was achieved.

The performance of participants in both groups worsened as the magnitude of sensor noise increased; i.e., TCT increased as did the number of oscillations about the goal values. Noise also caused participants to change their control strategies, although the effect was more pronounced in the P+F group; the authors attributed this effect to the fact that emergent features were less helpful as sensor noise increased, forcing this change.

Because the magnitude of sensor noise was varied randomly varied, the effects of specific levels could not be determined. The authors explored this in a second study (St-Cyr & Vicente, 2005), again employing the DURESS II simulation, two interface types, and the TCT and oscillation measures. Twenty students performed the simulated task for 110 trials. The “industry standard” noise was applied to all sensors for the first 60 trials. Then, over the next 50, the noise was increased for each subsequent block of 10 trials by scaling multipliers of 2 (trials 61-70), 3 (trials 71-80), 5(trials 81-90), 7 (trials 91-100), and 10 (trials 101-110).

As sensor noise increased, TCT increased (performance worsened). The effect was greater for the P+F interface. While this finding was consistent with the results of the first study, the results for the oscillation measure differed. The performance of the participants using the P interface did not change as a function of sensor noise. Thus, while their performance declined at first, at the two higher noise levels, it returned to a level equivalent to that observed under the industrial average noise. The authors hypothesized that this effect may reflect a shift in control strategy, but could not verify it (information about control recipes was not obtained). Overall, the results of this study are consistent with the previous study: Sensor noise impairs performance and the effect generally is worse for those using the P+F interface.

In these two studies, changes in sensor noise were applied globally to all DURESS sensors. This is not representative of what is likely to happen in an actual system where only one or a few sensors would be faulty at any one time. A third study addressed this issue (St-Cyr, 2006). Again, 20 students participated, and the same DURESS II simulation, two interface types, and performance measures were used, i.e., TCT, control stability (oscillations), and reported control recipes. The magnitude of sensor noise was increased on selected sensors to 10 levels above the industrial average.

The introduction of noise did not impact TCT and oscillation measures of the P group, but negatively impacted those of the P+F group. The control recipes revealed that while participants in this group used the emergent feature as a focal point of control when noise was low, they changed their strategy as noise increased. Thus, sensor noise distorted the emergent features, and entailed a compensatory shift in control strategy to compensate. The P group was unaffected because they did not have the graphic features to influence their behavior.

We summarize the lessons learned from the studies reviewed above. While there has not been a great deal of research on the effect of degradation of the sensor subsystem and human performance, such research as was conducted offers the following findings:

- Sensor degradations can make displays difficult to understand.
- Graphical displays, especially those employing emergent features, appear more subject to the effects sensor degradation than more traditional types of displays.[7]
- Operators have difficulty distinguishing between process- and sensor-failures.
- Improved instrumentation can help operators distinguish between sensor issues and process disturbances by supporting comparisons to related performance parameters.
- Operators' task performance worsens as the magnitude of sensor noise increases.
- Operators change their control strategies as sensor noise rises, and this effect is more pronounced when EID displays are used; this behavior may compensate for a decrease in the usefulness of emergent display features.

These findings show that the effects of sensor degradations on displays and human behavior are complex. We offer two examples illustrating this point. In one example, an operator is monitoring a plant in a steady-state condition, such as at 100% power, under relatively unchanging plant parameters. Then, the HSI shows a drop in the pressurizer's level. Based on this information presented, the operator may suspect a LOCA event has begun, when in fact, a degraded sensor is giving false level readings. As a second example, an operator takes a control action, such as to increase the pressurizer's level, and observes the HSIs to assure that it is doing so. If no change is observed, the operator may conclude a pump or valve has failed, when actually the level sensor is degraded. Thus, the level is increasing, but the increase is not shown in the HSI. Table 4-1 illustrates the complex relationship that can occur between different sensor conditions and an operator's situation assessment.

[7] We might conclude from these studies that graphical displays, such as those we described, should be avoided due to their sensitivity to sensor degradations. However, considerable research over the past decade demonstrated the effectiveness of such displays for supporting operator performance, especially when dealing with unplanned- and unanticipated-events (Burns et al., 2008; Jamieson, 2007a, 2007b; Lau et al., 2008a, 2008b; Vicente, 2002). The graphical features are easier for operators to process than mentally integrating individual parameters, and they reveal relationships between information that are important to situation assessment. Thus, graphical displays are likely to play a more important role in future control rooms. Rather than avoiding their use, methods for minimizing the potential negative influences of sensor degradation should be sought.

Table 4-1 Potential Relationship Between Sensor Failure and the Operator's Situation Assessment of a Low-Pressurizer-Level Event

Low Pressurizer Level Event	**Event Occurs**	**Event Does Not Occur**
Level Sensor Accurate	Correct Assessment	Correct Assessment
Level Sensor Fails In Normal Range	Incorrect Assessment	Correct Assessment
Level Sensor Fails Low	Correct Assessment	Incorrect Assessment)
Level Sensor Fails High	Incorrect Assessment	Incorrect Assessment

The studies we reviewed in this section had several limitations for generalizing the findings to the target operational context we are interested in. We summarize our target operational context along the following dimensions:

- *Application Domain* – commercial nuclear power plants
- *I&C System* – digital commercial I&C systems
- *Personnel* – highly-trained, professional operators
- *HSIs* – alarm, displays, and controls presented in control rooms and local control panels

Research results are generalized most easily to this operational context when the studies are based on the same types of personnel, application domains, I&C systems, and HSIs as found in the target operational context. To the extent that the findings discussed were obtained under different circumstances, our confidence in extrapolating the results to our target context is lowered. In considering the studies we reviewed in this section, we define several limits to the generalization of the results:

- *Application Domain* – While the domains varied, the simulated systems usually were very simple and did not involve the complexity of real-world operations.
- *I&C System* – The I&C "systems" modeled in these studies were greatly simplified from those that would be found in a commercial NPP, e.g., based on a few sensors rather than hundreds of them. In addition, the application of sensor noise often was unrealistic, e.g., when noise is applied equally to all sensors.
- *Personnel* – While some professional operators participated in these studies, most research used student participants with very restricted training. Unlike professional operators, they had limited expertise with the systems, minimal experience with operations, and their monitoring and control strategies were evolving.
- *HSIs* – The user interfaces were very simple, lacking the complexity and number of displays as are found in a typical plant.

The impact of more realistic sensor degradations on the performance of highly-skilled professionals, operating real-world nuclear power systems, and using a full suite of control room HSIs may well be different from what was observed in these studies. Additional research is needed to address these differences.

A variety of strategies can be employed to minimize the potential impact of degradations of the sensor and monitoring subsystems on operator performance;

- Analyze the impact of I&C failures on HSI
- Support monitoring of I&C systems and detecting degraded conditions
- Ensure information quality at the HSIs
- Distinguish directly sensed information sources from derived ones

Analyze the Impact of I&C Failures on HSIs

One concern about I&C degradations, particularity of the sensor and monitoring subsystem, is that they can (1) render displays difficult to interpret, and (2) perhaps worse, can make displays look as though a process disturbance has occurred. Analyses conducted during the design process should help to ensure that these effects are understood, and should offer the opportunity to minimize misleading the operators. These analyses should focus on identifying the HFE-significant I&C degradations; i.e., the failure modes and degraded conditions of the I&C system that potentially might impact HSIs used by personnel in undertaking risk-important tasks.

A variety of approaches were employed to address this concern, including human-reliability analysis (NRC, 2000), confusion matrices (Kim & Seong, 2008), and misdiagnosis-tree analysis (Kim, Jung, & Park, 2005; Kim, Jung, & Son, 2008). Each is briefly discussed below.

Recent approaches to human-reliability analysis recognize the importance of the potential impact of sensor failure on an operator's situation assessment, and, in turn, the affect of faulty situation assessments on errors of commission (e.g. Kim, Jung, & Park, 2005; Kim, Jung, & Son, 2008; NRC, 2000). For example, one approach to human reliability analysis (HRA) called "A Technique for Human Event Analysis" (ATHEANA) recognized the importance of situation assessment on human actions and errors (NRC, 2000). Factors that lead to incorrect assessments were identified as part of the analysis, including sensor failures. This led to the development of efforts to predict errors of commission resulting from poor situation assessment. ATHEANA's methods are useful in the current context in that they offer possible approaches to analyzing sensor degradations to identify those that might lead to incorrect situation assessments.

Kim and Seong (2008) proposed a method to evaluate the potential for senor faults to engender incorrect situation assessments that resembles a classic confusion-matrix technique. The methodology involved generating two sets of patterns, using a plant simulator. One set is HSI information patterns for transients and accidents of greatest concern; the other set is those that would result from various types of sensor failures. The analyst then compares the two sets of patterns to identify ones that are very similar and, therefore, could lead operators to misdiagnose a sensor failure as a transient or an accident.

Since there a very many HSIs in modern NPPs, conducting these analyses for all of them would require considerable effort. Accordingly, they might be applied in graded fashion by identifying the more important human actions and the HSIs most vital to plant safety.

Support Monitoring of I&C Systems and Detecting Degraded Conditions

O'Hara and Higgins (2008) developed guidelines to support operators in detecting, identifying, and managing the degradations of automatic systems. Many of them address HSI features that support operators in monitoring automation; in general, a large part of this guidance is applicable to I&C conditions. HSI displays should support the monitoring of the I&C system's performance, the identification of degradations in it, and trouble shooting of performance problems that exist.

Alerting operators via alarms to degraded I&C conditions will favor the operator's recognition of system degradations. If the HSI includes performance measures for I&C subsystems, operators can monitor that performance when needed. Comparisons of current performance with typical performance will enable operators to detect changes in the system changes. An example is to give operators details of time delays, particularly when they are longer those the operator typically experiences. NUREG-0700 already addresses this with respect to displaying failures (Guideline 1.1-22: Indication of Proper Display Operation and 1.1-23: Indication of Display Failure), but the principle can be extended to the entire I&C system.

Ensure Information Quality at the HSI

One approach to minimizing the impact of a degraded sensors and monitoring system is to ensure that the correct information is displayed at the operator's HSI, and to code any suspect information. Techniques such as signal validation and analytical redundancy (calculating expected parameter values using a model of the system's performance) can assess the correctness of the information before displaying it. The results of these techniques can validate information, invalidate it, or fail to determine either state. NUREG-0700 has guidance on these aspects of display design (see guidelines 1.4-9: Invalid Data, 1.4-10: Unvalidated Data, and 1.1-21: Analytical Redundancy).

Distinguish Directly Sensed Information Sources from Derived Ones

The Reising and Sanderson (2002a) study we discussed earlier showed how displays can be misleading when they include directly sensed and derived information (Figure 4-6). One way to minimize this issue may be to distinguish between these two types in a display so operators readily can determine between the two sources of information. Unfortunately, we know of no empirical evidence to confirm the benefit of this approach (see Section 4.5, Future Research Topics, "Effects of Sensor Degradations on Different Types of Information Sources").

4.2.2 Degraded Automation/Control and Communication Subsystems

As we noted in the introduction to Section 4, some research that, while not specifically directed at I&C degradation, provides insights that can be extrapolated to it. Specifically, research on automation gives clues into the degradation of the automation and control subsystem, while studies of time delays clarify degradation of the communication system. Each is discussed briefly below.

We reviewed these studies addressing the relationship between automation design and human performance, including automation degradation, in a recent NRC report (O'Hara & Higgins, 2010). We summarize the general findings on degraded automation here.

Automation degradations often are very difficult to detect and when automation completely fails, operators might be challenged in assessing the plant's current situation, and assuming manual control of the functions and tasks that automation was performing. Understanding why degradation is hard to deal with gives us insights to how the challenges can be minimized. O'Hara and Higgins (2010) identified two factors contributing to this difficulty: Over reliance on automation and the HSI's design.

The problem in detecting degradations of automation in part is because automation often performs tasks independently from plant personnel. Personnel often have other tasks for which they are responsible. While personnel do play a role in monitoring the performance of the automation, that responsibility often becomes compromised in the face of workload pressures. This problem is exacerbated when automation is reliable, and personnel trust and depend on it to function properly. Such trust in automation can lead to "over reliance of automation" (Parasuraman & Riley, 1997); i.e., personnel may continue to use automation, even when it does not correctly fulfill its functions. Over reliance contributes to the difficulty personnel have in detecting degradations of an automatic system.

When automation deteriorates to the point where it fails to perform properly, personnel have to carry out its tasks manually. This often is challenging because their over reliance leads to "out-of-the-loop unfamiliarity" (Lee, 2006; Wickens & Hollands, 2000); that is, the loss of situation awareness about the behavior of the automation and the status of the systems being controlled. Thus, in addition to assuming the responsibility for automation's tasks, personnel must engage in significant situation assessments. Such unplanned transition from automatic- to manual-control is a period of very high workload (Huey & Wickens, 1993). The shift often requires a change in the concept of operations wherein the roles and responsibilities of individual crew members must alter to compensate for the loss of automation.

Our NRC study on integrating advanced HSIs into an existing NPP control room offers an example of the shift in concept of operation (Roth & O'Hara, 1999, 2000). One of the HSIs was a computer-based procedure (CBP) system for emergency operating procedures (EOPs). The CBP automated many of the EOP tasks formerly performed by operators including

- retrieving data and assessing its quality
- analyzing the logic for each procedural step
- keeping track of location in the procedure
- tracking of continuous applicability
- assessing cautions, safety-function status trees, and fold-out page criteria.

As a result of the automation the CBP provided, EOP use was changed from a three-person activity to an activity mainly performed by one person.

Crews were observed during their training with the new systems on a full-scope simulator. The training included simulations of plant disturbances, one of which was a loss of the CBP system (thus a loss of automation). After the simulated scenarios, the crews were interviewed to garner information about the impact of the new systems on their tasks, teamwork, and performance.

Upon CBP failure, the crew transitioned to using paper EOPs and the conventional control room displays, and EOP use shifted from a one-person activity to one requiring three people. In this study, the loss of automation occurred early in the scenario and the crews successfully managed the transition. Also, the transition away from automation was made easier because the crews

were relatively inexperienced in CBP usage, and the change brought them back to their normal, familiar way of operating. The transition may have been significantly more difficult if the crew's normal mode of operation was using the CBP, and the loss of automation required them to transition to a mode wherein much less automation support is provided, and much more crew coordination and communication is required. Thus an important finding of this study is that it highlights that upon loss of automation, crews must transition as a team to a different concept of operations where individual team members assume different roles and responsibilities.

Another factor contributing to the difficulty personnel have in detecting automation degradations is the design of the HSIs used to monitor automation. Willems and Heiney (2002) stated that "As errors involving automation tend to be more cataclysmic and costly, the human interface has become more important than ever" (p. 3). The HSIs typically provide insufficient information about automation's goals, current activities, and performance (Liu, Nakata & Furuta, 2004; Lee & See, 2004; Parasuraman & Riley, 1997; Roth et al., 2004; Rook & McDonnell, 1993).

Control performance is influenced not only by the automation/control subsystem, but also by the communication subsystem. Increased time delays can be one form of performance degradation in a digital system. While research on time delays does not specifically addressed the deterioration of the communication system, insights from research on time delays provides an insight into the effects of such delays when attributed to communication system degradation.

Most systems have inherent time delays, or lags, that stem from

- time from when a control action is taken at the HSI to when the signal reaches the actuation system
- the time it takes for the system to change in response to the control action
- time between the change in system's response and the change in the HSI (feedback).

The first and third delays are affected by the communication subsystem.

Research showed that time delays affect human performance (Wickens 1984, 1986, 2004), as we summarize here. As time delays increase there is a decrease in closed-loop control (control based on feedback) and a shift to the more difficult open-loop control (based on prediction) strategies that increasingly destabilizes control. In this context, control stability refers to a system's response to operator inputs. When stability is good, the system responses and the operator's control inputs are coupled tightly; as it declines, the systems response progressively becomes more unpredictable. As the time between operator's input and system response lengthens, closed-loop control becomes more unstable. That is, there is a drop in the value of feedback as a means for operators to regulate their control actions. We illustrate this effect simply. Thus, an operator may have initiated a control action to increase pump speed to a specified value, but having observed no change in speed because of a time delay, the operator may again take another action to increase pump speed. The two control inputs cause the pump's speed to rise a much greater value than the operator intended. Consequently, the operator then takes a control action to reduce speed, but again, due to time delays, no change is observed; then, the operator repeats the same action generating a larger decrease in pump speed than desired. The operator's control of the pump has become unstable. When such time delays destabilize closed-loop control, often shift to a more difficult open-loop control strategy; i.e., control based on prediction rather than feedback. It is a more cognitively demanding, knowledge-based approach to control (Wickens, 1984).

Lorenzo (1990) gave the following example of the effect of delayed feedback on operator behavior in a chemical plant:

> A computer-based control system was so overloaded by a process upset that it ceased to update the video terminals in the CR. Unaware that the displayed information was inaccurate, operators unknowingly moved valves to their fully open or closed limits while waiting for the display to show some response. The mis-positioned valves worsened the upset, eventually causing an emergency shutdown of the unit when some relief valves lifted. (p. 15)

These findings suggest that degradations of the I&C's communication subsystem leading to time delays may degrade the operator's monitoring and control performance.

The various strategies we summarize below can minimize the potential impact of degradations of the automation/control and communication subsystems on operator performance:

Support I&C Degradation Detection and Management in Training

Operator training also plays an important role in supporting operators to detect automation degradations and to understand the types that can occur. A similar training can be extended to the rest of the I&C system. Indeed, Reising and Sanderson (2000a) stated that "If the operator knows the failure modes of a sensor, then sensor output can carry considerable information" (p. 580).

Training can provide operators with clear and specific information so that should the I&C subsystem become degraded they

- understand how and why it might degrade or fail
- understand the implications of such degradations for HSI and their own performance
- monitor the I&C system's performance so to detect and recognize degradations via control room HSIs
- perform recovery- and compensatory-actions, perhaps using procedures
- smoothly transition to backup systems when needed
- how the roles and responsibilities of crew members and the concept of operations are affected

Further, simulator training specifically giving operators experience of automation failures helps s them to deal effectively with any failures (O'Hara & Higgins, 2008). We think it is likely the same type of training can assist operators in recognizing and managing degradation in other I&C subsystems.

Support the Management of Time Delays

Another approach is stems from research on telerobotics, e.g., controlling robotic devices from a remote location. Telerobotic control often involves time delays, especially in space operations. To compensate for them, operators are given predictor (or predictive) displays that provide immediate feedback to operators about the effect of their control actions on system's performance. The predictions are based on models that determined what those effects would be. Predictor displays

effectively addressed human-performance issues arising from time delays (Wu, Wang, & Wang, 2006; Xiong, Li, & Xie, 2006).

4.2.3 Summary

There has been limited research on the effect of I&C subsystem degradation on HSIs and human performance, especially with professional operators. However, the findings offer some preliminary insights. We organize and summarize them by I&C subsystem below.

Research on the degradation of the sensor and monitoring subsystems offers the following insights:

- Sensor degradations can make displays difficult to understand particularly when operators use graphical displays with emergent features rather than traditional types.
- Operators can have difficulty distinguishing between process failures and sensor failures unless this discrimination specifically is addressed in the HSI design.
- The sensor's configuration affects an operator's ability to distinguish process failures and sensor failures. The latter are easier to detect when HSIs display has actual rather than computed values.
- The operator's task performance declines as the magnitude of sensor noise increases. In addition, with increasing noise, operators may change their control strategies; this effect becomes more pronounced when graphical displays are used. This behavior may compensate for the decrease in the usefulness of emergent features as sensor noise increases.

Research on the deterioration of automation and control subsystems reveals the following,

- automation degradations often are very difficult to detect
- when automation completely fails, operators may be challenged to assess the current status of the tasks that automation was performing and the systems it was controlling, and hence, to assume manual control of those tasks automation failures can lead to a need for a more manual CONOPS, changing the roles and responsibilities of crew members
- factors contributing to this difficulty include over reliance on automation and HSI design

Research on time delays affords some understanding of the effects of communication subsystem degradation on the operator's performance,

- as time lags increase, the operator's control performance decreases
- the operator's closed-loop control becomes increasingly unstable
- operators shift the control strategies and their performance becomes increasingly open-loop; i.e., based on prediction rather than feedback

Thus, we conclude from this limited research that the impacts of degraded I&C can be significant, and adversely affect the HSIs and the operator's performance. Also, we must consider these insights within the particular context of these studies. Many of the tests were undertaken by students, performing relatively simple tasks, using uncomplicated HSIs to monitor and control

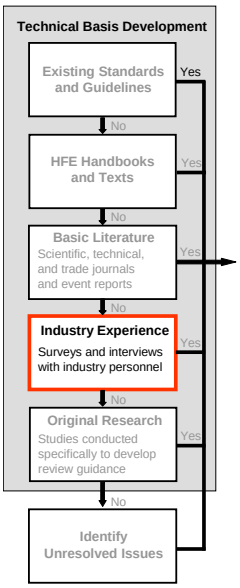
elementary systems. Research corroborating these findings is needed using professional operators and more realistic, complex environments.

As we noted in the introduction to this section, the insights derived from the research are limited by its scope. For example, only sensor failure and noise were studied in exploring the degradation of the sensor subsystem, Other than research on degraded automation, there is very little research on the effect of degradations to the other I&C subsystems on HSIs and human performance. Thus, the diversity of degradations and failure modes of the I&C system has hardly been probed. Additional research is essential to define robustly the relationships between degraded conditions and HSIs/performance.

We described a variety of strategies that might minimize the potential impact of I&C subsystem degradations on operator performance. The strategies include the following ones:

- Analyze the impact of I&C failures on HSIs
- Support monitoring of I&C systems and detecting degraded conditions
- Ensure information quality at the HSIs
- Distinguish directly sensed information sources from derived ones
- Support I&C degradation detection and management in training
- Support training on the management of time delays

4.3 Analysis of Industry Operating Experience



Operating experience gives information about the effects of degraded I&C on the operator's performance; however, little of it is available for digital I&C and computer-based HSIs (O'Hara et al., 2008a; 2008b; Wood et al., 2004). Especially lacking are studies that analyze numerous events to identify lessons learned for these systems. SMEs identified the lack of operation experience as a top-priority issue, entitled *Operating Experience and Lessons Learned* (O'Hara et al., 2008a; 2008b) with respect to using digital technology and computer-based HSIs.

With this caveat, we evaluated the information in studies and individual event reports (Licensee Event Reports or LERs). Our discussion is divided into five subsections. The first summarizes studies that collected and analyzed nuclear-industry experience with digital I&C degradations, focusing on their prevalence and general importance; they do not specifically address human performance. The second section discusses studies of operating experience that dwelled on the human-performance implications. In the third subsection, we analyze specific events involving I&C degradations for which there is information about the effects on operators. The fourth subsection discusses approaches to minimize these identified effects. The final subsection summarizes the lessons learned from our analysis of operating experience.

4.3.1 Analysis of the General Prevalence and Importance of I&C Degradations

Both the NRC and the commercial nuclear industry have been evaluating the incidence of digital I&C failures. Their findings help address general questions, such as how frequently digital systems fail, and if the outcomes are significant enough to be a concern.

Brill (2000) evaluated the number of NPP digital I&C failures based on information on the licensee event reports (LERs) compiled over five years starting in 1994. He found 385 events involving a digital I&C; eight percent all the LERs issued over the period. Figure 4-5 displays the distribution of digital I&C failures involving hardware, software, or HSIs, the latter including personnel and procedural errors involving the digital I&C systems.

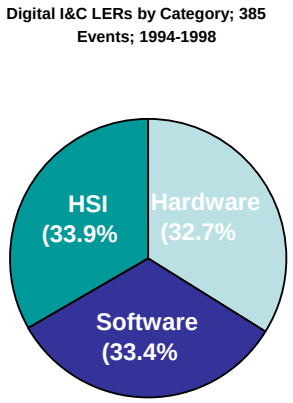


Figure 4-5 Distribution of I&C failures
(Source: Brill, 2000)

Many digital I&C failures resulted in reactor trips (see Figure 4-6), and 36 percent of the problems occurred in safety-significant systems (although some of these were administrative ones, such as missed surveillance tests required by plant technical specifications).

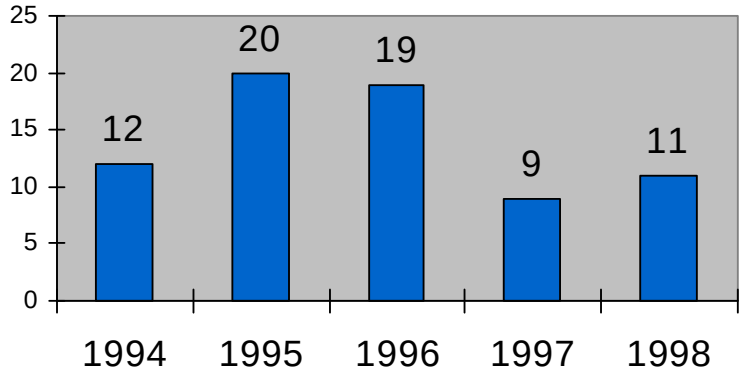


Figure 4-6 Percent of digital I&C failures resulting in reactor trips
(Source: Brill, 2000)

Brill concluded that the failure of digital systems affects plant performance and safety. This conclusion is consistent with recent research about the impact of failures of I&C systems on the plant's risk (Chu et al., 2008). They studied a digital feedwater control system for a PWR, demonstrating that the potential impact of failures of this type of digital control system on risk primarily were associated with the likelihood of a reactor trip and significant plant transient due to a loss of feedwater.

The NRC established a database to maintain data on digital I&C failures (Waterman, 2006) that includes approximately 400 selected digital I&C failures that occurred between 1987 and 2006. Many of them illustrate that digital I&C degradation potentially can affect human performance in the main control room, the technical support center, and emergency operations locations. The events Waterman identified illustrate that failures have occurred in each of the digital I&C subsystems described. The following are examples of operating experience during 2005 and 2006 and the I&C subsystem involved:

- *Sensor subsystem* – St. Lucie experienced failures on 3/16/06 and 3/19/06 that rendered inoperable the Emergency Response Data Acquisition and Display System (ERDADS). These failures resulted in the lack of updates to the Technical Support Center's operator consoles, leaving the displays essentially static during a training exercise.
- *Monitoring subsystem* – At St. Lucie Unit 2 on 6/29/06, the maximum power level allowed by the operating license was exceeded due to a software error in the distributed control system (DCS). The DCS calculated a slightly lower value for feedwater flow value than the actual one, and it was used as an input into the calorimetric power calculation. The error resulted in a non-conservative (lower) indicated power in the control room. Based on this faulty information, the operator increased power beyond the allowed level.
- *Monitoring subsystem* – The safety parameter display system at Wolf Creek was lost on 6/12/06 due to a multiplexer failure in the link between the computer and the display panel.
- *Automation/Control subsystem* – In October 2005, Byron Unit 2 experienced a reactor trip. The root cause was the failure of the Digital Electro-hydraulic System to automatically

runback the turbine as designed. This was due to an application software fault that effectively rendered all automated turbine runbacks inoperable.

- *Communication subsystem* – Diablo Canyon Units 1 and 2 experienced a failure of the data-communication system from the plant to the NRC Event Response Center in June 2006. Problems were identified in the electronics of the Emergency Response Facility Data System (ERFDS).

EPRI analyzed operating experience data involving digital I&C degradation that was reviewed to assess the potential for common-cause failure (CCF) (Torok et al., 2008). These data were derived from both LERs and the Institute for Nuclear Power Operations' (INPO's) operating experience reports.

The authors evaluated 322 events from a period of 20 years and found:

- The majority (18 of 27) common defect events in safety-related (Class IE) systems affected subsystems or channels, leaving the balance of the system unaffected and available to perform its overall safety function.
- Software changes often were implemented as corrective actions for non-software problems, thereby allowing the problem to reoccur if there were other software-changes made, and
- Most reported defects were discovered within 1 to 2 fuel cycles after putting the digital systems into service.

EPRI analyzed the digital I&C failures and identified the following causes:

- inadequate design (software and hardware)
- incorrect parameter value
- hardware failure
- human performance (incorrect set points cited as an example)
- ineffective configuration management
- inadequate testing

Torok et al. noted that the hardware and software of digital I&C can undergo deterioration with the potential of impacting the HSI. In some cases, the degradations have no affects on the system's function, while in others they are significant. Another assertion by the authors is that "…non-IE systems are more susceptible to common cause failure due to their functional complexity" and, "…their use of shared resources (e.g. power supplies)". Some events we discuss in the next section are associated with declines in the digital I&C system power supply that challenged the operating crew due to the multiple impacts they had on the HSI.

In summary, these studies show

- digital I&C degradation has occurred regularly, and expectedly will increase in frequency as more systems are used
- degradations occur in all I&C subsystems
- deterioration of digital I&Cs can have major consequences, i.e., involve reactor trips, and impact safety systems

- approximately a third of the events involved the HSI, indicating the possibility for the digital I&C failure to lower the operator's ability to monitor the plant and respond to the event
- impacts were experienced in key areas, including the main control room, the technical support center, and emergency operations locations

4.3.2 Studies Examining the Human Performance Effects of Degraded I&C

Galletti (1996) reviewed five events involving digital systems that had implications for human performance. One event involved a degraded monitoring subsystem; i.e., a microprocessor-based overhead annunciator (OHA) system locked up causing the loss of alarms in the main control room. This condition went undetected by the crew for over one hour. An operator discovered it when he received an alarm on an auxiliary alarm printer and noticed that the corresponding OHA window did not alarm. Subsequent investigation revealed that the OHA system could be locked up if an operator made a particular keyboard entry when a system panel switch was mispositioned. Key contributors to the event included

- *Inadequate system design* – The HSI did not adequately indicate of the monitoring system's failure.
- *Inadequate procedural guidance* – There was no procedural guidance to mitigate a loss-of-annunciator condition, or to use alternate control room indications when such a degraded condition occurred.
- *Lack of adequate operator training* – Operators were not trained to deal with a loss of annunciation situation. They were not cognizant of indications of OHA system degradations, and were not trained to routinely verify its proper operation.

When digital systems lock up (e.g., processors either stop processing or perform infinite calculations), there may be no obvious indications for the operators. Many things trigger lockups, including a power interruption, voltage change, or improper operator input. Operators may be unaware that a failure has occurred because the display may have stopped at a reading within the normal operating range. Digital systems do have alarms for system failures, but they alarms may not signal all degraded conditions.

Woods et al. (2004) obtained information from organizations involved with designing, operating, and licensing of digital I&C technology in new and modernized plants. One incident involved a software error that corrupted data at the Korean Uljin Nuclear Power Station Unit 3. The failure involved an application-specific integrated circuit in a network interface module of the digital plant control system (DPCS). The failure caused several non-safety components to behave unexpectedly, e.g., pumps starting, and valves repositioning without a command to do so. The operators detected and responded to the situation without any negative consequences. The problem was due to a common-cause software error that was fixed. In addition, an alarm was installed in the main control room to alert operators of possible network failures, and a procedure written to address such situations.

The NRC's development of "A Technique for Human Event Analysis" (ATHEANA) (NRC, 2000) assessed operating experience. The authors analyzed selected operational events to understand human performance using theories of human cognition and human reliability models. ATHEANA was intended to increase the degree to which an HRA can represent the kinds of human behaviors seen in accidents and near-miss events at NPPs, and at facilities in other industries

that involve similar kinds of human-system interactions. The goals of the ATHEANA methodology are to improve the analyst's ability to

- understand the kinds of human-system interactions that have played important roles in accident responses, including identifying and modeling of errors of commission and dependencies
- take advantage of, and integrate advances in the disciplines of psychology, engineering, plant operations, human factors, and probabilistic risk assessment (PRA) in modeling personnel actions

ATHEANA identified certain characteristics important to situations in which degraded digital I&C systems could be included. The factors that may complicate operators' responses to events include:

- Scenarios that deviate from operators' expectations, based on their training and experience,
- Multiple equipment failures and unavailabilities (especially dependent- or human-caused-ones) that go beyond those represented in operator's training in simulators and assumed in safety analyses, and,
- Instrumentation problems for which the operators are not fully prepared that might entail misunderstandings about the event.

The operating events reviewed in ATHEANA contained challenges to operators that were not considered in earlier risk analyses, including "…deviations associated with failures in instrumentation systems that make it difficult for operators to understand and plan suitable responses." In many cases, such deviations can lead operators to fail because of a mismatch between their expectations and the plant's behavior. For example, when a plant behaves in a way that is significantly different from the operators' expectations (a mismatch between plant behavior and training), and the operators respond in accordance with their expectations, their resultant actions can lead to loss of important equipment operation and functions for the conditions actually taking place.

In Table 4-2, we summarize several examples of degradations in the I&C sensor subsystem that affected human performance.

Table 4-2 Events Impacting Human Performance from ATHENA

Event	Sensor Subsystem and HSI	Human Performance
Crystal River 3 (RCS pressure transient during plant startup)	Indication of the pressurizer spray-valve's position was inconsistent with its actual position. There was no direct indication of pressurizer-spray flow.	Situation Assessment - Operators develop wrong situation model.
Dresden Unit 2 (Stuck open relief valve)	Due to a position-sensor failure, the position indications for the safety- relief valve showed the valve closed while it had failed open.	Situation Assessment - Operators were surprised by the increase in torus temperature because they developed the wrong situation model.
Ft. Calhoun (Inverter failure followed by stuck open relief valve)	Due to the failure of a position sensor the position indications for the safety-relief valve were faulty. Also, a power-supply failure degraded the computer displays normally used to monitor containment temperature and RCS cooling.	Monitoring and Situation Assessment - Operators had difficulty obtaining the needed information and developed the wrong situation model. Response planning also was impacted because procedures did not adequately address in detail the incorrect position indication.

The authors concluded that the incorrect indication provided to the operators caused them to be unaware of (1) the plant's actual state, (2) the severity of plant conditions, and (3) the deterioration in plant conditions.

4.3.3 Selected Case Studies of Events Involving Digital I&C Degradations

We evaluated eight events involving digital I&C degradations to identify more specifically their implication for the human performance. The evaluation is summarized in Table 4-3, at the end of this section.

We selected three events, listed below, for more detailed analysis since each was deemed significant in the NRC Information Notices issued. Two of them had warranted special NRC Inspection teams whose reports gave us more detailed information than typical is available in event reports.

- Inadvertent safety injection signal with failure to reset
- Degraded Ethernet communications
- Failure of the power supplies to the digital feedwater system

Inadvertent Safety Injection Signal with Failure to Reset

Here, the failure of a single component (zener diode) within a protective system's logic card caused an unusual transient so that several local manual actions were needed to reset the invalid signal and secure the safety-related equipment. The zener diode that failed was located in circuitry associated with the automatic initiation of a safety system. In the main control room, operating personnel were aware that the safety system was initiated, and determined that it was spurious (not valid). However, when they reset the initiation signal, the relays did not reset everything the operators expected because of the voltage had been degraded by the failed diode. In fact, the initiation signal for one safety-injection train could not be reset (it was "sealed-in.")

This event was documented in a Licensee Event Report (LER 379-07003) and NRC Information Notice 2009-03. These documents identify several instances where the crew's performance was impacted by the degraded I&C system:

- The operating crew attempted to reset both trains of the Safety Injection (SI), but could only reset Train A. They did not know why Train B could not be reset.
- There was no procedural guidance on how to respond to an SI signal that could not be reset from the control room.
- Motor-operated valves could not be operated from the control room, so operators had to be dispatched to manually operate them.
- A troubleshooting sheet that I&C personnel used to assist the operating crew was not sufficiently comprehensive and resulted in an incorrect configuration of the safety-system's logic. This error was detected during the recovery.

The diode failure degraded the automation/control subsystem and prevented the operators from responding by taking corrective actions via their controls. Consequently, they lost situation awareness and their ability to rectify the abnormal situation.

The NRC inspection report noted several examples wherein the actions taken by the operators were knowledge-based and skill-of-the-craft rather than procedurally driven. The inspection team also noted that "…the licensee did not have a surveillance or maintenance program that was able to identify degradation of reactor protection system logic cards;" nor did the licensee "…have a method of trending and documenting component performance and thus identifying degraded components prior to failure."

Table 4-3 lists the sequence of events, the different procedures used, the manual actions that were necessary, and the misleading information that was provided to the operating crew from the degraded digital I&C conditions.

Table 4-3 Sequence of Events for the Inadvertent Safety Injection Signal with Failure to Reset Event

Date/Time	Event/Action	Comment
6/29 1752	Unit 2 main feedwater pumps tripped due to spurious 'B' Train SI signal	
1753	Operators manually actuated both SI trains	Per emergency operating procedure
1800	Operators tried to reset the SI signal from the MCR but the "B" train would not reset	Degraded voltage condition caused 'B' train master relays to remain energized
1810-1830	One PORV begins lifting; pressurizer relief tank rupture disk ruptures; containment sump high level alarm; Boron injection tank (BIT) valve manually closed.	BIT Valve not operable from control due to sealed-in B train logic; PORV cycled ~ 50 times; 2800 gallons of reactor coolant flowed to the containment basement
1840	Operators restored letdown flow using guidance contained in Abnormal Procedure "Loss of Vital Instrumentation"	
1851	I&C technicians used troubleshooting procedure to assist Operations in resetting the B train SI signal	This involved placing the mode selector switch in TEST
1854-2058	Operating crew realigned equipment from the MCR. They could not secure the EDG which ran unloaded for two hours	The SI signal was still present. Operations placed the EDG switch in the Emergency Stop position
6/30 0839	Unit 2 entered cold shutdown mode	Significant numbers of manual valve operations were required to achieve cold shutdown
1100	Operations personnel removed the fuses from both trains of SSPS	This de-energized all master and slave relays so that equipment could be returned to its normal configuration

Degraded Ethernet Communications

NRC Information Notice 2007-15 (NRC, 2007) describes an event involving an overloaded Ethernet communication system linked to a recirculation pump's control system. The communication system broke down because of excessive data traffic. When the degradation occurred, the recirculating pump's speed-control demand signal fell to zero and decreased the pump's flow, resulting in a plant scram due to a potential high-power, low-flow condition. The two variable frequency drives (VFDs) regulating the speed of recirculating pumps failed, entailing the need for a manual scram. The variable frequency drive (VFD) controllers, connected to the plant's integrated computer system network, failed due to excessive traffic on the network. The NRC issued this notice because of the unanticipated effects that the failure of Ethernet, connecting non-safety equipment, had on the plant's safety and performance.

The degraded communication subsystem affected the controls (recirculation pump's speed controls) and information HSI subsystems; thus, the HSI subsystem gave the operators no indication that the Ethernet was experiencing heavy data traffic, and that it might be degraded (i.e., lowered their situation awareness). The crew also lost their ability to implement the appropriate response because they could not control the recirculating pump's speed and flow.

The Ethernet communication subsystem interacts with many aspects of the digital I&C system and with operating personnel. The t overload on it affected the recirculating system's controls (non-safety) that, in turn, caused a drop in speed of the motor-generator set and recirculating flow that instigated plant trip. The NRC concluded that "…careful design and control of the network architecture can mitigate the risks to plant networks from malfunctioning devices, and improper network performance, and ultimately result in safer plant operations."

The Licensee's corrective action included installing a network-firewall device that limits the connections and traffic to any potentially susceptible devices on the plant's network. The Notice states that "Excessive data packet traffic on the network may cause connected devices to have a delayed response to new commands or even to lockup, thereby, disrupting normal network operations. This excessive network traffic is sometimes called a broadcast (or data) storm. A network found to be operating outside of normal performance parameters with a device malfunctioning can affect devices on that network, the network as a whole, or interfacing components and systems. The effects could range from a slightly degraded performance to complete failure of the component or system."

In this event, the communication subsystem (data highway) significantly limited the ability of the operator to control essential plant equipment.

Failure of the Digital Feedwater System Power Supplies

A power supply in a Digital Feedwater Control System (DFWCS) degraded to the point where it could not carry the required load when a secondary power supply failed. A status light on the power supply indicated that it was operating normally, so the operators were unaware of its degraded condition. Failure of the power supplies tripped both turbines of the reactor feedwater pump. In addition, the motor-driven main feedwater pump did not start automatically as it should have. The reactor tripped on low-water level, and the High Pressure Core Spray (HPCS) and the Reactor Core Isolation Cooling (RCIC) pumps started automatically. However, the RCIC tripped on low suction pressure because it was misaligned, leaving the HPCS as the sole source of high-pressure injection into the vessel.

The degraded voltage condition generated difficult operating conditions; at one point allowing the operation of the main feedwater pump, but then causing it to trip as the voltage fluctuated below allowable limits. Following the event, plant personnel found other problems, including the RCIC flow controller having being left in a degraded condition after maintenance without the operations staff being aware of it.

The NRC conducted a special inspection of the plant and subsequently issued Information Notice 2008-13 on 7/30/2008 to alert licensees to the circumstances surrounding this event. An important piece of information that was misleading to the operators was that the indicator light of the power supply showed a normal condition, and the RCIC system's status light indicated that it was operable. Degradation of the power supply therefore impaired the operator's ability to assess the situation (degraded power supply) and to respond (RCIC System was not in automatic mode).

Table 4-4 Summary of Events Involving Degraded I&C Conditions

EVENT INVOLVING DIGITAL I&C DEGRADATION OR FAILURE	I&C SUBSYSTEM	HSI SUBSYSTEM	HUMAN PERFORMANCE IMPACT	COMMENTS
Inadvertent safety injection signal with failure to reset; LER 379-07003	▪ Auto/Control	▪ Control	▪ Situation Assessment ▪ Response Implementation	Power fluctuations to digital I&C components can result in unusual failure modes.
NRC Info Notice 2007-0015; based on Browns Ferry 3 Ethernet failure	▪ Auto/control ▪ Communication	▪ Control ▪ Information	▪ Situation Assessment ▪ Response Implementation	Electronic infrastructure (data highway) degradation.
Turkey Point LER 250-1994-005-02; EDG Load Sequencer Failure; Logic error would have prevented an auto initiation of a safety injection system	▪ Auto/Control	▪ Control	▪ Response Planning and Implementation	Testing of logic circuitry made the equipment inoperable
Software problem with the core protection calculators (LER 529-2005-004) would result in the use of the last known value in the event of a failure rather than initiating a trip signal.	▪ Monitoring	▪ Alarm ▪ Control	▪ Monitoring & Detection	Latent or undetected failure.
Perry LER 438-2007-008; failures of the digital feedwater control system power supplies that caused a reactor scram with complications including the loss of injection sources.	▪ Auto/Control ▪ Monitoring	▪ Operator Support System	▪ Situation Assessment ▪ Response Implementation	Personnel were unaware of the degraded condition of the DFWC system power supplies.
An event at the Indian Point Station in September 2006 involved the degradation of the Emergency Notification System caused by software and hardware problems. The result was the inability to activate the emergency notification sirens.	▪ Auto/Control ▪ Communication	▪ Information	▪ Response Planning	Digital I&C degradation impacts beyond the main control room.
The St. Lucie Unit 2 plant experienced failures on the emergency response data acquisition and display system (ERDADS) on two occasions in March 2006.	▪ Auto/Control ▪ Communication	▪ Operator support system ▪ Information	▪ Response Planning	The loss of signal resulted in static displays.
Byron Unit 2 experienced a failure of the Turbine's Digital Electro Hydraulic Control (EHC) system due to a software error. The automatic runback feature failed.	▪ Auto/Control	▪ Control	▪ Situation Assessment ▪ Response Implementation	Operations personnel were not aware that this feature was inoperable and did not have the ability to implement the action manually.

In Section 4.2.1, we discussed strategies that might be employed to minimize the potential effects of degraded sensor and monitoring subsystems on the operator's performance. One strategy was to support operators in monitoring the I&C system and detecting degraded conditions via improvements to HSIs. The operating experience we reviewed above reinforces this recommendation. Alarms or indications are needed to support the operator's awareness of problematic conditions. The three events of degraded digital I&C systems that led to difficult situations for the operator (described in section 4.3.3) could have been minimized or prevented had additional information had been available to the operator:

- Inadvertent Safety Injection Signal with Failure to Reset – an indication that the actuation logic had not reset would have led the operators to take alternate actions much sooner than they did.
- Degraded Ethernet Communications – an indication that the rate of communication had decreased significantly would have spurred operators to take manual action of the recirculating pumps.
- Failure of the Digital Feedwater System Power Supplies – an indication that the power supply was not at full capacity would have led the operator to solicit maintenance support to prevent a failure.

In Section 4.2.2, we discussed strategies that might be employed to minimize the potential impact of degraded automation/control on the operator's performance. One such approach was to support operators in detecting and managing I&C degradation by discussing these situations and the responses to them in training. The operating experience we reviewed above reinforces this recommendation.

4.3.4 Summary

General evaluations of operating experience involving digital I&C systems have shown that digital I&C degradations occur regularly in all digital I&C subsystems, and their frequency expectedly will increase new plants are built and more digital systems are used to modernize existing plants. Approximately one-third of the events involving digital I&C degradations impact the HSI (Brill, 2000), indicating a potential for their failures to lower the operators' ability to monitor the plant and respond to the event. The impacts are not limited to the main control room; they include the technical support centers and emergency-operations locations.

The outcome of these I&C degradations can be significant, involving safety systems and causing reactor trips; in fact, the commercial nuclear-power industry has recognized many safety-related issues involving them.

Degraded I&C systems challenge several aspects of the operator's performance because they might entail unexpected plant behavior, such as the inadvertent starting of equipment. This action can lead operators to misunderstand what is happening in the plant, so they have an inaccurate situation model. Degraded I&C systems also can hamper the operator's ability to implement responses by delaying responses and feedback when a communication system overloads and slow the system.

Further, operators may be unable to monitor, detect, and be aware of the implications of degraded I&C conditions on plant performance because of lack of alarms, of information concerning the conditions, and of training. Thus, these outcomes may engender a misinterpretation of the

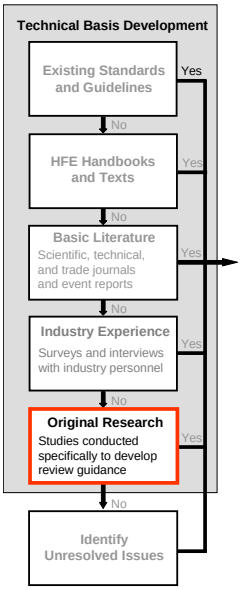
situation, and a lowered awareness of the plant's state and the severity of the conditions. Operators need improved alarms and better information on the key functional aspects of I&C and its role in the plant's response.

In addition, the operator's ability to appropriately plan responses to a degraded I&C condition is hampered by a lack of training in, and procedures for managing such conditions. The latter forces operators to rely solely on their knowledge to manage the event.

NUREG-0711 identifies the review of operating experience as an important means of ensuring that "…the applicant has identified and analyzed HFE-related problems and issues in previous designs that are similar to the current design under review". Summarizing the existing problems derived from our survey of operating experience in a manner similar to NUREG-6400, may provide the NRC's staff and applicants for operating licenses with more complete information about the effects of degraded conditions on the operators' performance. Task 3 of this project will further extend this matter.

As we noted in the beginning of this section, relevant operating experience at best is limited, so that additional studies are warranted to address the NRC-identified question of *Operating Experience and Lessons Learned.*

4.4 Analysis of a PWR Digital Feedwater Control System



In continuing our analyses, we examined a NPP's digital feedwater system. Previously, work was conducted for the NRC to determine the risk significance of digital I&C failures on this system. Chu et al. (2008) evaluated the use of traditional probabilistic risk assessment (PRA) methods for analyzing the risk contribution of digital systems adopting the Digital Feedwater Control System (DFWCS) for a specific PWR as their case study. They developed a detailed failure modes and effects analysis (FMEA) with the information obtained from the plant.

In this section, we assessed the effect of degradations of a major digital component of this system using the baseline information developed by Chu et al. Although the DFWCS is among the more complex digital control systems used in a NPP, it offers a representative example of the process that can to evaluate the effects on human performance of a digital I&C system degradation. Section 4.4.1 describes the system's key components and their relationship to the digital I&C system, and Section 4.4.2 assesses the effect of I&C degradations on the operator's performance. Section 4.4.3 discusses approaches to minimize the effects on the operator's performance that we identified. We give our conclusions in Section 4.4.4.

4.4.1 Description of the System

Here, we provide a functional- and physical-overview of the DFWCS. The plant has two reactor coolant loops, each having a reactor coolant pump and a steam generator (S/G). The feedwater system (FWS) consists of the following:

- steam-turbine-driven centrifugal S/G feedwater pumps (FWPs)
- minimum-flow control valves

- a pump-seal water system
- main feedwater regulating valves (MFRVs)
- bypass feedwater regulating valves (BFRVs)
- high-pressure feedwater heaters
- associated piping and instrumentation

There is one DFWCS per secondary loop. Figure 4-7 is a diagram of one reactor coolant loop with its associated DFWCS and the locations of the sensors. The DFWCSs of the two FWS trains share the sensors from the reactor coolant loops, and support both automatic- and manual-control.

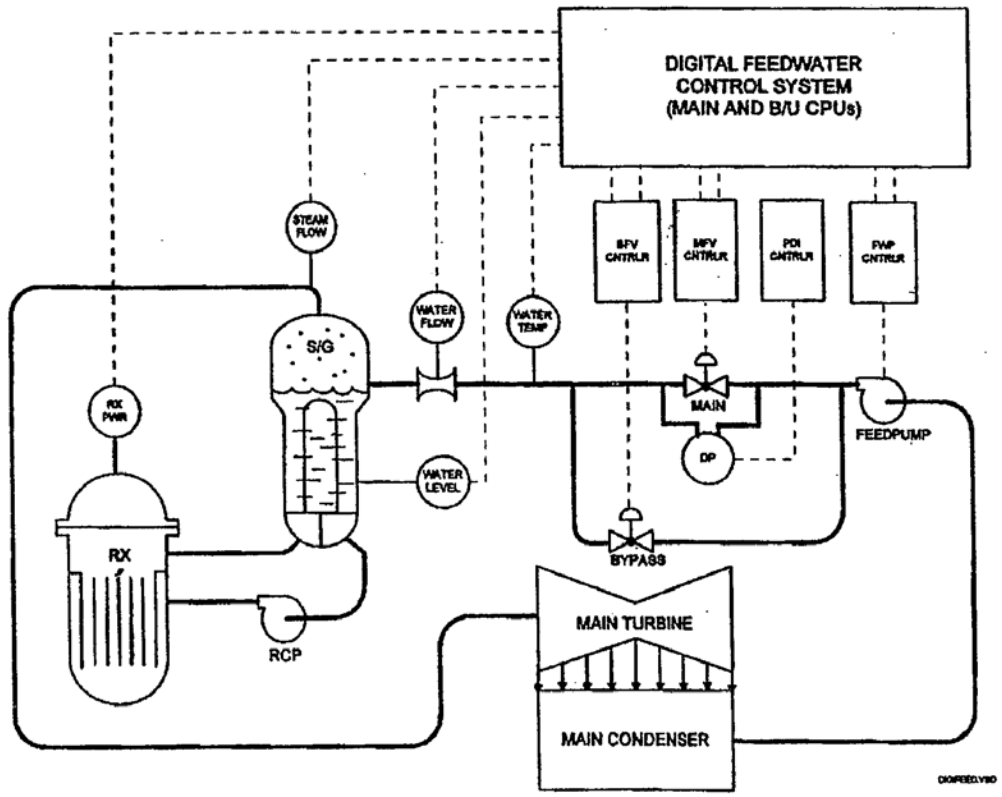


Figure 4-7 One reactor coolant loop with its associated DFWCS
(Source is Chu et al., 2008)

The DFWCS of each reactor coolant loop consists of two identical central-processing units (CPUs), viz., main and backup. The units run identical software to generate the control signals for the Manual/Automatic (M/A) controllers, i.e., the feedwater pump (FWP), main feedwater valve (MFV), and bypass feedwater valve (BFV) controllers. The Main CPU provides control demands. A failover to the Backup CPU may occur under certain circumstances, e.g., a large deviation between two feedwater level signals from the same S/G. Because of the importance of the feedwater control system, its design incorporates backup and manual override capabilities.

Figure 4-8 is a diagram showing the main components of the DFWCS (the two CPUs and the controllers), the components that are controlled (feedwater pump, MFRV, and BFRV), the HSI

(such as the displays of the MFV-, BFV-, FWP-, and pressure-differential indication (PDI)-controllers), and two of the sensors supplying data to the CPUs.

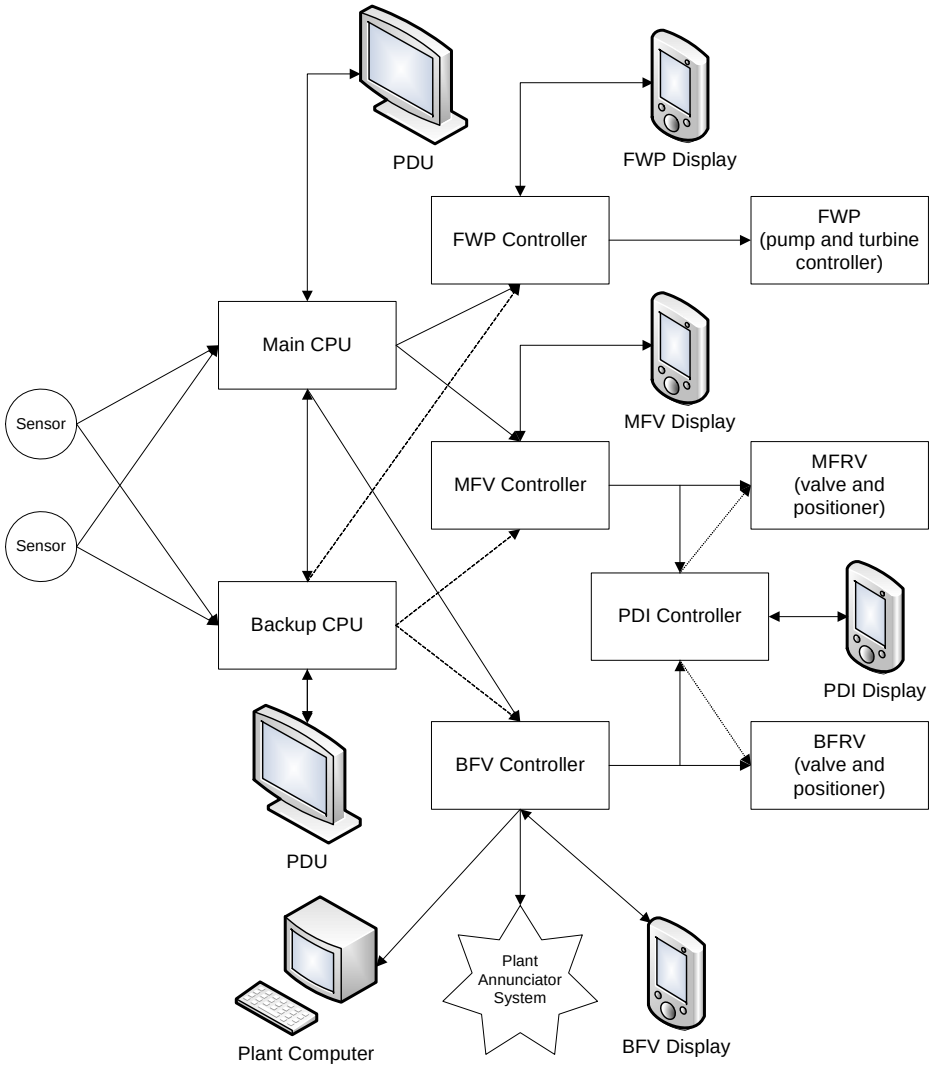


Figure 4-8 Diagram of the DFWCS and the associated HSIs

An arrow indicates the passage of a signal from one component to another, for example, from a sensor to a CPU, or from a CPU to the MFV. We depicted some of the main signals between all of these components, but omitted many other signals for clarity. Dotted lines represent the signals from the Backup CPU because the controllers do not use them unless this backup CPU takes control.

The DFWCS includes logic that monitors redundant input parameters for possible CPU input/output module failures or field transmitter failures that might have occurred. When they do, the system notifies the operators and minimizes process perturbations. The logic consists primarily of deviation checks, out-of- range checks on redundant input parameters, and rate of change checks. The subsequent actions depend upon the potential severity of the input failure modes, and are tailored to the actual configuration of the plant's field transmitter.

Table 4-5 presents the relationship between the main components of the DFWCS and the I&C subsystems of the process.

Table 4-5 I&C Subsystems of the DFWCS

DFWCS Components	I&C Subsystem
Sensors	Sensor
PDUs (one for each CPU, main and backup)	Monitoring, Automation and Control
MFV, BFV, FWP, and PDI controllers	Automation and Control, Communications

Figure 4-9 illustrates the system's HSI devices. Each CPU (main and backup) has a plasma display unit (PDU) in the main control room (MCR). Each PDU acts as an input/output terminal for its CPU, and is updated dynamically. The PDUs have an automatic screen-saver mode that blanks the screen when no data have been entered for approximately 10 minutes; that is, no-one has changed displays or input information. Touching the screen restores the display. To prevent inadvertent data-entry, the display must be completely visible before anything can be input. Alarm-status indications are displayed when an operator selects them, or when a deviation alarm occurs while the display is in screen-saver mode.

Each controller has a small panel display in the MCR near to the other feedwater- system's information and controls. The display of the steam-generator feedwater regulating valve controller (MFV) indicates the system's status, including output demands, as well as Auto/Manual (A/M) switches and increase/decrease pushbuttons for taking manual control. Secondary functions include monitoring- and logic-functions for auctioneering the main- and backup-CPUs, event timers, and signal deviation logic. The display offers two modes of operating an MFV controller:

- Manual mode ("M" button pushed). This allows operation of the feedwater regulating valve. Usually, this mode is used when there is a problem with the DFWCS.
- Automatic mode ("A" button pushed). This places the controller in Automatic mode so that it automatically processes the MFV's position-demand signal. It sends the signal to the feedwater-regulating valve to maintain the level of the S/G's set point. The controllers normally are operated automatically.

A section of the display indicates the set point in the controller, while another shows the actual S/G level.

The BFV controller is similar to the MFV controller. However, the former also sends data to the Plant Annunciator System and the Plant Computer (PC). For example, if the system detects that the failure of the main and backup CPUs, the Plant Annunciator alarms this condition. It also alerts the operators to several abnormal conditions in the system's operation. The PC informs the operators about the system's status under certain failure conditions.

Thus, the DFWCS HSI consists of four types of devices as shown in Table 4-6, along with their HSI process classification.

Table 4-6 HSIs of the DFWCS

HSI Device	Process HSI Classification
PDUs (one for each CPU, main and backup)	Controls
MFV, BFV, FWP, and PDI controller displays	Controls
Plant Annunciator System	Alarms
Plant Computer (PC)	Information System

4.4.2 Impact of Feedwater System Degradation on Human Performance

We chose the MFV controller for the detailed analysis because

- it controls the MFRV and failures in the position of this valve during power operation can lead to plant transients, including a reactor trip
- the HSI of the DFWCS informs the operators about the controller's status and the effects of failures of the controller

Our analysis assumed the following: (1) The plant is operating at full power, and, (2) the DFWCS is automatically controlling feedwater in the high-power mode. During this mode of operation, the BFV normally is closed, and the DFWCS controls the MFRV and FWP.

We evaluated the potential effects of the degraded I&C on human performance by postulating that a component the MFV controller had deteriorated, and propagated it through the HSI to determine its effects on human performance. The MFV controller is part of the "Automation and Control" subsystem. The following twenty-two degraded conditions of the MFV controller's input and output signals were analyzed,

1. Analog Input 0 (steam generator [S/G] level) fails to 0.0 *
2. Analog Input 1 (MFRV demand from the main CPU) fails to 0.0*
3. Analog Input 2 (MFRV demand from the backup [B/U] CPU) fails to 0.0
4. Analog Output 0 (output to the MFRV positioner, PDI controller, and other S/G) fails to 0.0
5. Analog Output 2 (S/G level set point output) fails to 0.0
6. Digital Input 0 (B/U CPU power fail or in test) fails open*
7. Digital Input 1 (B/U CPU Fail) fails open
8. Digital Input 2 (Main CPU power fail or in test) fails open
9. Digital Input 3 (Main CPU Fail) fails open*
10. Digital Input 0 (B/U CPU power fail or in test) fails closed
11. Digital Input 1 (B/U CPU Fail) fails closed
12. Digital Input 2 (Main CPU power fail or in test) fails closed
13. Digital Input 3 (Main CPU Fail) fails closed
14. Digital Output 0 (A/M status to the Main CPU) fails open
15. Digital Output 1 (A/M status to the B/U CPU) fails open
16. Digital Output 2 (B/U CPU failed status to CPUs) fails open
17. Digital Output 3 (Main CPU failed status to CPUs) fails open
18. Digital Output 0 (A/M status to the Main CPU) fails closed
19. Digital Output 1 (A/M status to the B/U CPU) fails closed
20. Digital Output 2 (B/U CPU failed status to CPUs) fails closed
21. Digital Output 3 (Main CPU failed status to CPUs) fails closed
22. Loss of power to the controller.*

These degradations of the MFV were the failure mode identified in the DFWCS's FMEA. Five of degraded conditions, denoted by asterisks, caused the loss of automatic control of the MFV controller, necessitating manual control.

We summarize our main insights gained from the analysis next. The Appendix to this report details the potential effect of each degraded condition on HSIs and human performance.

We deemed seventeen of the degraded conditions as latent failures because they do not cause loss of automatic control of the system, but lower its functionality to some extent. If other degraded conditions occur and/or the operators make a mistake(s) after a latent failure, the outcome can range from negligible to severe. In eight out of these seventeen degraded conditions, the MCR gives no indication that the degraded condition exists.

In fourteen of the degraded conditions, one or more of the HSIs give some indication that a failure occurred. Sometimes, the HSI only informs the operators that there was a failure, but did not specify the condition. Operators generally would need technical support from maintenance personnel to troubleshoot the specific cause of the failure. One interesting case is the failure mode "Analog Input 0 Fails to 0.0." The analog input 0 signal provides the S/G level to the MFV controller. The information is displayed to the operators, but the controller does not use it for any calculations or decisions. Accordingly, this failure mode does not directly affect the system's operation. However, the displayed S/G level will be (incorrectly) low, and may mislead operators to take erroneous actions to increase the S/G level, e.g., increasing the flow of feedwater to the S/G. This can lead to a high S/G level, and should the high-level set point be reached, the reactor will be tripped. The likelihood of this trip is low because the operators would have other information that they could use to determine that this level is wrong.

As noted above, five of the degraded conditions, as identified in our list above (#s 1,2,6,9,and 22) cause a loss of automatic control of the MFV (part of the Automation and Control subsystem) that requires operators to take manual control of the system. The failure to do so may entail a reactor trip due to an incorrect S/G level. In these five cases, the operators have available information about the degraded condition, but it is not annunciated (alarmed). Hence, some time may elapse before they become aware that a failure happened, potentially allowing the problem to worsen. A reactor trip entails a transient that challenges the operators, and potentially, the safety systems. Should some components or trains be unavailable at the time of the trip, the transient may evolve into a serious safety challenge, e.g., the accident at Three Mile Island Unit 2 in1979 started with a reactor trip with a loss of feedwater. Table 4-7 lists the five conditions involving loss of automatic control, the impacted HSI, and their human-performance implications.

Table 4-7 Degraded MFV Conditions Resulting in Loss of Automatic Control of the MFRV

Degradation Condition	Human-System Interface	Human Performance
Analog Input 1 (Valve demand from the main CPU) fails to 0.0	Controls and Information Systems	The operators have to take manual control of the MFRV using the PDI controller. Information about the condition is available (in the MFV controller and PC), but is not annunciated.
Analog Output 0 (output to the MFRV, PDI, and other S/G) fails to 0.0	Controls	The operators have to take manual control of the MFRV using the PDI controller. Information about the condition is available (in the PDI controller), but is not annunciated.
Digital Output 0 (A/M status to the Main CPU) fails open	Controls and Information Systems	The operators have to take manual control of the MFRV using the MFV controller. Information about the condition is available (in the PDU of the Main CPU and PC), but is not annunciated.
Digital Output 3 (Main CPU failed status to CPUs) fails closed	Controls and Information Systems	The operators have to take manual control of the MFRV using the MFV controller. Information about the condition is available (in the PDU of the Main CPU, MFV controller, and PC), but is not annunciated.
Loss of power to the controller	Controls and Information Systems	The operators have to take manual control of the MFRV using the PDI controller. Information about the condition is available (loss of display of the MFV controller, and the PC), but is not annunciated.

In Sections 4.2.1 and 4.3.3, we discussed strategies that might be adopted to minimize the potential impact of degraded sensor and monitoring subsystems on the operator's performance in monitoring the I&C system and detecting degraded conditions. One strategy was by improving the HSIs. Evaluating a portion of the digital feedwater control system gave us some insights into the possible effect of the I&C system's degradation on operator that supports this recommendation:

- Indications are needed to support operator awareness of degraded components within complex systems, such as the digital feedwater control system. We found that 8 of 17 degraded conditions in it are not communicated to the control room.
- Five of the degraded digital I&C conditions cause the loss of automatic control. Therefore, an alarm should alert the operator of the automatic-manual status of the system.

In addition, in Section 4.2.1, we suggested another such strategy would be to assess the outcome of I&C failures on the HSIs. Our consideration of the digital feedwater system supports this recommendation. Extending the designer's dissection of failure modes and effects to include how failure modes are processed through the HSI might identify the potential impacts of the HSI and human performance that could be incorporated in system design.

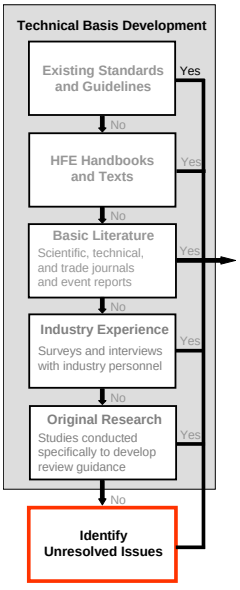
4.4.3 Summary

Our analysis of selected failure modes in a digital feedwater system revealed the following:

- Sensor failures can mislead operators about the plant's state. The problem is more complex when the control system uses different information than the operators, and, while responding appropriately to the situation, may appear to be malfunctioning to operators in view of their information and understanding of the situation. Further, operators may take inappropriate actions based in the erroneous information.
- Important degradation of the digital system may not be alarmed nor communicated to operators in a timely way. This can cause a delayed response, and possibly none at all.
- Degraded conditions may not affect the system's functionality and may not be communicated to the operators. This might create latent failures and subsequently more serious events should there be new failures or certain changes in conditions.
- Loss of automatic control places demands on operators, and can lead to significant transients, such as a reactor trip.

In addition, our analysis illustrates a method to assess the potential impacts on human performance from the degradation of the system's components by extending the analysis of failure modes and effects to cover how the HS1s process each failure mode. We uncovered weaknesses in the HSIs and offered opportunities for improvements.

4.5 Future Research Topics



The development of a technical basis for developing guidance often leads to the identification of unresolved issues (Figure 2-4). We suggest that these issues could be addressed by the following research topics. In the context of research on the effects of degraded I&C conditions on human performance, these topics take on added significance because of the limitations in the technical basis, as we discussed.

A set of research topics is presented below:[8]

- Identification of the Lessons Learned from Operating Experience on the Effects of Digital I&C Degradations on Personnel Performance
- Analysis Methods to Identify HFE-Significant I&C Degradations
- Generalization of the Findings on the Effects of Sensor Degradations on Performance to Our Target Context
- Effects of Sensor Degradations on Different Information Sources
- Effects of Sensor Degradations on Different Types of Display Formats
- Assessment of the Degradations of Other I&C Subsystems on Performance
- More Fine-Grained I&C System Characterization

[8] We made no recommendations for future research concerning degraded automation because they were published elsewhere (O'Hara & Higgins, 2010).

- Backup Systems for I&C and HSI Failures
- I&C System Degradation on Maintenance

Identification of the Lessons Learned from Operating Experience on the Effects of Digital I&C Degradations on Personnel Performance

There is little readily available operating experience for digital I&C and computer-based HSIs (O'Hara et al., 2008a; 2008b; Wood et al., 2004). We earlier identified this lack as a top-priority issue in *Operating Experience and Lessons Learned* (O'Hara et al., 2008a; 2008b). Thus, we recommend undertaking more research specifically to obtain this information, and to develop lessons learned from operating experience that learned provide a good foundation for formulating review guidance.

Analysis Methods to Identify HFE-Significant I&C Degradations

We noted the importance of identifying HFE-significant I&C degradations; i.e., the failure modes and degraded conditions of the I&C system that potentially might affect HSIs used by personnel in carrying out risk-important tasks. We also noted several methods for conducting such analyses, including HRA, FMEA, confusion matrix analysis, and misdiagnosis tree analysis. Additional research is needed to identify additional methodologies and undertake comparisons to highlight the strengths and weakness of each.

Generalization of the Findings on the Effects of Sensor Degradations on Performance to Our Target Context

As discussed in Section 4.2.1, the generalizability of the findings on the effects of I&C degradations on performance to our target context must established. Most findings came from studies wherein college students performed simplified operational tasks, using limited HSIs, in systems with very simplified I&C systems. Thus, we need to verify that the finding can be extended to more realistic sensor degradations, professional operators, nuclear power systems, and control room HSIs.

Effects of Sensor Degradations on Different Information Sources

Three types of information can be displayed on plant HSIs (Reising & Sanderson, 2002a)[9]:

- directly sensed
- derived information
- synthetic information

Directly sensed information is derived from a sensor measurement, e.g., the flow out of a tank based on a flow sensor in the output pipe (as illustrated in Figure 4-1). Derived information is displayed information that *could be* based directly on sensor measurement, but instead is derived from the measurements of other sensors. For example, in Figure 4-1, the flow into a tank might not be directly sensed, and instead, might be assessed from a change in level over time. This approach might be adopted to minimize the number of sensors in the system.

[9] Reising and Sanderson (2002a) distinguished between types of information, but did not label them. We used the labels "directly sensed," "derived information," and "synthetic information" in this report for convenience.

Synthetic information represents higher order information about a plant that cannot be sensed directly, but is derived mathematically from data gained from sensors, e.g., rate of change, and mass balance. Any such data used in these calculations from degraded or faulty sensors may propagate to the synthetic variable, and distort its meaning.

Although NUREG-0700 distinguishes the first two categories, the latter two have not been differentiated. The effects of sensor degradations and of an operator's ability to detect them may rest upon which of these three sources are involved.

Effects of Sensor Degradations on Different Types of Display Formats

The research discussed in this Section examined the effects of sensor degradations on two types of displays: Separable ones (showing individual parameters), and configural ones (wherein the information's dimensions uniquely are represented, while new emergent properties are created from interactions between the dimensions). The graphic displays discussed in Section 4.2.1 were the latter. However, the effects of sensor degradations on integral displays have not been studied. These displays depict the integration of information such that the individual parameters used to generate the display are not represented explicitly. Thus, integral displays may be more vulnerable than separable ones to sensor degradations since the raw data are not displayed (although, in most cases operators, will have access to it).

Assessment of the Degradations of Other I&C Subsystems on Performance

As we have discussed throughout this report, the studies on the effects of I&C degradations mainly are limited to the sensor subsystem and automation. Details of their effects on the other I&C subsystems in our characterization are required to support the development of review guidance. Such analyses will be supported by addressing the next topic.

More Fine-Grained I&C System Characterization

We used a simplified generic characterization of the I&C system. Future research might address more fine-grained one, supported by a comprehensive listing of the degradations and failures of digital systems.

Backup Systems for I&C and HSI Failures

Presently, the issue of backup systems for failed aspects of I&C systems and HSIs is treated piecemeal, e.g., the minimum inventory for complete digital-system failure and backup for loss of CBPs. A more systematic, comprehensive approach is needed that addresses all HFE-significant I&C degradations and HSI degradations.

I&C System Degradation on Maintenance

The scope of this research was limited to control room operations. However, maintaining digital systems also is a very significant consideration as well (O'Hara et al., 1996). Research is needed to address the relationship of maintenance and digital I&C system degradation.

4.6 Conclusions

To evaluate the effects of I&C degradations on HSIs and operator performance, we reviewed empirical research and operating experience. In addition, we analyzed selected failure modes of the digital feedwater system of a PWR. We distinguished significant effects in each of these three types of data. I&C degradations were prevalent in plants employing digital systems, and the overall effects on plant behavior can be significant, such as causing a reactor trip or causing equipment to operate unexpectedly.

We found effects on operator performance for degradations of each I&C subsystem. Examples include

- poor situation awareness due to deterioration of the sensor and monitoring subsystems
- poor situation awareness and response planning on the loss of automatic systems
- unstable control and errors in performance due to delays in the communication subsystem
- effects on teamwork and shifts in the concept of operations due to loss of computer-based HSIs

We also found that plant designs may not consider the effect of I&C degradation on the operation of the plant and the performance of personnel to the extent they probably should. Important degradations may not be alarmed, and operators may have insufficient information at their HSIs, in procedures, and in training to deal with them.

The paucity of available information limits the strength of these findings. As we noted in Section 4.1, few studies specifically examined the effects of degraded I&C systems on the operator's performance. Those available have methodological issues that restrict generalizing their results to real-world complex system operations. Similarly, in Section 4.2 we noted the dearth of information on operating experience pertaining to digital I&C degradations. Additional research, such as the study described in Section 4.3, can help shed light these effects.

5 DISCUSSION

New and advanced reactors will install integrated digital I&C systems to support operators in monitoring and controlling the plant. Even though digital systems typically are highly reliable, their potential for degradation or failure could greatly affect the operator's performance and, consequently, impact plant safety. In this research project, we investigated the effects on human performance and plant operations of degraded I&C systems. Our objective was to develop HFE review guidance addressing the detection and management of such conditions by plant operators.

Accordingly, we reviewed information on the effects of degraded I&C systems on the performance of HSIs and operators. We characterized the I&C system under four subsystems: Sensor, Monitoring, Automation and Control, and Communications. Our technical basis included strategies and approaches for addressing the identified effects. Specifically, we reviewed pertinent standards and guidelines, empirical studies, and plant-operating experiences. In addition, we evaluated the potential effects of selected failure modes of the digital feedwater system on the HSIs and operator performance.

Among our more important findings was the paucity of information available pertaining to our objectives. Few studies specifically assessed the effects of various types of I&C degradations on HSIs and human performance; most research that was undertaken focused on sensor issues and automation. While operating experience on degraded digital I&C systems certainly exists, very little is applicable to our needs.

Acknowledging this caveat, the results indicated that I&C degradations are prevalent in plants employing digital systems, and the overall effects on the plant's behavior can be significant, such as causing a reactor trip or equipment to operate unexpectedly. These degradations can impact the HSIs that operators use to monitor and control the plant. Examples of these effects include

- poor situation awareness due to degradations of the sensor and monitoring subsystems
- poor situation awareness and response planning on degradations of automatic systems
- teamwork effects and shifts in the concept of operations due to loss of automation support from the computer-based HSIs
- control instability reflecting delays in the communication subsystem

One specific example we discussed was related to sensor degradations. They make displays difficult to interpret and sometimes mislead operators by making it appear that a process disturbance has occurred.

We also found that plant designs may not consider the effect of I&C degradation on the operation of the plant and its operators to the extent they probably should. Important degradations may not be alarmed and operators may not have sufficient information at their HSIs, in procedures, and from training to deal with them.

We identified two primary strategies for addressing the human performance issues. One strategy is to analyze the potential impact of I&C failures on HSIs as part of the design process that will aid in identifying HFE-significant I&C degradations. One example is extending the analyses of failure modes and effects to encompass an evaluation of how the HSIs process failure modes, and to

detail potential impacts on human performance that can be addressed in system design. The second strategy is to improve the HSIs so that they better support operators in monitoring the I&C system and in detecting and managing degraded conditions.

We used the technical basis to develop HFE review guidance that addresses the treatment of degraded I&C conditions in HFE programs. The guidelines from this project can be integrated into NUREG-0711 and NUREG-0700 to offer NRC staff updated review guidance to help ensure that applicants address degraded I&C conditions in their design process, and that HSIs support the operators who manage them. Given the limited basis, as noted above, the guidance is fairly high-level and does not individually address all of the I&C subsystems.

Our findings fully support the NRC's and industry's assessment of degraded I&C as a priority topic. Therefore, we consider that additional research is warranted to better understand the effects of degraded conditions on HSIs and the operator's performance. We identified several topics for future research:

- Identification of the Lessons Learned from Operating Experience on the Effects of Digital I&C Degradations on Personnel Performance
- Analysis Methods to Identify HFE-Significant I&C Degradations
- Generalization of the Findings on the Effects of Sensor Degradations on Performance to Our Target Context
- Effects of Sensor Degradations on Different Information Sources
- Effects of Sensor Degradations on Different Types of Display Formats
- Assessment of the Degradations of Other I&C Subsystems on Performance
- More Fine-Grained I&C System Characterization
- Backup Systems for I&C and HSI Failures
- I&C System Degradation on Maintenance

We believe the findings from studies addressing these topics greatly will enhance the technical basis of information available, and support the development of further HFE guidance on this important topic.

6 REFERENCES

ANSI/IEEE (1987). *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems* (ANSI/IEEE Std. 352-1987). New York, NY: Institute of Electrical and Electronics Engineers.

Beare, A., Gaddy, C., Parry, G. & Singh, A. (1991). An Approach for Assessment of the Reliability of Cognitive Response for Nuclear Power Plant Operating Crews. In G. Apostolakis (Ed.) *Probabilistic Safety Assessment & Management (PSAM)*, New York: Elsevier Science.

Bennett, K. (1992). Representation aiding: Complementary decision support for a complex, dynamic control task. *Control Systems*, 19-24.

Bennett, K. & Flach, J. (1992). Graphical displays: Implications for divided attention, focused attention, and problem solving. *Human Factors*, *34*, 513-533.

Bennett, K., Nagy, A., & Flach, J. (1997). Visual displays. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (Second Edition). New York, NY: John Wiley and Sons.

Bennett, K., Toms, M. & Woods, D. (1993). Emergent features and graphical elements: Designing more effective configural displays. *Human Factors*, *35*, 71-97.

Brill, R. (2000). *Instrumentation and Control Digital System Failures in Nuclear Power Plants (From LER Data*); NRC.

Burns, C. & Hajdukiewicz, J. (2004). *Ecological Interface Design*. Boca Raton, FL: CRC Press, Taylor & Francis.

Burns, C., Skraaning, Jr., G., Jamieson, G., Lau, N., Kwok, J., Welch, R. & Andresen, G. (2008). Evaluation of ecological interface design for nuclear process control: Situation awareness effects. *Human Factors*, *50*, 663–679.

Buttigieg, M., Sanderson, P., & Flach, J. (1988). Object vs. separate displays for process failure detection: The emergent features approach. In *Proceedings of the Human Factors Society 32nd Annual Meeting*. Santa Monica, CA: Human Factors Society.

Carruth, R. & Sotos, W. (1996). Design concepts for the reactor protection and control process instrumentation digital upgrade project at the Donald C. Cook nuclear plant units 1 and 2. *IEEE Transactions on Nuclear Science*, *43*, 1899-1902.

Chu, T., Martinez-Guridi, G., Yue, M., Lehner, J. & Samanta, P. (2008). *Traditional Probabilistic Risk Assessment Methods for Digital Systems* (NUREG/CR-6962). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Dudenhoeffer, D., Hallbert, B, Miller, D., Quinn, T., Arndt, S., Bond, L., O'Hara, J., Garcia, H., Holcomb, D., Wood, R. & Naser, J. (2007). *Technology Roadmap: Instrumentation, Control, and Human Machine Interface to Support DOE Advanced Nuclear Power Plant Programs* (INL/EXT-06-11862). Washington, DC: Department of Energy.

EPRI (2002). *Guideline on Licensing Digital Upgrades* (EPRI TR-102348). Palo Alto: CA: Electric Power Research Institute.

Flach, J. (1989). An ecological alternative to egg-sucking. *Human Factors Society Bulletin*, *32 (9)*, 4-6.

Flach, J. (1990). The ecology of human-machine systems: Introduction. *Ecological Psychology*, *2*, 191-205.

Flach, J. & Bennett, K. (1992). Graphical interfaces to complex systems: Separating the wheat from the chaff. In *Proceedings of the Human Factors Society 36th Annual Meeting*. Santa Monica, CA: Human Factors Society.

Flach, J. & Hancock, P. (1992). An ecological approach to human-machine systems. In *Proceedings of the Human Factors Society 36th Annual Meeting*. Santa Monica, CA: Human Factors Society.

Galletti, G. (1996). Human factors issues in digital system design and implementation. In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*. La Grange Park, IL: American Nuclear Society.

Gibson, J. (1979). *The ecological approach to visual perception*. Boston, MA: Houghton Mifflin, Co.

Hayes, T & Kisalu, J. (2005). I&C for AP 1000. *Nuclear Engineering International Journal*; February 2005 Issue, pages 36-41.

Holcomb, D. & Wood, R., (2006). Challenges for Instrumentation, Controls, and Human-Machine Interface Technologies. *Nuclear News,* Volume 49, Number 13, Pages 31-36.

Huey, B. & Wickens, C. (1993). *Workload Transition: Implications for Individual and Team Performance*. Washington, D.C.: National Academy Press.

IAEA (1999). *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook* (IAEA Technical Report 387). Vienna, Austria: International Atomic Energy Agency.

IEEE (2004). *IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities* (IEEE Std. 1023-2004). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2003). *IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations* (IEEE Std. 7-4.3.2-2003). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2002). *IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations* (IEEE Std. 497-2002). New York, NY: Institute of Electrical and Electronics Engineers. New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (2000). *IEEE Standard Application to the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems* (IEEE Std. 379-2000). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (1998). *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* (IEEE Std. 603-1998). New York, NY: Institute of Electrical and Electronics Engineers.

IEEE (1990). *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries* (IEEE Std. 610). New York, NY: Institute of Electrical and Electronics Engineers.

INPO (2005). *Review of Circuit Card/Board Related Failures that Contributed to Automatic and Manual Scrams* (Topical Report TR5-43). Atlanta, GA: Institute of Nuclear Power Operations.

Jamieson, G., Miller, C., Ho, W. & Vicente, V. (2007a). Ecological interface design for petrochemical process control: An empirical assessment. *IEEE Transactions on Systems, Man, Cybernetics*, *37*, 906–905-920.

Jamieson, G., Miller, C., Ho, W. & Vicente, V. (2007b). Integrating task- and work domain-based work analyses in ecological interface design: A process control case study. *IEEE Transactions on Systems, Man, Cybernetics*, *37*, 887–905.

Kahneman, D. & Triesman, A. (1984). Changing views of attention and automaticity. In R. Parasuraman and R. Davies (Eds.), *Varieties of Attention*. New York, NY: Academic Press.

Kemeny, J. (1979). *Report of the President's Commission on the Accident at Three Mile Island*. Springfield, VA: National Technical Information Services.

Kim, J, Jung, W, & Park, J. (2005). A systematic approach to analysing errors of commission from diagnosis failure in accident progression. *Reliability Engineering and System Safety, 89*, 137–50.

Kim, J, Jung, W, & Son, Y. (2008). The MDTA-based method for assessing diagnosis failures and their impacts in nuclear power plants. *Reliability Engineering and System Safety, 93*, 337–349.

Kim, M. & Seong, P. (2006). A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety, 91*, 580–593.

Kim, M. & Seong, P. (2008). A method for identifying instrument faults in nuclear power plants possibly leading to wrong situation assessment. *Reliability Engineering and System Safety, 93*, 316–324.

Kisner, R. *et al*. (2007). *Technical Review Guidance and Acceptance for Digital Communications and Workstations in Highly Integrated Control Rooms* (Draft NUREG/CR). Washington, D.C.: U.S. NRC.

Lau, N., Veland, Ø., Kwok, J., Jamieson, G., Burns C., Braseth A. & Welch R. (2008a). "Ecological interface design in the nuclear domain: An application to the secondary subsystems of a boiling water reactor plant simulator. *IEEE Transactions on Nuclear Science*, *55*, 3579-3596.

Lau, N., Jamieson, G., Skraaning, Jr., G. & Burns, C. (2008b). Ecological Interface Design in the Nuclear Domain: An Empirical Evaluation of Ecological Displays for the Secondary Subsystems of a Boiling Water Reactor Plant Simulator. *IEEE Transactions on Nuclear Science*, *55*, 3597-3610.

Lee, J. (2006). Human Factors and Ergonomics in Automation Design. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (3rd Ed.). New York, NY: John Wiley & Sons, Inc.

Lee, J. & See, K. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors,* 46 (1), 50-80

Liu, Q. Nakata K. & Furuta K. (2002).Display Design of Process Systems Based on Functional Modeling. *Cognition, Technology & Work*, *4*, 48–63.

Lorenzo, D. (1990). *A manager's guide to reducing human errors: Improving human performance in the chemical industry*. Washington, DC: Chemical Manufacturers Association.

Moray, N., Jones, B., Rasmussen, J., Lee, J., Vicente, K., Brock, R. & Djemil, T. (1993). *A performance indicator of the effectiveness of human-machine interfaces for nuclear power plants* (NUREG/CR-5977). Washington, DC: U.S. Nuclear Regulatory Commission.

Moray, N., Lee, J., Vicente, K., Jones, B., & Rasmussen, J. (1994). A direct perception interface for nuclear power plants. In *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Neisser, U. (1967). *Cognitive Psychology*. New York, NY: Appleton-Century Crofts.

NRC (2009). *Digital I&C; Highly-integrated Control Rooms-Communications Issues* (HICRc) (DI&C-ISG-04, ML083310185); Rev. 1, 3/6/09; Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2008a). *Main Feedwater System Issues and Related 2007 Reactor Trip Data* (Information Notice 2008-13, 7/30/08). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2008b). Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF): Interim Staff Guidance (DI&C-ISG-05, ML082740440). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2008c). *Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments: Interim Staff Guidance* (DI&C-ISG-03, ML080570048) Revision 0, 8/11/08, Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007a). *Standard Review Plan* (NUREG-0800), Chapter 18, Human Factors Engineering. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007b). *Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations* (Information Notice 2007-15, 4/17/07). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007c) *Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety Related Computer-based I&C Systems in Nuclear Power Plants*. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007d). *Standard Review Plan* (NUREG-0800); Chapter 8, Branch Technical Position 8.5 - Supplemental Guidance for Bypass and Inoperable Status Indication for Engineered Safety Features Systems, Revision 3. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2006a). *Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants* (Regulatory Guide 1.97, Revision 4). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2006b). *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Revision 2* (Regulatory Guide 1.152). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2001). *Review of TRICONEX Corporation Topical Reports 7286-545 and 7286-546* (Revision 1, TAC No. MA 8283). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2000). *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)* (NUREG-1624, Rev. 1). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (1981). *Report on Millstone Unit 2 Loss of 125V DC Bus Event on January 2, 1981* (AEOD/C104). Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (1973), *Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems* (Regulatory Guide 1.47). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J. (2004). Identifying and addressing lessons learned from plant modernization programs guidelines for control room modernization. *Nuclear Plant Journal*, 22 (2), 47-48.

O'Hara, J. (1994). *Advanced Human-system Interface Design Review Guideline* (NUREG/CR-5908). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J. & Brown, W. (2002). *The effects of interface management tasks on crew performance and safety in complex, computer-based systems*. (NUREG/CR-6690). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J., Brown, W., Lewis, P., & Persensky, J. (2002). *Human-system Interface Design Review Guidelines* (NUREG-0700, Rev 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara J. & Higgins, J. (2010). *Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis* (Technical Report BNL-91017-2010). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Higgins, J., Brown, W., O'Hara, J., Fink, R., Persensky, J., Lewis, P., Kramer, J., Szabo, A., & Boggi, M. (2008a). *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants* (NUREG/CR-6947). Washington, D.C.: U. S. Nuclear Regulatory Commission.

O'Hara, J., Higgins, J., Brown, W. & Fink, R. (2008b). *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants: Detailed Analyses* (BNL Technical Report No: 79947-2008). Upton, NY: Brookhaven National Laboratory.

O'Hara, J., Higgins, J. & Kramer, J. (2000). *Advanced information systems: Technical basis and human factors review guidance* (NUREG/CR-6633). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J., Higgins, J., Persensky, J., Lewis, P., & Bongarra, J. (2004). *Human factors engineering program review model* (NUREG-0711, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

O'Hara, J. & Roth, E. (2005). Operational Concepts, Teamwork, and Technology in Commercial Nuclear Power Stations. In C. Bowers, E. Salas, & F. Jentsch (Eds.) *Creating High-Tech Teams: Practical Guidance on Work Performance and Technology*. Washington, DC: American Psychological Association.

O'Hara, J., Stubler, W., & Higgins, J. (1996). Hybrid human-system interfaces: Human factors considerations (BNL Report J6012-T1-4/96). Upton, New York: Brookhaven National Laboratory.

O'Hara, J., Stubler, W., & Higgins, J. (1998). *The development of HFE design review guidance for hybrid human-system interfaces* (BNL Report J6012-T6-12/98). Upton, New York: Brookhaven National Laboratory.

O'Hara, J., Stubler, W., Higgins, J., & Kramer, J. (2000). Hybrid Human-System Interfaces: Trends and Challenges. In *Proceedings of the Third American Nuclear Society International Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies*. La Grange Park, Illinois: American Nuclear Society, Inc.

O'Hara, J., Stubler, W, & Kramer, J. (2000). Soft controls: Designing for error tolerance. In *Proceedings of the Third American Nuclear Society International Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*. La Grange Park, Illinois: American Nuclear Society, Inc.

Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, *39* (2), 230-253.

Portman, F. & Lipner, M. (2002). Computerised procedures and parallel information to guide the operator. *Modern Power Systems.* available online at: http://www.modernpowersystems.com/storyprint.asp?sc=2014631

Reising, D. & Sanderson, P. (2000).Testing the impact of instrument location and reliability on ecological interface design: Fault diagnosis performance. In *Proceedings of the IEA 2000/HFES 2000 Congress.* Santa Monica, CA: Human Factors and Ergonomics Society.

Reising, D. & Sanderson, P. (2002a). Work domain analysis and sensors I: Principles and simple example. *International Journal of Human-Computer Studies*, *56*, 569- 596.

Reising, D. & Sanderson, P. (2002b). Work domain analysis and sensors II: Pasteurizer II case study. *International Journal of Human-Computer Studies*, *56*, 597-637.

Reising, D. & Sanderson, P. (2004). Minimal instrumentation may compromise failure diagnosis with an ecological interface. *Human Factors*, *46*, 316-333.

Roth, E., Hanson, M., Hopkins, C., Mancuso, V. & Zacharias, G. (2004). Human in the Loop Evaluation of a Mixed-initiative System for Planning and Control of Multiple UAV Teams. In *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting.* Santa Monica, CA: Human Factors and Ergonomics Society.

Rook, F. & McDonnell, M. (1993). Human Cognition and the Expert System Interface: Mental Models and Inference Explanations. *IEEE Transactions on Systems, Man, and Cybernetics. 23* (6), 1649-1661.

Roth, E., Mumaw, R. & Lewis, P. (1994). *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies* (NUREG/CR-6208). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Roth, E. & O'Hara, J. (2002). *Integrating digital and conventional human system interface technology: Lessons learned from a control room modernization program*. (NUREG/CR-6749). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Roth, E. & O'Hara, J. (1999). Exploring the impact of advanced alarms, displays, and computerized procedures on teams. In *Proceedings of the Human Factors and Ergonomics Society - 43rd Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Smith, P., Bennett, K. & Stone, R. (2006). Representation aiding to support performance on problem-solving tasks. R. Williges (Ed.). *Reviews of Human Factors and Ergonomics, Vol. 2*. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O. (2006). Impact of Sensor Noise magnitude on Emergent Features of Ecological Interface Designs. *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O., & Vicente, K. (2005). Sensor Noise and Ecological Interface Design: Effects of increasing noise magnitude on operators' performance. *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

St-Cyr, O., & Vicente, K. (2004). Sensor Noise and Ecological Interface Design: Effects on operators' Control performance. *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.

Stubler, W., O'Hara, J., & Kramer, J. (2000). *Soft controls: Technical basis and human factors review guidance* (NUREG/CR-6635). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Vicente, K. (2002). Ecological Interface Design: Progress and Challenges. *Human Factors, 44,* 62-78.

Torok, R. (2008). *U.S. Commercial Nuclear Power Plant Digital I&C System Operating Experience*. Palo Alto, CA: Electric Power Research Institute (EPRI).

Torok, R., Naser, J., Sandell, L. & Harris T. (2006). I&C Issues for New Nuclear Plant Deployment. *Proceeding of the 16th Annual Joint POWID/EPRI Controls and Instrumentation Conference 49th Annual ISA POWID Symposium*. Research Triangle Park, NC: International Society of Automation (ISA).

Vicente, K. (1999) *Cognitive work analysis*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Vicente, K., Moray, N., Lee, J., Rasmussen, J., Jones, B., Brock, R. & Djemil, T. (1996). Evaluation of a Rankine cycle display for nuclear power plant monitoring and diagnosis. *Human Factors*, *38*, 506-521.

Vicente, K. & Rasmussen, J. (1992). Ecological interface design: Theoretical foundations. *IEEE Transactions on Systems, Man, and Cybernetics*, *2*, 589-606.

Vicente, K. & Rasmussen, J. (1990). The ecology of human-machine systems II: Mediating 'direct perception' in complex work domains. *Ecological Psychology*, *2(3)*, 207-249.

Waterman, M. (2006). Unpublished data-base of digital I&C failures from 1987-2006; NRC.

Wickens, C. (1986). The effects of control dynamics on performance. In K. Boff, L. Kaufman, and J. Thomas (Eds.), *Handbook of perception and human performance*. New York: Wiley.

Wickens, C. (1984). *Engineering psychology and human performance*. Columbus, OH: Merrill Publishing Company.

Wickens, C. & Carswell, C. (1995). The proximity compatibility principle: Its psychological foundation and relevance to display design. *Human Factors*, *37*, 473-494.

Wickens, C. & Hollands J. (2000). *Engineering Psychology and Human Performance* (3rd ed). Upper Saddle River, NJ: Prentice-Hall Inc.

Wickens, C., Lee, J., Liu, Y., Gordon, S. (2004). *Human Factors Engineering* (2nd Edition). Upper Saddle River, NJ: Prentice Hall.

Willems, B. & Heiney M. (2002). *Decision Support Automation Research in the En Route Air Traffic Control Environment* (DOT/FAA/CT-TN02/10). Washington, DC.: Federal Aviation Administration.

Wood, R., Easter, J., Korsah, W. & Remley, G. (2004). Advance Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants (NUREG/CR-6842). Washington, D.C.: U.S. Nuclear Regulatory Commission

Woods, D. & Roth, E. (1988). Cognitive systems engineering. In M. Helander (Ed.), *Handbook of human-computer interaction*. New York, NY: North-Holland.

Woods, D., Wise, J., & Hanes, L. (1981). An evaluation of nuclear power plant safety parameter display systems. In *Proceedings of the Human Factors Society 25th Annual Meeting*. Santa Monica, CA: Human Factors Society.

Wu, Q., Wang, Z., & Wang, Z. (2006). Experiments on Stewart platform teleoperation with predictor display. In *Sixth International Symposium on Instrumentation and Control Technology: Sensors, Automatic Measurement, Control, and Computer Simulatio*n, Bellingham, Washington: SPIE.

Xiong, Y., Li, S., & Xie, M. (2006). Predictive display and interaction of telerobots based on augmented reality. *Robotica*, *24* (4), 447-453.

Part 2:

HFE Guidelines for Reviewing The Effects of Degraded I&C Conditions on HSIs' and Operators' Performance

7 DESIGN PROCESS REVIEW GUIDELINES

This section contains guidance for reviewing how an applicant's HFE program addresses degradations of the I&C system. Each individual guideline contains a review criterion, followed a brief summary of the literature. Related guidance from NUREG-0711 and NUREG-0700 is identified in the discussion sections. In most cases, the guidance offered below provides a more complete treatment of the topic by extending it from one limited aspect of the I&C system, such as the sensor subsystem, to the entire I&C system. The related industry standards also are identified.

1. Applicants should review operating experience to identify the effects of failure modes and degraded conditions of the HSI and I&C subsystem on personnel performance.

   Discussion: Thus, Review Criterion 4 in NUREG-0711, Section 3, Operating Experience Review, identifies topics to be included in the review and in interviews with plant personnel. They include instrument failures, including system logic and control units; HSI equipment and processing failures (e.g., loss of video display units or of data processing); and transients, such as a loss of power to selected buses or the control room's power supplies. This guideline generalizes the NUREG-0711 criterion to the entire I&C system.

   There is limited general knowledge from operating experience with digital I&C systems in the commercial nuclear industry, especially as that related to HSIs and personnel performance. Thus, applicants should proactively seek this information for I&C designs that are similar to their own, and use it as input to their HFE program.

2. Applicants should conduct analyses to identify HFE-significant I&C degradations; i.e., the failure modes and degraded conditions of the I&C system that potentially might affect the HSIs used by personnel in crying out their risk-important tasks.

   Discussion: There are three key points about this review guideline: (1) Analysis of the effects of I&C degradations on HSIs and personnel performance, (2) evaluation of degraded conditions in addition to complete failure, and (3) focusing the analysis on the impacts on operations. Each is discussed below.

   While applicants typically analyze the effect of I&C failure modes and degradations on key plant systems, they do not expand it routinely to HSIs and personnel performance.[10] For example, we found that extending a designer's failure modes and effects analysis to include how the failures impact the HSIs can identify potential human performance impacts that can be addressed in system design (Section 4.4). The ways in which resources, such as computer-based procedures and other HSIs, can degrade should be analyzed and understood fully so they can be dealt with in the HFE program to ensure personnel perform risk-important tasks correctly.

   Attention should be paid to degradations, not just complete failure. Complete failure, such as that of a computer-based procedures system, is easily recognized, and existing guidance already specifies the need for a backup system. More subtle degradations may be troublesome to discern, yet may affect the information provided by HSIs, and thus, personnel performance.

[10] For example, NUREG-0800, Section 7.7, states that the review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that are associated with digital systems, such as software design errors and random hardware failures.

There are very many HSIs in modern NPPs, so analyzing all of them may be impractical. Thus, evaluations may be applied in a graded fashion, by identifying the more important human actions and the HSIs most closely related to plant safety. Many lower-level digital I&C failures that occur do not impact I&C system functionality from an operations perspective; maintenance personnel resolve the as part of their normal activities. The key in this guideline is identifying those degradations that lower the ability of personnel to monitor, detect, and assess situations, plan responses, and implement responses associated with risk-important tasks. A degraded digital I&C system power supply is an example of an analysis that should be conducted because of the likelihood of impacting the HSI.

This guidance is a more complete treatment of NUREG-0700's guidance on the sensor subsystem. NUREG-0700, Appendix B.1, Review Guidelines for the Information Display Design Process, B.1.3, Human-System Interface Design, Criterion 6 - The effects of instrumentation failures on graphic displays should be analyzed. Potential failure problems should be evaluated in the context of the following questions:

- Can operators detect a failure of instrumentation?
- Can instrument failures result in representations that operators interpret as real process failures; perhaps more importantly, can such process failures be misinterpreted as instrument failures?
- If operators detect a failure, should use of the display be suspended?
- Since the display may integrate many parameters into a single visualization, what effect does its loss have on operations and how effectively can operators transition to backup displays?

This guidance is consistent with that in IEEE Std. 7-4.3.2-2003 (IEEE, 2003), specifying that a hazard analysis be undertaken to identify conditions that are not identified by the normal design review and testing process. "The hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems." Section D.4.2.3.2 states that fault tree analysis and failure modes and effects analyses are techniques that can be used to determine hazards. Section D.4.2.4.4 of this standard acknowledges that "the system-level impact of a hazard may be subtle, such as the display of an erroneous value that subsequently causes an operator to take an inappropriate action".

3. The applicant's PRA and HRA activities should determine the impact of HFE-significant I&C degradations on human error and plant risk.

Discussion: Recent approaches to HRA recognize the importance of the potential impact of sensor failure on the operator's situation assessment, and, in turn, the effect of incorrect ones on errors of commission (e.g. Kim, Jung, & Park, 2005; Kim, Jung, & Son, 2008; NRC, 2000). For example, the HRA approach called "A Technique for Human Event Analysis" (ATHEANA) recognized the importance of situation assessment on human action and error (NRC, 2000). Factors leading to faulty assessments are identified as part of the analysis, including sensor failures. This led to t efforts to predict errors of commission resulting from poor situational assessment. ATHEANA's HRA methods are useful in the current context in that they afford possible approaches to analyzing sensor degradations to identify those that might lead to incorrect situation assessments.

The analyses will support the applicant's efforts to address the staff's ISG on *Review of New Reactor Digital Instrumentation and Control Probabilistic Risk Assessments* (NRC, 2008c). The ISG notes that human errors associated with DI&C system failures have become more important contributors to CDF, and highlight several considerations that applicants should address in their PRAs:

- Evaluate the acceptability of how the failure of control room indication is modeled.

- Assess the acceptability of the recovery actions taken for loss of DI&C functions, referring to RG 1.200 and HRA Good Practices NUREGs for guidance. "If recovery actions are modeled, they should consider loss of instrumentation and the time available to complete such action.
- Assure that for self-testing and diagnostic features**,** the PRA accounts for the possibility that the system does not reconfigure itself after detecting a failure. Also, a diagnostic feature may not detect all of the failure modes, only those it was designed to discover. .
- If a communication network is shared, the effects on all systems due to failures of the network should be modeled jointly. "The impact of communication faults on the related components or systems should be evaluated."
- Interactions within a DI&C system should be considered (multi-tasking, multiplexing).

4. Applicants should analyze the impacts of HFE-significant I&C degradations to ensure that they are not displayed in HSIs in ways that personnel will confuse with other process disturbances.

   Discussion: One concern about I&C degradations, particularly of the sensor- and monitoring-subsystem, is that they can (1) render displays difficult to interpret; and, (2) perhaps worse, can make displays look as though a process disturbance has occurred. Analyses during the design process will help ensure that their effects are understood and the opportunity for misleading operators is minimized. The literature includes a variety of approaches to resolve this concern, including human reliability analysis (NRC, 2000), confusion matrices (Kim & Seong, 2008), and misdiagnosis tree analysis (Kim, Jung, & Park, 2005; Kim, Jung, & Son, 2008). Section 4.2.3 of this document briefly discusses these approaches.

   The analyses conducted for this guideline will support applicant's ability to address the guidance in the ISG on *Digital I&C; Highly-Integrated Control Rooms-Communications Issues* (NRC, 2009). Section 3.2, Human Factors Considerations, cites the potential for providing operators with obsolete or erroneous information r without advising them of potential inaccuracies. It states that applicant's should demonstrate that they have considered these kinds of issues.

   The guidance is also consistent with IEEE Std. 603-1998 (IEEE, 1998) and IEEE Std. 497-2002 (IEEE, 2002). IEEE Std. 603-1998 states, "The design of the information display system shall minimize the possibility of ambiguous indications that could be confusing to the operator" and IEEE Std. 497-2002, Section 6.5, Information Ambiguity, states "… the failure of an accident monitoring instrument channel shall not result in information ambiguity that could lead the operator to defeat or fail to accomplish a required safety-related function." "If analysis shows that credible failures can result in information ambiguity, a signal validation technique should be employed. If the signal validation process cannot be automatically accomplished, additional information shall be provided to allow the operators to deduce the actual conditions so that they may properly perform their role."

5. The applicant's task analysis should identify the task requirements for managing HFE-significant I&C degradations so that risk-important tasks can be performed.

   Discussion: Task analysis is the means by which the operator's task requirements for managing I&C degradations are identified. Those requirements are needed to define the features of the HSI design needed to support operators in monitoring and responding to such degradations.

   This guidance is an extension of NUREG-0711, Section 5, Task Analysis, Review Criterion 1 that identifies the scope of task analysis. It is also a more complete treatment of NUREG-0700's guidance for CBPs. NUREG-0700, Appendix B.3 - Review Guidelines for the Computer-based Procedure System Design Process, B.3.4 - Task Analysis, Criterion 3 states, "Tasks associated with CBP failure and

back-up should be identified to define the requirement for indicating malfunctions. The task of smoothly transitioning from CBPs to a back-up method (such as PBPs) also should be addressed."

6. Applicants should determine the alarms and the information personnel need to detect HFE-significant I&C degradations in a timely manner, and to identify the extent and significance of the condition.

   Discussion: This information is an essential input to designing HSIs that will be effective in supporting operators to detect and manage degraded conditions.

7. Applicants should determine the necessary back-up systems, if any, needed to ensure that risk-important tasks can be performed.

   Discussion: Depending on the extent of redundancy and diversity in the I&C systems involved and the type of support given to operators, backup systems may be necessary. For example, if there is a major loss of digital I&C, a backup may be needed to manage safety functions.

8. Applicants should determine the necessary compensatory actions and supporting procedures required to ensure that personnel effectively can manage the HFE-significant I&C degradation, and the transition to back-up systems.

   Discussion: Managing I&C degradations requires more than good HSIs. The actions to be taken must be analyzed, and the need for procedural support also determined to help operators to manage the condition.

9. Operator training programs should support personnel in

   - understanding how and why the I&C subsystems might degrade or fail
   - knowing the implications of such degradations for HSI and their own task performance
   - monitoring the I&C system's performance, so degradations are detected and recognized via the control room's HSIs
   - performing recovery actions and compensatory actions, perhaps using procedures, in the event of a degraded condition
   - smoothly transitioning to backup systems when needed
   - comprehending how the roles and responsibilities of crew members and the concept of operations will be impacted

   Discussion: Operator training plays an important role in supporting operators to detect automation degradations, and in understanding the types of degraded conditions that can occur (O'Hara & Higgins, 2008). A similar approach can be extended to the rest of the I&C system.

   For failures of automatic systems, learning from classroom- and on-the-job-training is enhanced by simulator training that specifically provides operators with experience of different failures (O'Hara & Higgins, 2008). We deem it likely the same type of training can help operators to recognize and manage degradation in other I&C subsystems. .

   This guidance also is a more thorough treatment of existing guidance in NUREG-0700 on information systems and CBPs:

- NUREG-0700, Appendix B.1, Review Guidelines for the Information Display Design Process, B.1.4Training Program Development, Criterion 2 - Operators should be trained on the relationship between the display form and the plant states it is intended to represent, including failure modes and their effect on graphical representation.
- NUREG-0700, Appendix B.3, Review Guidelines for the Computer-based Procedure System Design Process, B.3.9, Training Program Development, Criterion 4 - The training program should inform operators about limited and complete failures of the CBP. Operators should be trained to determine when to override CBP evaluations and advice. They should be able to manage the transition to PBPs when CBPs are lost and move back to them when system function is restored.

10. HFE-significant I&C degradations should be addressed in integrated system validation to ensure that measures taken in designing HSIs developing procedures and training operators will successfully mitigate the potential effects of these conditions on personnel's' performance of risk-important tasks.

    Discussion: This guidance is a more complete treatment of HSI and I&C degradations than exists in the current guidance. NUREG-0711, Section 11.4.3.2, Review Criterion 1 identifies as a test objective: Validate that the integrated system performance is tolerant of failures of individual HSI features. Additional guidance is given in NUREG-0711, Section 11 - Human Factors Verification and Validation, on sampling operational conditions. Section 11.4.1.2, Review Criterion 1 identifies failure events, including

    - instrument failures [e.g., safety-related system logic and control unit, fault tolerant controller, local "field unit" for multiplexer (MUX) system, MUX controller, and break in MUX line], including I&C failures that exceed the design basis, such as a common-mode I&C failure during an accident
    - HSI failures (e.g., loss of processing and/or display capabilities for alarms, displays, controls, and computer-based procedures)

    In addition, NUREG-0700, Appendix B.3, Review Guidelines for the Computer-based Procedure System Design Process, B.3.10, Human Factors Verification and Validation, Criterion 6 - Operators should be able to detect CBP errors and failures.

8 HSI DESIGN REVIEW GUIDELINES

This section contains guidance for reviewing an applicant's HSI design for monitoring the I&C system and its subsystems, and for detecting and managing degradations. Each individual guideline follows the NUREG-0700 format described in Section 2.3. Related guidance from NUREG-0700 is identified in the Additional Information section of each of them.

8.1 HSIs for Monitoring I&C System Conditions

8.1-1 Overall Representation of an I&C System

The HSI should provide a representation of the I&C system and its subsystems.

Additional Information: The representation of the I&C system and its subsystems should be sufficiently detailed to enable operators to monitor its HFE-significant performance, and detect HFE-significant I&C degradations.[91047]

8.1-2 Hierarchal Access to Information

Information should be presented using a hierarchal approach enabling operators to quickly and easily determine the overall status of I&C system and subsystems from top-level displays, and to access more detailed information on lower level displays.

Additional Information: Information hierarchies provide operators with a means to monitor the I&C system's status at a brief glance and then to access progressively more detailed information to support their situation assessment and troubleshooting. The displays should contain navigation aids to enable users to quickly and easily move from high- -level displays to low-level displays in the hierarchy (see NUREG-0700, Section 2.5.1, Display Selection and Navigation).[91047]

8. 1-3 Indicate Important Status and Performance Parameters

The HSI should provide information about each I&C subsystem's status and performance parameters needed to monitor the HFE-significant aspects of the system and detect I&C degradations.

Additional Information: The intent of this guideline is give operators knowledge about how well the HFE-significant aspects of the I&C system are performing. If the HSI includes performance measures for I&C subsystems, operators can monitor that performance. Comparing current performance with typical performance will support operators in detecting changes in the system. [91047]

8.1-4 Operator Requested Status Check

The HSI should provide the capability for operators to request a system check.

Additional Information: If operators suspect that the I&C system may not be performing as expected, the ability to request a status check y can help them resolve the concern.[91047]

8.2 HSI Response to I&C System Changes

8.2-1 Notification of Important Changes

The HSIs should notify operators to important changes in I&C system status and performance.

Additional Information: Alerts should be commensurate with the need for the operators' attention. For example, their attention is not needed immediately, then a nonintrusive message is appropriate. Some success was found with automation-generated verbal notifications .[91047]

8.2-2 Alert to Degraded Conditions

The HSI should alert operators when I&C system performance is deteriorating. *Additional Information:* In the context of this guideline, in a degraded condition, the I&C system still is carrying out its function, but its performance is not optimal. The communication subsystem provides an example. If the

subsystem is performing, but time delays exist slowing down information display and response to the operator's control inputs, operators should be alerted to the condition .[91047]

8.2-3 Alarm to I&C System Failure

The HSI should alarm when a failure of the I&C system or subsystem occurs.

Additional Information: In the context of this guideline, when the I&C system's (or subsystem) performance has degraded to the point where it cannot meet its function, it is considered failed. When the failure reflects an HFE-significant I&C degradation, the operator should receive an alarm. As with all alarms, operators should be given timely warning so they can institute compensatory actions or backup procedures .[91047]

8.2-4 Information on Failure Cause

The HSI should support operators in determining the cause(s) of degraded conditions and failures.

Additional Information: Automation, for example, can mask failures and degraded conditions in other plant systems when it compensates for them. This can lead to the operator's loss of situation awareness and becomes problematic when the situation reaches a point at which automation no longer compensates, and personnel have to take over.[91047]

8.2-5 Support Failure Recovery

The HSI should support operators in determining the steps for failure recovery or back-up actions should recovery be impossible.

Additional Information: When a failure is detected, the HSI should provide displays and information allowing personnel rapidly to determine what actions they must take to respond to the failure. For example, the HSI for an automated process that fails over to manual mode should, in addition to alerting personnel that manual control is required, point to or directly display the actions or procedure necessary to carry out the required manual actions. [91047]

8.3 Information Source and Quality

8.3-1 Validation Data Presented in HSIs

Data presented in the HSI should be validated where possible.

Additional Information: One approach to minimizing the impact of a degraded sensor and monitoring system is to ensure the information displayed at the operator's HSI is correct, and to code suspect information. Techniques such as signal validation and analytical redundancy (calculating the expected parameter values using a model of system performance) can be used to evaluate the correctness of information before displaying it. The results of these techniques can validate or invalidate information, or fail to determine whether or not it or not. Guidance on these aspects of information validation are addressed in NUREG-0700 Guidelines 1.4-9 - Invalid Data, 1.4-10 -Unvalidated Data, 1.1-21 - Analytical Redundancy, 5.3-2 - Data Reliability/Validation for Critical Plant Variables, 5.3-3 - Display of Data Reliability/Validation for Critical Plant Variables.[91047]

8.3-2 Identify Information Source

The HSI should support operators in distinguishing between directly sensed and derived information.

Additional Information: The effect of degraded I&C conditions can be misleading when displays include both directly sensed and derived information. One approach to minimize this concern is to distinguish between these sources n in a display, so operators can readily determine what information is directly sensed vs. that derived from sensors.[91047]

GLOSSARY

Applicant - An organization, such as a nuclear plant vendor or utility, that is applying to the U.S. Nuclear Regulatory Commission for design certification or plant licensing.

Architecture - The organizational structure of a system.

Closed-loop control - A control system in which the output is measured and compared with a standard representing the acceptable range, and any deviation from the standard is fed back into the system in a way that will reduce the deviation (IEEE, 1990).

Common cause failure (CCF) – A malfunction that results in an incorrect response or loss of function across multiple channels, sub-systems or systems at the same time.

Configural display – A display in which information dimensions uniquely are represented, but where new emergent properties are created from interactions between the dimensions. Configural-display representations often use simple graphic forms, such as a polygon.

Control stability - The stability of a control system relates to its response to inputs or disturbances. A system that remains in a constant state unless affected by an external action and returns to a constant state when the external action is removed is considered to be stable.

Degraded condition – A state in which the parameter, component, or system operates at less than its fully intended function, including failure.

Design failures – Failures that are caused by design flaws, i.e., a system response is unsafe (or not previously analyzed) even though it complies with the intended design algorithm.

Diverse instrumentation and control – The existence of a backup system, component, or software that is not of the same design or operational principle as the primary one. Diverse systems are not susceptible to common-cause failures.

Emergent feature – A high-level, global perceptual feature produced by the interactions among individual parts or graphical elements of a display (e.g., lines, contours, and shapes).

Failure- Degraded or terminated ability of a functional unit to perform a required function.

Fault detection – The process of determining which system, component, or parameter is faulty through various means of error-checking techniques and surveillances.

Fault tolerance – The existence of redundancy and/or diversity with fault-detection capability. Continuity of operations is assured by providing the needed function using a capability that is fault free.

Firmware – The combination of a hardware device and computer instructions and data that reside as read-only software on that device.

HFE-significant I&C degradations - The failure modes and degraded conditions of the I&C system that have the potential to impact HSIs used by personnel in performing risk-important tasks.

Human factors - A body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psycho-social considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training, job performance aids, and human performance evaluation (see "Human factors engineering").

Human factors engineering (HFE) – HFE is the application of knowledge about human capabilities and limitations to plants, systems, and equipment design. HFE provides reasonable assurance that the design of the plant, systems, equipment, human tasks, and the work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support the plant (see "Human factors").

Human-system interfaces (HSIs) - A human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this document, "system" refers to a nuclear-power plant. Major HSIs include alarms, information displays, controls, and procedures. Using HSIs is influenced directly by factors such as (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities, such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and, (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise. HSI use also is affected indirectly by other aspects of plant design and operation, such as the crew's training, shift schedules, work practices, and management and organizational factors.

Integral display – A display that depicts the integration of information in such a way that it does not represent explicitly the individual parameters used to generate it.

Latent fault – Faults that are undetected in an I&C system.

Microprocessor – A programmable digital device that incorporates the function of a central processing unit on a single semiconductor integrated circuit.

Open-loop control – A control system in which the output is permitted to vary in accordance with the inherent characteristics of the system and no function of the output is used as feedback to the system (IEEE, 1990).

Parameter drift - The latent tendency of a control system output to digress from the desired effect.

Redundancy - In fault tolerance, the presence of auxiliary components in a system to perform the same or similar functions as other elements for preventing or recovering from failures.

Remote Multiplexing Unit (RMU) - A device used to process digital data so that it can be transferred over an established communication pathway.

Risk-important human actions - Actions that plant personnel undertake to provide reasonable

assurance of plant safety. Actions may comprise one or more tasks. There are both absolute- and relative-criteria for defining risk important actions. From an absolute standpoint, a risk-important action is any action whose successful performance is needed to provide reasonable assurance of meeting the predefined risk criteria. From a relative standpoint, risk-important actions are defined as those with the greatest risk in comparison to all human actions. The identification can be done quantitatively from a risk analysis, and qualitatively from various criteria, such as concerns about task performance based on considering performance-shaping factors.

Sensor noise - Irrelevant data that hamper recognition and interpretation of data of interest (IEEE, 1990).

Separable display – Each process parameter is presented individually, and no relationships between them appear in the representation itself. The key aspect of separable displays is not that the individual parameters are presented, but that no interaction or relationship between them is perceived

Software failure – System failure due to the activation of a design fault in a software component.

Appendix A: Analysis of the Effects of MFV Controller Degradations on HSIs and Operator Performance

We identified the HSIs involved and postulated the potential impacts on operator performance using the documentation available and the Failure Modes and Effects Analysis (FMEA) of a PWR's digital feedwater control system (DFWCS) for each degraded condition of the MFV controller. We analyzed the following 22 degraded conditions of this controller's input and output signals:

1. Analog Input 0 (steam generator [S/G] level) fails to 0.0
2. Analog Input 1 (MFRV demand from the main CPU) fails to 0.0
3. Analog Input 2 (MFRV demand from the backup [B/U] CPU) fails to 0.0
4. Analog Output 0 (output to the MFRV positioner, PDI controller, and other S/G) fails to 0.0
5. Analog Output 2 (S/G level setpoint output) fails to 0.0
6. Digital Input 0 (B/U CPU power fail or in test) fails open
7. Digital Input 1 (B/U CPU Fail) fails open
8. Digital Input 2 (Main CPU power fail or in test) fails open
9. Digital Input 3 (Main CPU Fail) fails open
10. Digital Input 0 (B/U CPU power fail or in test) fails closed
11. Digital Input 1 (B/U CPU Fail) fails closed
12. Digital Input 2 (Main CPU power fail or in test) fails closed
13. Digital Input 3 (Main CPU Fail) fails closed
14. Digital Output 0 (A/M status to the Main CPU) fails open
15. Digital Output 1 (A/M status to the B/U CPU) fails open
16. Digital Output 2 (B/U CPU failed status to CPUs) fails open
17. Digital Output 3 (Main CPU failed status to CPUs) fails open
18. Digital Output 0 (A/M status to the Main CPU) fails closed
19. Digital Output 1 (A/M status to the B/U CPU) fails closed
20. Digital Output 2 (B/U CPU failed status to CPUs) fails closed
21. Digital Output 3 (Main CPU failed status to CPUs) fails closed
22. Loss of power to the controller.

The following table summarizes the results of the analysis.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Analog Input 0 (S/G level) Fails to 0.0	The signal is for display only.	The MFV display of S/G level will be low. There is no specific alarm or message.	Information about this failure mode is not available directly. Failure can affect the operator's ability to manually control the MFRV because this indication of the S/G level is not available to the operator.
Analog Input 1 (MFRV demand from the main CPU) Fails to 0.0	The controller initially will forward the failed demand signal to the MFRV positioner, the PDI controller, and the CPUs of the other S/G. The PDI controller then will detect the signal failure and automatically become the manual controller for the MFRV. The MFRV must be manually controlled via the PDI controller.	The MFV controller will display a "DEV" message when the Main CPU's demand signal differs from that of the backup (B/U) CPU by more than a setpoint after a time delay. The deviation status will be sent to the BFV controller that will activate a message in the Plant Computer. The PDI controller will display a "MFV Fail" message. There is no auditory alert to the operators.	The operators have to take manual control of the MFRV using the PDI controller. However, since information about this failure mode is available, but not annunciated, their control actions may be delayed.
Analog Input 2 (MFRV demand from the B/U CPU) Fails to 0.0	The MFV controller will continue to forward the signal from the main CPU to its output. No effect on the system's operation.	The MFV controller will display a "DEV" message when the Main CPU's demand signal differs from that of the B/U CPU by more than a setpoint after a time delay. The deviation message will be sent to the BFV controller that will activate a System Trouble message at the Plant Computer. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Analog Output 0 (Output to the MFRV positioner, PDI controller, and other S/G) Fails to 0.0	The demand signal to the MFRV positioner will fail to 0, and the valve will begin to shut. The PDI controller will detect the failure and automatically transfer to the manual mode. The PDI controller's output then will rise to the pre-failure value of the MFV controller's output and the MFRV will return to that position. The MFRV must be manually controlled from the PDI controller.	The PDI controller will display a "MFV Fail" message. Hence, information about this failure mode is available, but not annunciated.	The operators have to take manual control of the MFRV using the PDI controller.
Analog Output 2 (S/G level setpoint output) Fails to 0.0	The CPUs will detect a setpoint deviation if the related setpoints limit is exceeded, and revert to a built-in setpoint. Hence, the system is unaffected by this failure mode.	A system-deviation message in the Plant Computer will be activated, if a setpoint deviation is detected. Hence, information about this failure mode is available, but not annunciated. The setpoint display at the BFV controller will be low. The operator may use the MFV controller to manually adjust the SG level setpoint. However, the setpoint at the display of the BFV controller will remain low.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Input 0 (B/U CPU Power Fail or in Test) Fails Open	The MFV controller will block the B/U CPU's demand signal from its output. System operation will not be affected. The B/U CPU's status is sent to the CPUs and could affect the deviation logic of the CPUs. The signal normally is closed indicating that the B/U CPU is OK.	The MFV controller will indicate that the B/U CPU is failed by displaying the message "BCPU FAIL." The B/U CPU's status will be sent to the BFV controller that will transmit a message to the PC. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Digital Input 1 (B/U CPU Fail) Fails Open	The controller will not be able to determine the correct status of the B/U CPU. System operation is unaffected unless other failures occur. The signal normally is open indicating the B/U CPU is OK.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Input 2 (Main CPU Power Fail or in Test) Fails Open	Failover will occur from the main CPU to the B/U CPU. The MFV controller will send a Main CPU Fail signal to the CPUs and to the BFV controller. The Main CPU Fail signal affects the deviation logic of the B/U CPU. The signal normally is closed indicating the Main CPU is OK.	The MFV controller will indicate that the Main CPU is failed by displaying the message "MCPU FAIL." The BFV controller will send a message to the Plant Computer. Hence, information about this failure mode is available, but not annunciated.	The system's operation is unaffected, so no significant impact on human performance is anticipated.
Digital Input 3 (Main CPU Fail) Fails Open	The controller will not be able to determine the status of the Main CPU. System operation is unaffected unless other failures occur. The signal normally is open indicating the main CPU is OK.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Digital Input 0 (B/U CPU Power Fail or in Test) Fails Closed	The controller will not be able to determine the correct status of the B/U CPU. System operation is unaffected unless other failures occur. The signal normally is closed indicating the B/U CPU is OK.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Input 1 (B/U CPU Fail) Fails Closed	The MFV controller will block the B/U CPU's demand signal from its output. System operation will not be affected. The B/U CPU's status is sent to the CPUs and could affect their deviation logic. The signal normally is open indicating that the CPU is OK.	The MFV controller will indicate that the B/U CPU is failed by displaying the message "BCPU FAIL." The B/U CPU's status will be sent to the BFV controller that will transmit a message to the PC. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Input 2 (Main CPU Power Fail or in Test) Fails Closed	The MFV controller will be unable to determine the correct status of the Main CPU. The operation of the system is unaffected unless other failures occur. The signal is normally closed.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Input 3 (Main CPU Fail) Fails Closed	A failover will take place from the Main CPU to the B/U CPU. The MFV controller will send a Main CPU Fail signal to the CPUs and to the BFV controller. The Main CPU Fail signal affects the deviation logic of the B/U CPU. The operation of the system is unaffected unless other failures occur. The signal normally is open indicating the main CPU is OK.	The MFV controller will indicate that the Main CPU is failed by displaying the message "MCPU FAIL." The BFV controller will send a message to the Plant Computer. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Digital Output 0 (A/M Status to the Main CPU) Fails Open	A manual signal will be sent to the Main CPU, and the Transfer Inhibit Alarm window will be activated. Assuming the Main CPU is in control, and the MFV controller is in auto, the Main CPU will switch to the tracking mode, tracking the MFV controller's output. That output will be sent from the Main CPU to the MFV controller. The automatic control of the MFRV effectively is lost, and the operators have to take manual control using the MFV controller. The signal normally is closed in automatic mode.	The PDU of the Main CPU will display the "Transfer Inhibit Alarm." A message also will be sent to the Plant Computer. Hence, information about this failure mode is available, but not annunciated.	The operators have to take manual control of the MFRV using the MFV controller.
Digital Output 1 (A/M Status to the B/U CPU) Fails Open	Assuming the Main CPU is in control and the controller is in auto, system operation will not be affected. The signal normally is closed in automatic mode.	The PDU of the B/U CPU will display the "Transfer Inhibit Alarm." A message also will be sent to the Plant Computer. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Output 2 (B/U CPU Failed Status to CPUs) Fails Open	The failed signal will be sent to the Main and B/U CPUs. Assuming the Main CPU is in control, and the MFV controller is in auto, system operation is unaffected. The signal normally is open indicating the B/U CPU is OK.	There is no indication of the failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Digital Output 3 (Main CPU Failed Status to CPUs) Fails Open	The failed signal will be sent to the Main and B/U CPUs. Assuming the Main CPU is in control, system's operation is not affected. This signal normally is open indicating the Main CPU is OK.	There is no indication of the failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Output 0 (A/M Status to the Main CPU) Fails Closed	The failed signal will be sent to the Main CPU. If the Main CPU is in control, the system's operation is not affected. The signal normally is closed when in automatic mode.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Output 1 (A/M Status to the B/U CPU) Fails Closed	If the Main CPU is in control, and the MFV controller is in automatic mode, then the system's operation is not affected. The signal normally is closed when the controller is in automatic mode.	There is no indication of this failure.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Digital Output 2 (B/U CPU Failed Status to CPUs) Fails Closed	The failed signal will be sent to both CPUs. The B/U CPU will continue in tracking mode. If the Main CPU is in control, and the MFV controller is in automatic mode, system operation will be unaffected. The failed signal may affect the deviation logic of the Main CPU. The signal normally is open indicating the B/U CPU is OK.	The PDUs of the CPUs display a message indicating that the B/U CPU failed. A message also is sent to the PC. Hence, information about this failure mode is available, but not annunciated.	Since the system's operation is unaffected, no significant impact on human performance is anticipated.
Digital Output 3 (Main CPU Failed Status to CPUs) Fails Closed	The failed signal will be sent to both CPUs. The Main CPU will enter a tracking mode, and will send demand signals received from the MFV back to this controller. The MFV controller cannot detect the failure of the Main CPU when this CPU is tracking. Hence, there is a loss of automatic control of the MFRV. The signal normally is open indicating the Main CPU is OK.	The PDU of the Main CPU will display a message indicating that the Main CPU failed. The MFV controller will show the message "MCPU FAIL," and send a signal to the BFV controller that will transmit a message to the PC. Hence, information about this failure mode is available, but not annunciated.	The operators have to take manual control of the MFRV using the MFV controller.

Degraded Condition	System Impact	HSI Impact	Human Performance Impact
Loss of power to the controller	All analog outputs from the MFV controller fail to 0. All digital outputs from this controller fail to Open status. The PDI controller will switch automatically to manual mode of operation, and initially its output will raise to the pre-failure output level of the MFV controller. The MFRV has to be controlled manually using the PDI controller. The CPUs will use the built-in S/G level setpoint and track PDI controller's output.	The MFV controller will be off. The PDI controller will display a "MFV Fail" message. The BFV controller possibly will send a message to the PC. Hence, information about this failure mode is available, but not annunciated.	The operators have to take manual control of the MFRV using the PDI controller.