BNL-93951-2010-CP

The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance

John O'Hara, W. Gunther & G. Martinez-Guridi
Brookhaven National Laboratory

Jing Xing & Valerie Barnes
U.S. Nuclear Regulatory Commission

Presented at the Seventh American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC &HMIT 2010)
Las Vegas, NV

November 7-11, 2010

Energy Sciences and Technology Department

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

DISCLAIMER

The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance

John O'Hara, Bill Gunther & Gerardo Martinez-Guridi
P.O. Box 5000
Brookhaven National Laboratory
Upton, NY 11973-5000
ohara@bnl.gov; gunther@bnl.gov; martinez@bnl.gov

Jing Xing & Valerie Barnes
U.S. Nuclear Regulatory Commission
Jing.Xing@nrc.gov; VXB3@nrc.gov

ABSTRACT

Integrated digital instrumentation and control (I&C) systems in new and advanced nuclear power plants (NPPs) will support operators in monitoring and controlling the plants. Even though digital systems typically are expected to be reliable, their potential for degradation or failure significantly could affect the operators' performance and, consequently, jeopardize plant safety. This U.S. Nuclear Regulatory Commission (NRC) research investigated the effects of degraded I&C systems on human performance and on plant operations. The objective was to develop technical basis and 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 control system of a currently operating pressurized water reactor (PWR) 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 findings as the technical basis upon which to develop HFE review guidance.

Key Words: human factors engineering, human-system interfaces, instrumentation and control, degraded conditions, operator performance

1 INTRODUCTION

The designs of new and advanced nuclear power plants (NPPs) differ in several important respects from those currently operating in the United States (U.S.), including their instrumentation and control (I&C) systems. Current plants employ predominantly analog I&C technology, while new plants are designed to include digital I&C technology. The latter technology expectedly will offer functions and capabilities that are vital for performance and plant safety. Together with the NPP's personnel, the I&C system might be considered as the plant's "central nervous system." It (1) senses basic parameters; (2) monitors the plant's processes, performance, and various barriers that prevent release of radioactive material; and (3) 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 those used in NPPs 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., 2008a). Employing these advanced techniques will provide more intricate and more complex control of plant systems and processes than those currently used. Digital I&C systems also support new forms of automation that make greater use of interactions between personnel.

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. 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, including "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 normal and off-normal events, thus supporting the goals of efficiently and safely producing power. 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 and/or indication. Some human-performance considerations in dealing with operations under degraded I&C conditions included detecting the failure of the digital system, and the ability to transition to back-up systems when failures occur.

Similar to the NRC, the Electric Power Research Institute (EPRI) and the Nuclear Energy Institute (NEI) highlighted degraded I&C systems as a technical issue, referred to as "Failure management for new human-system interface (HSIs)," facing new plant development (Torok et al., 2006).

2 OBJECTIVES AND METHODOLOGY

The objectives of this NRC research were 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. This paper addresses the first of these objectives.

For the purposes of this study, "degraded" refers to a full range of 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 throughout an NPP also is a 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.

We followed the methodology established to develop HFE review guidance to address safety review needs (O'Hara et al., 2008b). Figure 1 is an overview of the main steps in the process. Of the four steps shown, this research addresses the second, technical basis and guidance development. Technical basis and guidance development involves several phases including topic characterization, technical-basis development, and guidance development and documentation. The first step of the methodology was researched earlier (O'Hara et al., 2008, 2008b) when "Operations under conditions of degraded I&C" was identified as a top-priority issue. The last two steps will be accomplished in future research.

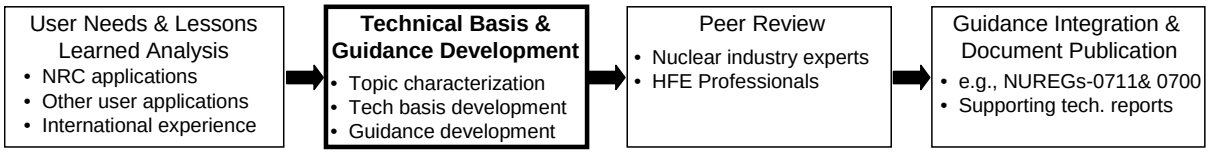

Figure 1. Major steps in developing NRC HFE guidance

We developed a characterization representing the I&C system, HSIs, and human performance, as illustrated in Figure 2, and identified the key constituent elements of each level. Our characterization provides a way of organizing the evaluation of other research and events into a standardized framework for developing general lessons learned. Once the characterization was developed, we reviewed industry standards and guidelines, empirical studies, and plant operating experience to identify the effects of degraded I&C on personnel. In addition, we evaluated the potential effects on HSIs and the operators' performance of selected failure modes of the digital feedwater control system of a currently operating PWR. Our findings are summarized in Section 3, Results. A complete report on this research and the resulting review guidelines can be found in O'Hara et al. (2010).

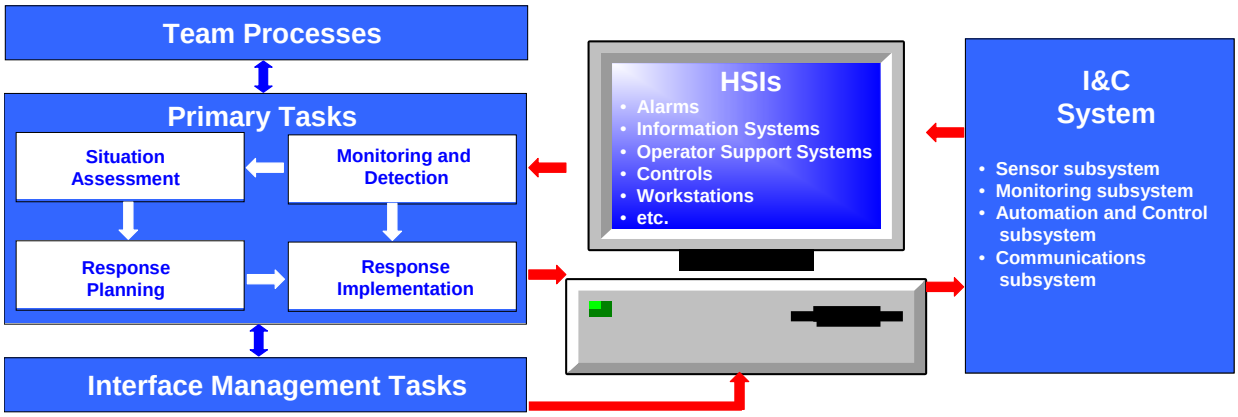

Figure 2. Characterization of the I&C system, the HSI, and human performance

3 RESULTS

In this section, we present the findings related to our evaluation of industry standards and guidelines, empirical studies, plant operating experience, and selected failure modes of a digital feedwater control system.

3.1 Industry Standards and Guidelines

Over the years, the nuclear industry expended much effort to help ensure that the quality of I&C systems and HSIs used in NPPs will support safe operations. In the U.S., this goal was met through the implementation of industry standards (e.g., Institute of Electrical and Electronics Engineers, 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 staff guidance (ISGs) documents and branch technical positions (BTPs).

The nuclear industry, through EPRI and the Institute for Nuclear Power Operations (INPO), established standards of performance for operations and safety of which the I&C 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 industry standards. For instance, RIS 2002-22 (NRC, 2002) 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.

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.

3.2 Analysis of Basic Literature

In this section, we summarize the findings from 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. We also addressed 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.

Research on the effect of degradation of the sensor subsystem and human performance offers the following findings (Moray et al., 1993; Moray et al., 1994; Reising & Sanderson, 2000 & 2004; St-Cyr & Vicente, 2004; St-Cyr & Vicente, 2005; St-Cyr, 2006; Vicente et al., 1996):

- Sensor degradations can make displays difficult to understand.
- Graphical displays, especially those employing emergent features,[1] appear more subject to the effects of sensor degradation than simpler displays.
- 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 graphical 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 PWR 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, the operator may initially suspect a problem is developing, when in fact; a degraded sensor is giving false level readings. As a second example, an operator takes a control action to increase the pressurizer's level, and observes the HSIs to assure that level is rising. 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 directly shown in the HSI. Table I illustrates the complex relationship that can occur between different sensor conditions and an operator's situation assessment of a low-pressurizer-level event.

We also identified some research that, while not specifically directed at I&C degradation, provides insights that can be extrapolated to it. Specifically, research on automation provides clues into the degradation of the automation and control subsystem, and studies of time delays provide insights into degradation of the communication system. Each is summarized briefly below.

[1] 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.

We reviewed the studies addressing the relationship between automation design and human performance, including automation degradation, in a recent NRC report (O'Hara & Higgins, 2010). The general findings related to degraded automation are:

- 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
- when automation fails teamwork is affected when operators have to manually perform automation's tasks, thereby changing the roles and responsibilities of crew members
- factors contributing to this difficulty include over reliance on automation and HSI design

Table I 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

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

Most systems have inherent time delays, or lags, that stem from (1) time from when a control action is taken at the HSI to when the signal reaches the actuation system; (2) the time it takes for the system to change in response to the control action; and (3) time between the change in system's response and the change in the information provided to system users through the HSI (feedback). The first and third delays are affected by the communication subsystem. Research on time delays affords some understanding of the effects of communication subsystem degradation on the operator's performance (Lorenzo, 1990; Wickens 1984, 1986; Wickens et al., 2004):

- as time lags increase, the operator's control performance decreases
- the operator's closed-loop control (control based on feedback) becomes increasingly unstable

- operators shift the control strategies they are using and their performance becomes increasingly open-loop (control based on prediction rather than feedback)

Designers may employ a variety of strategies to 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 at the HSIs
- Ensure information quality at the HSIs
- Distinguish directly sensed information sources from derived ones in displays
- Support I&C degradation detection and management in training
- Support training on the management of time delays

Thus, we conclude from this review of the limited literature available that the impacts of degraded I&C can be significant, and adversely affect the HSIs and the operator's performance. The insights derived from this review are limited by the fact that the research has only examined a few of the ways in which I&C systems can fail. 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 of the other I&C subsystems on HSIs and human performance. Thus, the diversity of degradations and failure modes of an I&C system has hardly been probed. Additional research is essential to define robustly the relationships between degraded conditions and HSIs/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.

3.3 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., 2008b; Wood et al., 2004). Especially lacking are studies that analyze numerous events to identify lessons learned for these systems. With this caveat, we evaluated the information in studies and individual event reports (Licensee Event Reports or LERs).

Both the NRC and the commercial nuclear industry have been evaluating the incidence of digital I&C failures (Brill, 2000; Torok, 2008; Waterman, 2006). Their findings help address general questions, such as how frequently digital systems fail, and if the outcomes are significant enough to be a concern. 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
- degradation of a digital I&C system can have major consequences, e.g., involve reactor trips and other transients that can challenge reactor safety systems
- approximately a third of the incidents involved the HSI, indicating the possibility for a digital I&C failure to lower the operator's ability to monitor the plant and respond to an event
- impacts were experienced in key areas, including the main control room, the technical support center, and emergency-operations locations

We evaluated eight events involving digital I&C degradations to identify more specifically their implications for human performance. The evaluation is summarized in Table II, located at the end of this

paper. Analyses of these events show that degraded digital 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 digital I&C systems also can hamper the operator's ability to implement responses by delaying responses and feedback when a communication subsystem overloads and slows system performance.

Further, operators may be unable to monitor, detect, and be aware of the implications of degraded digital I&C conditions on plant performance because of a lack of alarms, information concerning the conditions, and training. Thus, these deficiencies may engender a misinterpretation of the situation, and a lowered awareness of the severity of the conditions. Operators may need improved alarms and better information on the key functional aspects of digital I&C and its role in the plant's response.

3.4 Analysis of a PWR Digital Feedwater Control 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 currently operating PWR as their case study. At this plant, there is a DFWCS for each of the two secondary loops. They developed a detailed failure modes and effects analysis (FMEA) with the information obtained from the plant.

We assessed the effect of degradations of a major digital component of this system using some of this information as our starting point. Although the DFWCS is a complex digital control system used in a NPP, it can be used to illustrate the process for evaluating the effects on human performance of a digital I&C system degradation.

We chose the controller of the main feedwater regulating valve (MFRV) for the detailed analysis because:

- it controls the MFRV and failures in the controlled 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 some failures of the controller

We evaluated the potential effects of the degraded I&C on human performance by postulating that a hardware component of the MFRV controller had deteriorated, and propagated possible types of deterioration through the HSI to determine its potential effects on human performance. The MFRV controller is part of the "Automation and Control" subsystem (see Figure 2). 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 bypass feedwater regulating valve (BFRV) normally is closed, and the DFWCS controls the MFRV and a feedwater pump (FWP).

Twenty-two degraded conditions of the MFRV controller's input and output signals were analyzed. Seventeen of the degraded conditions are 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 HSI provides 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 does not specify the condition. Operators may need technical support from specialized 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 steam generator (S/G) level to the MFRV 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 indication of the level is wrong.

Five of the degraded conditions cause a loss of automatic control of the MFRV. Operators are required to take manual control of the system and failure to do so may cause 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 plant to get closer to a trip. A reactor trip is 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; for example, the accident at Three Mile Island Unit 2 in 1979 started with a reactor trip with a loss of feedwater.

Thus, our analysis of selected failure modes in a digital feedwater control system revealed the following:

- A single failure of a digital control system 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 the system is responding appropriately to the situation, it may appear to be malfunctioning to operators in view of their information and understanding of the situation. Further, operators may take inappropriate actions based on 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.
- 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 additional failures or changes in conditions.
- Loss of automatic control places demands on operators, and can lead to a transient, such as a reactor trip.

There are strategies that might be adopted to minimize the potential impact of degraded I&C subsystems on the operator's performance in monitoring the I&C system and detecting degraded conditions. One strategy is 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 this performance 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 are not communicated to operators through the HSI. Note that one does not necessarily want every possible indication presented in the HSI. An analysis should be performed to determine which personnel should receive the indications, e.g., operations or maintenance personnel.
- Five of the degraded digital I&C conditions cause the loss of automatic control. Therefore, it seems advisable to include an audible alarm that would alert the operator of the automatic-manual status of the system.

Another such strategy would be to assess the outcome of I&C failures on the HSIs. Our consideration of the digital feedwater control system supports this recommendation. Extending the failure modes and effects analysis to include how failure modes are processed through the HSI might identify the

potential impacts on the HSI and human performance; insights gained through this type of study then could be incorporated in system design as well as HFE review guidance.

4 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 expected to be reliable, their potential for degradation or failure could greatly affect the operator's performance and, consequently, impact plant safety. Among our more important findings was the paucity of information available pertaining to the effects of degraded I&C conditions on the operator's performance. Few studies specifically assessed these effects; most research that was undertaken focused on sensor issues and automation. Although operating experience on degraded digital I&C systems 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 and, therefore, operator performance. 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
- when automation fails, teamwork is affected when operators have to manually perform automation's tasks, thereby changing the roles and responsibilities of crew members
- operator control action instability resulting from 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 that may be necessary. Important degradations may not be alarmed and operators may not have sufficient information at their HSIs, in procedures, or from training to deal with them.

We identified two primary strategies for addressing the human performance issues associated with degraded I&C systems. One strategy is to analyze the potential impact of I&C failures on HSIs that will aid in identifying HFE-significant I&C degradations. One example is extending a FMEA to encompass an evaluation of how the HSIs process failure modes, and to detail potential impacts on human performance that may be addressed by modifying the related system's design. The second strategy is to improve the HSIs so that they better support operators in monitoring an I&C system and in detecting and managing degraded conditions of the system and of the NPP.

We used the information obtained as the technical basis 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. The guidance resulting from this research can be integrated into the appropriate NRC 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 can support the NRC staff's review of new plants and of digital I&C upgrades to existing plants.

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 more complex situations involving actual operators
- 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
- Identification of the relationship of maintenance on I&C System Degradation

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.

5 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 Michael Boggi, former NRC Project Manager, and Jim Higgins of BNL for their insights and helpful comments.

6 REFERENCES

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

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.

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.

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.

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

NRC (2002). *NRC Use of EPRI/NEI Joint Task Force Report, "Guideline On Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision Of EPRI TR-102348 To Reflect Changes To The 10 CFR 50.59 Rule"* (Regulatory Issue Summary 2002-22). 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., Gunther, W., & Martinez-Guridi, G. (2010). *The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance* (BNL Tech Report No. 91047-2010). Upton, NY: Brookhaven National Laboratory.

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. & Fink, R. (2008a). *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., Brown, W., O'Hara, J., Fink, R., Persensky, J., Lewis, P., Kramer, J., Szabo, A., & Boggi, M. (2008b). *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., 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., Stubler, W., & Higgins, J. (1996). Hybrid human-system interfaces: Human factors considerations (BNL Report J6012-T1-4/96). Upton, New York: Brookhaven National Laboratory.

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

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.

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., 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.

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

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.

Table II Summary of Selected 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.
Browns Ferry 3 - Ethernet failure (NRC Info Notice 2007-0015)	▪ Auto/control ▪ Communication	▪ Control ▪ Information	▪ Situation Assessment ▪ Response Implementation	Electronic infrastructure (data highway) degradation.
Turkey Point - EDG Load Sequencer Failure; Logic error would have prevented an auto initiation of a safety injection system (LER 250-1994-005-02)	▪ Auto/Control	▪ Control	▪ Response Planning and Implementation	Testing of logic circuitry made the equipment inoperable
Software problem with the core protection calculators would result in the use of the last known value in the event of a failure rather than initiating a trip signal (LER 529-2005-004)	▪ Monitoring	▪ Alarm ▪ Control	▪ Monitoring & Detection	Latent or undetected failure.
Perry - failures of the digital feedwater control system power supplies that caused a reactor scram with complications including the loss of injection sources (LER 438-2007-008)	▪ 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. (Waterman, 2006)	▪ 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. (Waterman, 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. (LER 455-2005-001)	▪ 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.