



**BNL-79947-2008**

***Human Factors Considerations with Respect to  
Emerging Technology in Nuclear Power Plants***

John M. O'Hara, James C. Higgins, and William S. Brown  
Brookhaven National Laboratory

Robert Fink  
CDF Services, Inc.

**September 2008**

**Energy Sciences and Technology Department**

**Brookhaven National Laboratory**

P.O. Box 5000  
Upton, NY 11973-5000  
[www.bnl.gov](http://www.bnl.gov)

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

## **DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

# Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants

*Prepared for:*

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

*Prepared By:*

John M. O'Hara, James C. Higgins, and William S. Brown  
Brookhaven National Laboratory  
Energy Sciences and Technology Department  
Upton, NY 11973-5000

Robert Fink  
CDF Services, Inc.  
Fayetteville, AR 72701

September 2008



## **ABSTRACT**

This Nuclear Regulatory Commission (NRC) sponsored study has identified human performance research that may be needed to support the review of a licensee's implementation of new technology in nuclear power plants. To identify the research issues, current industry developments and trends were evaluated in the areas of reactor technology, instrumentation and control technology, human-system integration technology, and human factors engineering (HFE) methods and tools. The research issues were organized into seven high-level HFE topic areas: Role of Personnel and Automation, Staffing and Training, Normal Operations Management, Disturbance and Emergency Management, Maintenance and Change Management, Plant Design and Construction, and HFE Methods and Tools. The issues were then prioritized into four categories using a "Phenomena Identification and Ranking Table" methodology based on evaluations provided by 14 independent subject matter experts. The subject matter experts were knowledgeable in a variety of disciplines. Vendors, utilities, research organizations and regulators all participated. Twenty issues were categorized into the top priority category. This Brookhaven National Laboratory (BNL) technical report provides the detailed methodology, issue analysis, and results. A summary of the results of this study can be found in NUREG/CR-6947. The information gathered in this project can serve as input to the development of a long-term strategy and plan for addressing human performance in these areas through regulatory research. Addressing human-performance issues will provide the technical basis from which regulatory review guidance can be developed.



## **ACKNOWLEDGMENTS**

The authors wish to thank J Persensky, Paul Lewis, Joel Kramer, Autumn Szabo and Mike Boggi (the NRC Project Managers); Michael Waterman, Kent Welter, and James Bongarra (NRC technical reviewers); and Richard Deem of BNL for their thorough review and helpful comments on this report. Special thanks and gratitude to the subject matter experts who provided their comments, suggestions, and insights during a workshop held in support of this project. We would also like to acknowledge the efforts of Maryann Julian of BNL for her dedication and contributions throughout the project.



# CONTENTS

	<u>Page</u>
<b>ABSTRACT</b> .....	<b><u>iii</u></b>
<b>ACKNOWLEDGMENTS</b> .....	<b><u>v</u></b>
<b>ABBREVIATIONS</b> .....	<b><u>xi</u></b>
<b>1 INTRODUCTION</b> .....	<b><u>1</u></b>
1.1 Background .....	<u>1</u>
1.2 Objectives .....	<u>2</u>
1.3 Report Organization .....	<u>2</u>
<b>2 METHODOLOGY</b> .....	<b><u>3</u></b>
2.1 Approach .....	<u>3</u>
2.2 Data Sources .....	<u>3</u>
<b>3 ISSUE IDENTIFICATION</b> .....	<b><u>7</u></b>
3.1 New Reactor Designs and Technology .....	<u>7</u>
3.1.1 Generation II Plant Modernization .....	<u>8</u>
3.1.1.1 Design Description .....	<u>8</u>
3.1.1.2 Potential Issues .....	<u>9</u>
3.1.2 Generation III Reactor Designs .....	<u>14</u>
3.1.2.1 Design Descriptions .....	<u>16</u>
3.1.2.2 Potential Issues .....	<u>22</u>
3.1.3 Generation IV Reactor Designs .....	<u>25</u>
3.1.3.1 Generation IV Design Goals .....	<u>26</u>
3.1.3.2 Potential Human-performance Issues Related to Generation IV Goals .....	<u>27</u>
3.1.3.3 Design Descriptions .....	<u>29</u>
3.1.3.4 Potential Design Related Issues .....	<u>33</u>
3.1.4 Summary of New Reactor Design and Technology Related Issues ...	<u>35</u>
3.2 Digital Instrumentation and Control Technology .....	<u>36</u>
3.2.1 Advanced Functional Capabilities .....	<u>37</u>
3.2.2 Managing Digital I&C Systems .....	<u>46</u>
3.3 Human-system Integration Technology .....	<u>50</u>
3.3.1 Organizational Factors .....	<u>51</u>
3.3.2 Advanced Human System Interfaces .....	<u>53</u>
3.3.3 Computerized Support Systems .....	<u>61</u>
3.4 Advances in HFE Methods and Tools .....	<u>64</u>
3.4.1 Current HFE Methods and Tools .....	<u>64</u>
3.4.2 Trends in HFE Methods and Tools .....	<u>68</u>
<b>4 ISSUE SUMMARY AND ORGANIZATION</b> .....	<b><u>71</u></b>
4.1 Defining Concept of Operations .....	<u>71</u>
4.2 Organization of Human-performance Issues Into High-level Topic Areas ...	<u>74</u>

# CONTENTS (Cont'd.)

	<u>Page</u>
<b>5 HUMAN PERFORMANCE ISSUE PRIORITIZATION .....</b>	<b><u>81</u></b>
5.1 Overview .....	<u>81</u>
5.2 Objective .....	<u>81</u>
5.3 Methodology .....	<u>81</u>
5.3.1 Subject Matter Experts .....	<u>81</u>
5.3.2 Issue Evaluation Procedures .....	<u>81</u>
5.3.3 Issue Prioritization .....	<u>84</u>
5.4 Results .....	<u>85</u>
5.4.1 Priority Groupings .....	<u>85</u>
5.4.2 Bases For Priority 1 Issues .....	<u>87</u>
<b>6 SUMMARY AND CONCLUSIONS .....</b>	<b><u>91</u></b>
<b>7 REFERENCES .....</b>	<b><u>93</u></b>
<b>Appendix - Detailed HSI Issues Description .....</b>	<b><u>99</u></b>

## TABLES

	<u>Page</u>
Table 2-1 Organizations Contacted Regarding New Reactor Work .....	<u>4</u>
Table 3-1 Example of the Impact of Technology on Teamwork .....	<u>12</u>
Table 3-2 Reactor Designs for Near-term Deployment .....	<u>15</u>
Table 3-3 Design Characteristics for Near-term Reactor Designs With Potential Human-performance Issues .....	<u>23</u>
Table 3-4 Generation IV Reactor Design Goals .....	<u>26</u>
Table 3-5 Examples of Design Errors .....	<u>28</u>
Table 3-6 Characteristics of Generation IV Reactor Design With Potential Human-performance Issues .....	<u>34</u>
Table 4-1 Relationship of Issues to High-level Topic Areas .....	<u>76</u>
Table 4-2 Organization of Issues into High-level Topic Areas .....	<u>78</u>
Table 5-1 Organization of Issues into Priority Categories .....	<u>85</u>

## FIGURES

Figure 3-1 Evolution of Nuclear Power Technology .....	<u>7</u>
Figure 3-2 Hybrid Control Room .....	<u>9</u>
Figure 3-3 ABWR Control Room .....	<u>17</u>
Figure 4-1 Concept of Operations Dimensions .....	<u>73</u>
Figure 5-1 Issue Prioritization Based on Ratings of Safety Significance and Immediacy .....	<u>86</u>



## ABBREVIATIONS

A-A	abstraction-aggregation
ABWR	Advanced Boiling Water Reactor
ACR-700	Advanced CANDU Reactor 700
AECL	Atomic Energy of Canada, Ltd.
AIAA	American Institute of Aeronautics and Astronautics
ANS	American Nuclear Society
AP600	Advanced Plant 600
AP1000	Advanced Plant 1000
APR1400	Advanced Power Reactor 1400
APWR	Advanced Pressurized Water Reactor
ATWS	anticipated transient without scram
BNL	Brookhaven National Laboratory
BWR	boiling water reactor
CANDU	CANada Deuterium Uranium (Atomic Energy of Canada Limited)
CAREM	Central Argentina de Elementos Modulares
CBP	computer-based procedure
CEA	Commissariat à l'Energie Atomique.
CFR	U.S. Code of Federal Regulations
COSS	computerized operator support system
CR	control room
CSCW	computer supported cooperative work
CSN	Spanish Council for Nuclear Safety
CSNI	Committee on the Safety of Nuclear Installations
CTA	cognitive task analysis
D&C	Plant Design and Construction
DCIS	distributed control and information system
DEM	Disturbance and Emergency Management
DoD	Department of Defense
DOE	Department of Energy
EBS	extra borating system
EdF	Electricite de France
EFWS	emergency feed water system
EID	ecological interface design
EOP	emergency operating procedures
EPG	emergency procedure guidelines
EPR	Evolutionary Pressurized Water Reactor
EPRI	Electric Power Research Institute
ESBWR	Economic (European) Simplified Boiling Water Reactor
FANP	Framatome ANP
FITNESS	Functional Integrated Treatments for Novative Ecological Support System
GDSCS	gravity driven cooling system
GFR	Gas-cooled Fast Reactor
GT-MHR	Gas Turbine-Modular High Temperature Reactor
HC-BWR	High Conversion Boiling Water Reactor
HFE	human factors engineering
HMI	human-machine interface
HMT	HFE Methods and Tools
HPCS	high pressure core spray

## ABBREVIATIONS (Cont'd.)

HRA	human reliability analysis
HRP	Halden Reactor Project
HSE	United Kingdom Safety and Health Executive
HSI	human-system interface
HSK	Swiss Nuclear Safety Inspectorate
HTGR	High Temperature Gas-cooled Reactor
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IEEE	International of Electrical and Electronics Engineers
IMR	International Modular Reactor
INEEL	Idaho National Engineering and Environmental Laboratory
IRIS	International Reactor Innovative and Secure
IRSN	Institute de Radioprotection et de Surete Nucleaire
IRWST	in-containment refueling water storage tank
ISO	independent system operator
KAERI	Korea Atomic Energy Research Institute
LFR	Lead-cooled Fast Reactor
LOCA	loss of coolant accident
LOFW	loss of feed water
LHSI	Low Head Safety Injection
LWR	light water reactor
MCM	Maintenance and Change Management
MEMS	micro electro-mechanical sensors
MHSI	medium head safety injection
MOX	mixed oxide (plutonium/uranium nuclear fuel)
MSR	Molten Salt Reactor
MWe	megawatts (electric)
MWth	megawatts (thermal)
NERI	Nuclear Energy Research Initiative (DOE)
NOK	Nordostschweizerische Kraftwerke AG
NOM	Normal Operations Management
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
OECD	Organization for Economic Co-operation and Development
ORNL	Oak Ridge National Laboratory
PBP	paper-based procedure
PBMR	Pebble Bed Modular Reactor
PIRT	Phenomena Identification and Ranking Table
PRA	probabilistic risk analysis
PSA	probabilistic safety assessment
PWR	pressurized water reactor
R&D	research and development
RCCS	reactor cavity cooling system
RCIC	reactor core isolation cooling
RHR	residual heat removal
RO	reactor operator
RPA	Role of Personnel and Automation
RPV	reactor pressure vessel

## ABBREVIATIONS (Cont'd.)

RV	reactor vessel
S&T	Staffing and Training, and Teamwork
SA	situation awareness
SAR	safety analysis report
SART	silence, acknowledge, reset, test
SBWR	Simplified Boiling Water Reactor
SCWR	supercritical-water-cooled reactor system
SDCV	spatially dedicated, continuously visible
SFR	Sodium-cooled Fast Reactor
SKI	Swiss Nuclear Safety Inspectorate
SLC	standby liquid control
SMART	System-integrated Modular Advanced Reactor
SME	subject matter expert
SPDS	safety parameter display system
SRO	senior reactor operator
SRV	safety relief valve
STUK	Radiation and Nuclear Safety Society of Finland
SWR-1000	Siedewasser Reactor-1000
TMI	Three Mile Island
U.K.	United Kingdom
U.S.	United States
VDU	video display unit
VHTR	Very-high-temperature Reactor System
VR	virtual reality
VTT	Technical Research Centre of Finland



# 1 INTRODUCTION

## 1.1 Background

Over two decades have passed since a new commercial nuclear power plant (NPP) has been built in the United States (U.S.). There is now a renewed interest in nuclear energy and the U.S. is exploring the possibility of constructing new reactors within the next decade; in part, through the Department of Energy's (DOE) Nuclear Power 2010 Program (DOE, 2002a):

Deploying new base-load nuclear generating capacity in this decade would support the National Energy Policy objectives of enhancing U.S. energy supply diversity and energy security. The Nuclear Power 2010 program, unveiled by the Secretary of Energy on February 14, 2002, is a joint government/industry cost-shared effort to identify sites for new nuclear power plants, develop advanced nuclear plant technologies, and demonstrate new regulatory processes leading to a private sector decision by 2005 to order new nuclear power plants for deployment in the United States in the 2010 timeframe.<sup>1</sup>

Looking longer-term, the U.S. is participating in the international effort to identify and develop the next generation of commercial nuclear power plants as part of the International Generation IV reactor initiative<sup>2</sup> (DOE, 2002b, 2003), and through the DOE's Nuclear Energy Research Initiative (NERI). NERI was established to address and help overcome the principal technical and scientific issues affecting the future use of nuclear energy.<sup>3</sup>

The state-of-the-art commercial nuclear plant today is referred to as a Generation III plant. Currently operating commercial nuclear power plants in the U.S. are considered Generation II plants. Generation III plants employ decades-old reactor technology, simplified or passive safety features, digital instrumentation and control (I&C) systems, and computer-based control rooms. The designs being considered for near-term and future deployment include more advanced light water reactors (LWRs) (sometimes referred to as Generation III+), as well as, non-LWR designs. The term "Generation IV" refers to future plants that will be brought into service approximately 20 years from now. They are expected to be very different from today's plants both in terms of reactor technology and concept of operations (Persensky & O'Hara, 2005).

Licensing is a significant consideration for all new plants. The U.S. Nuclear Regulatory Commission (NRC) has performed design certification reviews of several new plant designs, such as General Electric's Advanced Boiling Water Reactor (ABWR), Westinghouse's Advanced Plant 600 (AP600) and Advanced Plant 1000 (AP 1000), and Combustion Engineering's System 80+. These designs are Generation III LWRs whose reviews date back to the early 1990s. The reviews of Generation III and Generation IV plant designs may pose new challenges due to new reactor designs, advances in I&C, and new approaches to human-system interface (HSI) design.

---

<sup>1</sup> Retrieved October 10, 2005 from <http://www.ne.doe.gov/planning/NucPwr2010.html>

<sup>2</sup> Information on DOE's Generation IV Program retrieved February 14, 2008 from <http://nuclear.energy.gov/genIV/neGenIV1.html>

<sup>3</sup> Information on DOE's NERI Program retrieved February 14, 2008 from <http://nuclear.energy.gov/neri/neNERIresearch.html>

To assure its regulations and review guidance will adequately support safety reviews of the human factors aspects of new generations of NPPs, the NRC is conducting research to identify potential human-performance issues and the technical basis needed to address them.

## **1.2 Objectives**

The objective of this study is to identify potential human-performance issues related to the role of personnel operating new NPPs and the technological advances that will support that role. As used in this report, the phrase “research issue” or the term “issue” refers to:

- an aspect of new NPP development or evaluation for which available information suggests that human performance may be negatively impacted
- an aspect of new reactor development or design for which it is suspected that human performance may be impacted, but additional research and/or analysis is needed to better understand and quantify that impact
- a technology or technique that will be used for new plant design or implementation for which there is little or no review guidance

## **1.3 Report Organization**

The remainder of this report is divided into several sections. Section 2 describes the approach used in identifying potential human-performance research issues associated with new reactors. Section 3 presents the human-performance issues identified. Section 4 summarizes the issues and their organization into high-level topic areas. The research issues were then evaluated by a group of subject matter experts and prioritized. The evaluation and prioritization methodology and the results are presented in Section 5. A summary of the results and conclusions is provided in Section 6.

This report also has an appendix containing a detailed discussion of the human-system interface (HSI) research issues identified in earlier NRC studies. These HSI issues are summarized in the main body of the report and references to the appendix are provided where appropriate.

Note that a summary of this report is contained in NUREG/CR-6947 (O’Hara et al., 2008).

## 2 METHODOLOGY

### 2.1 Approach

This research was conducted in three Phases. In Phase 1, human-performance issues associated with new reactors and new technology were identified. At present, only a few Generation III reactors are in operation. Information on their operating experience is limited and not generally published in the industry literature. For reactor designs that have yet to be designed and built, information concerning their operations or the design of their control rooms is very limited (especially for reactor concepts for longer-term deployment, i.e., Generation IV designs).

Our approach to identifying potential human-performance research issues related to new reactors was to examine current industry developments and to make projections into the near and longer-term future. It should be noted that as one looks further out in time, the projections become less well defined and less reliable. Industry developments were reviewed from the following perspectives:

- reactor design and technology
- instrumentation and control technology
- human-system integration technology
- human factors engineering (HFE) methods and tools

In Phase II of the research, a framework was developed that organized the issues into seven high-level topic areas: Role of Personnel and Automation, Staffing and Training, Normal Operations Management, Disturbance and Emergency Management, Maintenance and Change Management, Plant Design and Construction, and HFE Methods and Tools.

In Phase III, the issues were evaluated by a group of subject matter experts. The evaluations were then used to prioritize the issues in terms of importance. A detailed discussion of the methodology for this phase is presented in Section 5.

In this report, the research and development pathways to address the topics and issues are not discussed (see O'Hara et al., 2008 for a discussion of the NRC's general approach to review guidance development in addressing human factors and human-performance issues).

### 2.2 Data Sources

A variety of different data sources were used, including existing technical literature, contacts within new reactor R&D organizations, relevant industry workshops, and site visits to control room simulators reflecting the latest technology. Each is briefly described below.

#### Technical Literature

A main source of information came from NRC, DOE, and Electric Power Research Institute (EPRI) reports related to new reactors and new technology. Additional reports were also obtained through conference reports and papers as well as web searches.

## Contacts with Relevant Organizations

Organizations involved in research and development relating to new reactors were contacted via e-mail and/or telephone to obtain pertinent information. A list of the organizations is provided in Table 2-1.

**Table 2-1 Organizations Contacted Regarding New Reactor Work**

<b>Country</b>	<b>Organization</b>
International Organizations	International Atomic Energy Agency (IAEA)
	Organization for Economic Co-operation and Development (OECD)
United States	Idaho National Engineering and Environmental Laboratory (INEEL)
	Oak Ridge National Laboratory (ORNL)
	Electric Power Research Institute (EPRI)
Sweden	Swiss Nuclear Safety Inspectorate (SKI)
	SwedPower
	Linköpings University
Norway	Halden Reactor Project (HRP)
Finland	Technical Research Centre of Finland (VTT)
	Radiation and Nuclear Safety Society (STUK)
Switzerland	Swiss Nuclear Safety Inspectorate (HSK)
United Kingdom (U.K.)	U.K. Safety and Health Executive (HSE)
Spain	Spanish Council for Nuclear Safety (CSN)
France	Electricite de France (EdF)
	Commissariat à l'Energie Atomique.(CEA)
	Institute de Radioprotection et de Surete Nucleaire (IRSN)
Canada	Atomic Energy of Canada, Ltd. (AECL)
Korea	Korea Atomic Energy Research Institute (KAERI)
Japan	Technova, Inc.
	Mitsubishi Heavy Industries

## Industry Workshops

### *DOE Workshop on Instrumentation, Controls and Human-Machine Interface Technology*

The Instrumentation, Controls and Human-Machine Interface (I&C and HMI) Technology Workshop was held in Gaithersburg, Maryland in May 2002. It was sponsored by the DOE's Office of Nuclear Energy, Science, and Technology to solicit input for research planning in support of DOE's Nuclear Power 2010 and Generation IV programs. The need for such a workshop was established during an earlier workshop conducted by the Nuclear Energy Research Advisory Committee (NERAC, 2000).

The goal of the workshop was to identify and examine I&C and human factors considerations for the design of next generation reactors and focused on six major topics:

- Sensors and Measurement Systems
- Diagnostics and Prognostics
- Computational Methods
- Computing and Communications Architectures
- Human-system Interaction
- Regulatory Framework

The results were published in a report by Miller et al. (2002).

*Organization for Economic Co-operation and Development (OECD) Workshop on Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and the Role of Human Factors and Organization*

This workshop was held in Paris, France during October 2003. It was organized by the OECD's Nuclear Energy Agency, specifically the Committee on the Safety of Nuclear Installations (CSNI) and the Institute de Radioprotection et de Sûreté Nucléaire (IRSN). The workshop was a follow-up to a workshop held in Halden, Norway, entitled *Approaches for the Integration of Human Factors into the Upgrading and Refurbishment of Control Rooms* also sponsored by OECD. Both provided information on operating experience with new systems in existing power plants.

Visits to Control Room Simulators Reflecting the Latest Technology

Two visits to advanced control room simulators were made. One was to General Electric's ABWR simulator for the Lungman Plant being fabricated in San Jose, California. The Lungman Plant is the latest ABWR being built in Taiwan.

The second site visit was to the FITNESS (Functional Integrated Treatments for Novative Ecological Support System) simulator. The FITNESS simulator was developed by Electricity de France (EdF) and is located in Septen, France. It is an advanced and innovative human-system interface design for an advanced pressurized water reactor (APWR).



### 3 ISSUE IDENTIFICATION

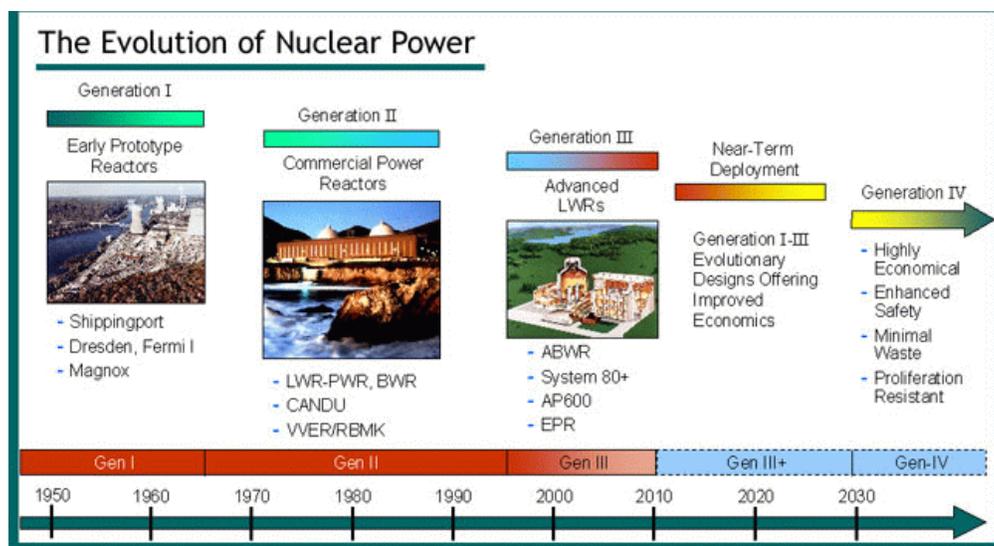
This section discusses issues identified in the areas of:

- New Reactor Designs and Technology
- Digital Instrumentation and Control Technology
- Human-system Integration Technology
- Advances in HFE Methods and Tools

Information contained in this document was current when it was written. However, due to rapid developments occurring in these areas, some specific details may have changed.

#### 3.1 New Reactor Designs and Technology

Commercial NPPs have evolved over several generations of plant designs (see Figure 3-1).



**Figure 3-1 Evolution of Nuclear Power Technology**

(source: U.S. Department of Energy – <http://nuclear.energy.gov/genIV/neGenIV1.html>)

Examining the lessons learned and developments in each of these generations provides an understanding of human performance demands in new plants and the potential issues that may arise. In advancing from one generation to the next, less specific information is available. For example, while the modernization of Generation II plants has been underway for over a decade and important lessons have been learned, Generation IV plants have yet to be fully designed and, consequently, no operational information exists. However, by examining Generation IV concepts and design features, the types of issues that may arise can be anticipated.

### 3.1.1 Generation II Plant Modernization

#### 3.1.1.1 Design Description

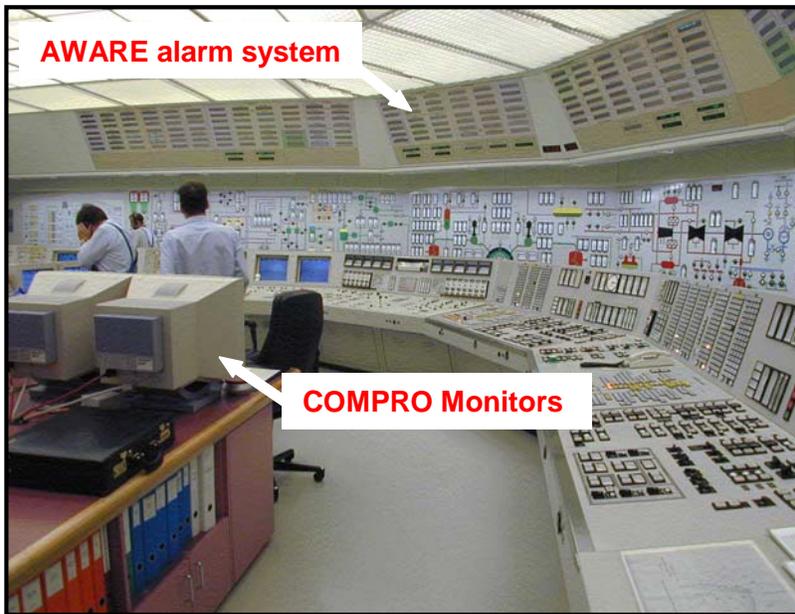
Generation II plants are those that were designed and built from the 1960s through 1990. The current fleet of commercial plants in the U.S. are Generation II boiling water reactors (BWR) and pressurized water reactors (PWR). These plants employ predominantly analog I&C technology. Their HSIs are primarily hardwired controls (e.g., switches, knobs, and handles) and displays (e.g., alarm tiles, gauges, linear scales, and indicator lights) located in the main control room and numerous local control stations throughout the plant. HSIs are also located in support facilities, such as the technical support center.

In recent years, plants have been modernizing their I&C systems and HSIs. There are many reasons for these modernization programs, including:

- To address obsolescence and lack of spare parts
- To meet the need for equipment replacement due to high maintenance cost or lack of vendor support for existing equipment
- To implement new functionality necessary for adding beneficial capabilities
- To improve plant performance, HSI functionality, and reliability
- To enhance operator performance and reliability
- To address the difficulties in finding young professionals with education in, and experience with older analog technology

These modernization programs provide insights that are important to the objectives of this project because the technology used in the modernization is very similar to that used in new reactor designs. Thus, many of the issues encountered in modernization programs are applicable to new reactor designs.

These modifications can affect personnel in various ways. They can impact the role of personnel in; the tasks to be performed, the way their tasks are accomplished, and their knowledge, skills, and training. As part of modernization, HSIs are becoming more computer-based, incorporating features such as soft controls, computer-based procedures, touch-screen interfaces, sit-down workstations, and large-screen overview displays. As computer-based technologies are integrated into control rooms that were largely based on conventional technology, hybrid HSIs are created. Figure 3-2 shows the Beznau control room following a modernization program that resulted in a new computer-based alarm system, graphical plant information system, and computer-based procedure system. In the figure, the new alarm system and dual monitors for the procedure system can be seen (see Roth & O'Hara, 2002, for additional details about the systems involved in the Beznau modernization program).



**Figure 3-2 Hybrid Control Room**  
(photo of Beznau control room, courtesy of Nordostschweizerische Kraftwerke AG, NOK, in Switzerland)

The potential benefits of modernization are compelling and can result in more efficient operations and maintenance. The potential benefits also include increased efficiency and power output, as well as reduced operating costs. Implementing new digital systems provides the opportunity to give personnel information they did not have with conventional systems. Improved instrumentation and signal validation techniques can help ensure that the information is more accurate, precise, and reliable. In addition, data processing techniques and the flexibility of computer-based information presentation enable designers to organize information in ways that are much better suited to personnel tasks and information processing needs.

It is also important to recognize that, if poorly designed and implemented, there is the potential to negatively impact performance, increase errors, and reduce human reliability, which will produce a detrimental effect on safety and cost-effective power production.

Modernization programs provide insights into crew performance with key features of new reactors, i.e., computer-based HSIs and digital I&C systems. Thus, the lessons learned in this context may be applicable to future plants. Potential issues that have been encountered in the introduction of digital I&C and computer-based HSIs are summarized in the next section.

### *3.1.1.2 Potential Issues*

NRC research on plant modernization focused on the impact of technology change on human performance (O'Hara et al., 1996; O'Hara, 2004).<sup>4</sup> The following main issues were identified:

<sup>4</sup> Note that plant experience related to digital I&C technology itself and associated issues are described in NUREG/CR-6842 (Wood et. al, 2003).

- Personnel Acceptance of the Technology
- HSI Design Deficiencies
- Unanticipated Impact of Technology
- Increase in Complexity and Opacity
- Understanding How HSIs are Really Used
- Change in the HSI Demands and Training Requirements
- Knowledge Gap Between the Licensee Organizations and Suppliers

### Personnel Acceptance of Technology

When new technology is initially introduced, plant personnel do not always embrace it. There is a familiarization curve for crew acceptance. Many control rooms have remained relatively unchanged, except for minor improvements and modifications, for decades. Over the years, through training and experience, crew members develop expert knowledge and skills for monitoring and operating the plant with the HSIs provided. When faced with the prospect of significant changes, some crew members are reluctant to accept new technology. In some plants this has led some personnel to retire or request new assignments. It can be expected that during this period of familiarization, the potential for errors will increase, due to both a lack of understanding for how the new HSIs should be used and negative transfer of training, i.e., when behavior associated with the old HSIs makes it more difficult to learn to use the new HSIs. However, after training with the new HSIs and an initial period of familiarization, personnel generally do not want to return to the old technology.

While operators of new plants may not necessarily be dealing with a change in technology from analog to digital (although this situation may arise for near-term deployment of new reactors), they are likely to be faced with a change from the HSIs in their previous plant to those of a new plant. Thus, issues associated with negative impacts on safety due to the learning curve effects need to be addressed.

### HSI Design Deficiencies

There is a tendency to believe that because a design employs new technology, it is well designed. However, one lesson learned from plant modernization is that this is not necessarily the case. Some examples of this include:

- data overload; i.e., from too much data and too many alarms
- the organization of information in the computer-based system makes operational tasks more difficult
- high interface management demands are created (i.e., a greater cognitive workload), increasing the time required to work with and manage the HSIs (O'Hara & Brown, 2002)

These types of problems can be attributed to specific design characteristics of computer-based interfaces, such as a limited display area, serial access to the HSIs, navigation elements, and HSI flexibility. Sometimes, when the problems of data overload and interface management arise, personnel feel that they do not have sufficient display area to look at information simultaneously (i.e., too few monitors).

Thus, it will be important for new designs to ensure that appropriate HFE processes are applied to ensure that designs meet personnel task requirements, performance demands, and are well designed from the standpoint of human cognitive and physical characteristics. NRC review methods and criteria will have to keep pace with these advances in HSI designs.

### Unanticipated Impact of Technology

New technology can have unanticipated consequences for team and individual performance (Kazak & Malcolm, 2004; Whitsitt, 2004). While some changes in the plant have relatively obvious effects, such as the creation of new tasks that have to be performed, other changes are more subtle. For example, while at a high-level a task may be unchanged, e.g., the operator has to align a system, at a more detailed level, the way the task is performed may be very different, e.g., a series of displays have to be retrieved from a computer system and the operator uses on-screen "soft controls" to perform the alignment. To crew members accustomed to manipulating switches on a control board, this new type of operation is very different. Perhaps more significantly, the new systems may result in modified task demands, e.g., the amount of time available to perform a task is reduced. Thus, crew personnel perform tasks can be changed by plant modifications in subtle ways.

Even with good HFE design and evaluation methods, it can be difficult to anticipate all the effects that technology may have. With the extent of technology changes anticipated in future plants, improved methods to identify technology impacts will be needed, especially those that are not anticipated.

An example of the unintended consequences of technology was reported by Roth and O'Hara (2002) and is summarized in Table 3-1. As new reactor designs may rely on many new and novel technologies, unanticipated impacts on human performance may have safety significance.

**Table 3-1 Example of the Impact of Technology on Teamwork**

As part of one utility's digital I&C upgrade, a computer-based emergency operating procedures (EOPs) system was installed. Prior to the upgrade, EOP use was an activity that involved the entire control room crew. The supervisor read the procedure and made decisions at each step as to how to proceed. The operators retrieved the needed data for each procedure step and communicated it to the supervisor. At the supervisor's instruction, they would take any required actions. This required a lot of communication and coordination.

The computer-based procedures (CBP) significantly changed this activity. It performed many of the tasks that formerly the crew members did, including:

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

As a result, workload was greatly reduced and procedure use became a one-person activity. The operators were far less engaged in EOP use, except to take occasional control actions. The operators felt they were out of the loop, had lost situation awareness of EOP activities, and were not sure what to do. Team cohesiveness was lessened at a critical time (when plant circumstances require EOP use).

The situation was addressed by the operations and training departments. The roles and responsibilities of the individual crew members were redefined and steps to foster teamwork were put in place. First, operators were to manage alarms and check key parameters on their side of the plant (reactor and balance of plant). Then, specific stop points were added into the procedure where the supervisor updated the operators on the procedure status and the crew shared their assessments and informed the supervisor of key findings. Because the shift supervisor and operators worked more independently and attended to separate sources of information, this provided the opportunity to keep each other informed and to ensure a common understanding between crew members. It also provided better situation awareness for each of the individual crew members, thus providing more people who were actively involved in evaluating plant status and who could provide valuable input at critical times. EOP training was then used to reinforce this new approach to emergency management.

### Increase in Complexity and Opacity

One of the recurrent themes that cut across many of the issues identified here is that of complexity. While the reactor designs, in some ways, are seeking greater simplicity, the HFE aspects of the plant are likely to be more complex than in today's plants. Increases in sensing capabilities, information processing support, intelligent agents, automation, and software mediated interfaces that distance personnel from the plant itself are all potentially beneficial, but add to complexity for the crew members.

In general, computer-based systems add to the overall complexity of the plant. Operating crews can have difficulty understanding what the computer system is doing. Often lower-level data is processed into higher-level information that might be depicted as synthetic variables or

graphics. While this is done to help personnel by providing higher-level information, it can also make it more difficult to understand because of the processing done on the data and what is presented to personnel. One contributing factor is that the behavior of computer-based systems is often not sufficiently observable and the means provided by the HSI for personnel to communicate with computer-based systems are often inadequate. Further, computer systems can produce incomplete or inaccurate solutions. Therefore, operating crews must know the appropriate uses and limitations of such systems. This may be the case with future systems as well. As the computer-based systems incorporate more automation and intelligence, the complexity factor may increase.

Complexity was also identified as an issue in a recent survey of experience at several new reactor sites (Wood et al., 2003).

One important aspect of this issue is that little is known about the underlying factors that make a plant, system(s) HSI, scenario, task, or operation complex to plant personnel. If complexity were better understood, then a measure of complexity could be developed and used as part of a safety evaluation. Such a measure may take several forms depending on the level of design detail available.

#### Understanding How HSIs are Really Used

Plant personnel sometimes do not use HSIs in the manner expected by designers. For example, computer-based control rooms are designed with vast amounts of data, which is available through hundreds, and sometimes thousands, of displays. This data is viewed by the operator through a limited number of video display units (VDUs); thus, only a small amount of information is presented at any one time. Designers expect that operators will use the flexibility of the computer-based interfaces to configure the HSI in a way that will address the specific task at hand. Interface management facilities must be used to exercise that flexibility. However, if operators opt not to do so, then a very significant question can be raised: What is the effect of failing to perform interface management tasks on primary task performance and plant safety? The implication of adopting such a workload management strategy may be that performance becomes data-limited, i.e., information necessary for task performance may be missed, operators could lose situation awareness, errors can be made, and plant safety may be reduced (O'Hara & Brown, 2002).

In such situations, operators adopt numerous strategies to create workarounds and aids to compensate for limitations in designs (O'Hara & Brown, 2002). These strategies help manage workload and have the general effect of decreasing system flexibility, increasing predictability, and increasing simplicity. The strategies help operators to apply the technology to their task environment in locally pragmatic ways (Woods et al., 1994; Cook & Woods, 1996).

An important aspect of performing safety reviews will be to establish a realistic view as to how HSIs will be used and a recognition that the designer's vision may not fully characterize the human-performance issues that may be encountered.

## Change in HSI Demands and Training Requirements

In today's plants, detailed operation of the HSI is often learned on the job. This is because the HSIs themselves, such as gauges, J-handles, and push buttons, are relatively simple devices with limited flexibility. However, in computer-based control rooms, more time may have to be devoted to the use of the HSIs in formal personnel training because of their added flexibility and complexity. Personnel will need to know how data is processed, how system modes affect user inputs, and the strategies needed to manage the interface (e.g., information access, navigation, and workstation configuration). In training programs for future systems, it may be important that HSI features, functions, and use are an integral part of personnel training.

Another training-related issue in modernization programs is the coordination of design activities, implementation of upgrades, simulator modifications, and ongoing training. This challenge is even greater for multi-outage modernization programs at multi-unit sites. In the U.S. for instance, plants are unlikely to shut down for the extended periods required to make all modifications. Thus, over many outages, modifications may be made resulting in interim configurations that lie between the starting design and their endpoint vision. Each of the interim configurations has to be addressed in training. While new plant designs do not have all the coordination issues described above, the availability and timing of simulation capability to support design, evaluation, and training is still an issue.

## Knowledge Gap Between Licensee Organization and Supplier

The initial knowledge gap regarding digital- and computer-based technology between a licensee in the beginning stages of an I&C/HSI modernization program and their vendor/supplier has been a significant issue in many plants (Forsberg, 2004; Gunnarsson & Farbrot, 2004; Harmon & Kerch, 2004). Misunderstandings can arise between what a licensee requests, and how vendors interpret their requests. As the licensee gains knowledge and familiarity with the new digital technology, they frequently recognize that modifications to their plans are needed, often at additional cost.

This is also a potential issue for licensee organizations (combined license applicants) seeking to build new plants. In addition to digital I&C and HSIs, the licensee organization may also have to deal with different reactor technologies. An existing nuclear licensee may be familiar with LWR technology, so an adjustment may have to be made when dealing with a different technology, such as gas/graphite technology for a modular, pebble bed design.

### **3.1.2 Generation III Reactor Designs**

Several Generation III plants, such as the ABWR, have been built and are operating in different countries outside of the U.S. In general, Generation III designs differ most significantly from Generation II plant designs in the amount and complexity of the digital I&C employed and in the design of the control room. The extent of software processing of information is much greater than in earlier generation reactors, and operating crews work at seated workstations (rather than large control boards) in a fully computerized 'glass-cockpit' environment.

Generation III+ plants (shown in Figure 3-1 as near-term deployment designs) are improvements to the current fleet of Generation III plants. The III+ designs make more extensive use of digital technology than the Generation III designs. The most significant change is that the

reactor designs being considered for near-term deployment include novel design features such as passive safety systems and small modularized reactors.

Design features and characteristics are described below for selected Generation III reactor designs. Following the description, the implications of design features and characteristics for human performance are discussed. The designs selected for discussion are those that are candidates for near-term deployment in the U.S. (see Table 3-2). Key sources of information and reactor descriptions contributing to this section include: DOE (2002a), DOE (2002b), DOE (2003), Risk and Safety Technical Working Group (2002), and new reactor descriptions found on the internet.

### **Table 3-2 Reactor Designs for Near-term Deployment**

#### **U.S. Near-term Deployment (2010)**

(Discussed in Section 3.1.2.1)

- ABWR (Advanced Boiling Water Reactor)
- AP1000 (Advanced Plant 1000)
- ESBWR (Economic Simplified Boiling Water Reactor)
- GT-MHR (Gas Turbine-Modular High Temperature Reactor)
- PBMR (Pebble Bed Modular Reactor)
- SWR-1000 (Siedewasser Reactor-1000)
- EPR (Evolutionary Pressurized Water Reactor)

#### **European Near-Term Deployment (2015)**

##### Advanced Boiling Water Reactors

- ABWR II (Advanced Boiling Water Reactor II)
- ESBWR (European Simplified Boiling Water Reactor)
- HC-BWR (High Conversion Boiling Water Reactor)
- SWR-1000 (Siedewasser Reactor-1000)

##### Advanced Pressure Tube Reactor

- ACR-700 (Advanced CANDU Reactor 700)
- Advanced Pressurized Water Reactors
- AP600 (Advanced Pressurized Water Reactor 600)
- AP1000 (Advanced Pressurized Water Reactor 1000)
- APR1400 (Advanced Power Reactor 1400)
- APWR+ (Advanced Pressurized Water Reactor Plus)
- EPR (Evolutionary Pressurized Water Reactor)

##### Integral Primary System Reactors

- CAREM (Central Argentina de Elementos Modulares)
- IMR (International Modular Reactor)
- IRIS (International Reactor Innovative and Secure)
- SMART (System-integrated Modular Advanced Reactor)

##### Modular High Temperature Gas-Cooled Reactors

- GT-MHR (Gas Turbine-Modular High Temperature Reactor)
- PBMR (Pebble Bed Modular Reactor)

### 3.1.2.1 Design Descriptions

#### ABWR (Advanced Boiling Water Reactor)

The ABWR has received design certification (DC) from NRC under Title 10 of the Code of Federal Regulations (10 CFR) Part 52. Two ABWRs are operating in Japan, and four are under construction, two in Taiwan and two in Japan. While the ABWR design is usually associated in the United States with General Electric, the two units now being built in Japan are products of Toshiba and Hitachi. All three vendors (General Electric, Toshiba, and Hitachi) have shown an interest in building ABWRs in the U.S. There are many variations in ABWR design, especially in the 1250-1500 megawatts electric (MWe) capacity range.

The ABWR building volume is about 70 percent of the current BWRs, making it a more compact design. The ABWR has 10 recirculation pumps that are internal to the reactor vessel. The main safety systems consist of: three trains of low pressure core flood which are used for residual heat removal (RHR), two trains of high pressure core spray (HPCS), one train of reactor core isolation cooling (RCIC), standby liquid control (SLC), and an automatic depressurization system. These systems are not very different from current BWR designs, except in BWRs, the control rod drives are hydraulic, while in the ABWR, they are electro-hydraulic. Having an additional drive mechanism capability reduces the probability of failure, but increases the system complexity. The ABWR has a passive containment flooding system to dump suppression pool water on the building floor in the event of a severe "core on the floor" accident. It also has a passive containment vent system using rupture discs that prevent catastrophic failure of containment and ensuring fission product scrubbing through the suppression pool.

The ABWR, as certified by the NRC for use in the U.S., did not have a detailed HSI design, but the Design Control Document (DCD) outlined a number of standard features that would be utilized when a plant was ordered. These standard features include:

- use of a single integrated control console staffed by two operators (see Figure 3-3)
- use of the plant process computer and on-screen monitoring for safety systems and both control and monitoring for non-safety systems
- use of a Class 1E computer to drive VDUs for safety system control and monitoring
- incorporation of operator-selectable automation of pre-defined plant operational sequences
- use of a large overview display panel
- incorporation of safety-parameter display system (SPDS) information onto a large overview display
- use of fixed position displays for certain important parameters
- incorporation of a supervisor's monitoring panel that contains all the screens available to the operators
- presentation of alarms on fixed position alarm tiles on a large display panel and on VDUs
- inclusion of alarm prioritization and filtering

- installation of a minimum inventory of controls, displays and alarms to be used for emergency procedure guideline (EPG) implementation that would be installed on fixed positions in the control room (CR)



**Figure 3-3 ABWR Control Room**  
(photo of the ABWR in Japan, courtesy of Tokyo Electric Power Co.)

#### AP1000 (Advanced Pressurized Water Reactor 1000)

Both the AP1000 and the AP600 have received Design Certification under 10 CFR Part 52. The Westinghouse designed AP1000 is a PWR with passive safety features and a simplified design compared to current PWRs. The plant is a larger version the AP600 plant. The two-loop configuration can produce over 1000 MWe. The AP1000 design uses passive safety systems that use forces such as gravity and natural circulation. No pumps, fans, diesels, chillers, or other rotating machinery are used in the passive safety sub-systems. The passive safety systems include passive safety injection, passive residual heat removal, and passive containment cooling.

The AP1000 will have a compact CR designed for one operator and one supervisor. Additional features planned for the CR are: a large overview display panel, workstation VDUs with computer based displays and soft controls, a small number of fixed position dedicated controls and displays, advanced alarm processing, and computer-based procedures.

#### ESBWR (Economic Simplified Boiling Water Reactor)<sup>5</sup>

The ESBWR is a new simplified BWR design by General Electric. It was submitted for NRC design certification review in August 2005. The ESBWR is based on several earlier design ideas, including the ABWR, Simplified Boiling Water Reactor (SBWR), and the European

<sup>5</sup> In many reports this design is also referred to as the European Simplified BWR.

SBWR. Its passive safety features include: accumulator driven scram system, accumulator driven backup boron injection system, isolation condenser, depressurization and gravity driven cooling system (GDCCS), suppression pool, and passive containment cooling.

The ESBWR is a boiling water reactor with a pressure suppression type primary containment and the reactor building functioning as the secondary containment. This design meets the single failure criterion. No safety related support systems are needed except DC power.

The reactor vessel (RV) is designed with an increased internal flow path length using a long “chimney” that aids natural circulation. There are no recirculation pumps and natural circulation provides all flow. The large RV volume provides a long time before the core is uncovered after loss of feed water (LOFW) or loss of coolant accident (LOCA) initiating events. The large RV volume also reduces reactor pressurization rates and limits safety relief valve (SRV) actuations. The RV has a head vent for non-condensable gases.

The control system and control room design will have evolved from that of the ABWR at Lungmen, Taiwan. No immediate operator action is needed for design basis accidents. The standard design features of the ESBWR control room are:

- a single, integrated control console staffed by two operators
- computer system driven on-screen control VDUs for safety-related system monitoring and non-safety-related system control and monitoring
- a set of on-screen control VDUs for safety-related system control and monitoring, called the Essential Distributed Control and Information System (DCIS), and separate on-screen control VDUs for non-safety-related system control and monitoring, called the Non-Essential DCIS. The operation of these two sets of VDUs is independent. Further, the first set of VDUs and all equipment associated with their safety-related system control and monitoring functions are divisionally separated and qualified to Class 1E standards.
- dedicated function switches on the control console
- operator selectable automation of pre-defined plant operation sequences
- an operator selectable semi-automated mode of plant operations, which provides procedural guidance on the main control console VDUs but does not control plant systems and equipment
- the capability to conduct all plant operations in an operator manual mode
- a large display panel that presents information for use by the entire control room operating staff
- a large display panel of fixed-position displays of key plant parameters and major equipment status
- fixed-position displays of both Class1E-qualified and non-1E display elements
- independent fixed-position displays from the Non-Essential DCIS
- a large VDU within the large display panel
- a “monitoring only” supervisor’s console

- the continuous display of the SPDS function on the fixed-position displays on the large display panel
- a spatial arrangement between the large display panel, the main control console and the shift supervisor's console, which allows the entire control room operating crew to conveniently view the information presented on the large display panel
- fixed-position alarm tiles on the large display panel
- the application of alarm processing logic to prioritize alarm indications and to filter unnecessary alarms
- VDUs to provide alarm information in addition to the alarm information provided through the fixed-position alarm tiles on the large display panel

### GT-MHR (Gas Turbine-Modular High Temperature Reactor)

The General Atomic GT-MHR is a High-temperature, Gas-cooled Reactor (HTGR) design. It is a modular plant with a capacity of 600 megawatts thermal (MWth), or about 300MWe. Plans exist to use GT-MHRs in Russia to burn surplus plutonium supplies. For commercial power reactor applications, the design would use uranium based-fuels enriched to as high as 19.9 percent U-235 content; thus, below the 20 percent level of highly enriched uranium. In initial designs, the conversion of the energy in the heated Helium coolant to electricity would be performed directly in a gas turbine.

The GT-MHR is designed such that it will not meltdown, even with a total loss of coolant. The reactor's low power density and geometry assure that decay heat will be dissipated passively by conduction and radiation without ever reaching a temperature that can threaten the integrity of the ceramic-coated fuel particles. The advanced gas turbine technology planned will improve thermal efficiency from the mid 30 percent of current NPPs to nearly 50 percent.

Both the reactor and the power production module are designed to be located below ground level. There is no need for active systems in the event of subsystem failure. The GT-MHR has two active, diverse heat removal systems, the power conversion system, and a shutdown cooling system that can be used to remove decay heat. In the event that neither of these active systems is available, an independent passive means is provided to remove core decay heat. The reactor cavity cooling system (RCCS) surrounding the reactor vessel provides sufficient cooling to keep radionuclides contained within the refractory coated fuel particles without the need for active safety systems or operator intervention.

Because coolant temperatures in HTGR-type reactors are much higher than in LWRs, the design can be used as a commercial heat source, e.g., as a non-polluting method to produce hydrogen or be used for industrial process heat applications.

### PBMR (Pebble Bed Modular Reactor)

The PBMR is a small HTGR reactor (around 165 MWe) that uses more highly enriched uranium than is presently used in LWR designs. The PBMR is a helium-cooled, graphite-moderated high-temperature reactor. Helium is used as both the coolant and the energy transfer medium to a closed cycle gas turbine and generator.

The PBMR consists of a vertical steel pressure vessel, lined with a layer of graphite bricks. This graphite layer serves as an outer reflector for the neutrons generated by the nuclear reaction and as a passive heat transfer medium. This graphite reflector encloses the reactor core. When fully loaded, the core would contain 456,000 fuel spheres (pebbles). Each sphere consists of coated uranium particles encased in graphite to form a fuel sphere (60 mm in diameter or about the size of a tennis ball). The geometry of the fuel region is annular and located around a central graphite column that serves as an additional nuclear reflector. The nuclear reaction takes place in the fuel annulus. Helium flows through the pebble bed core and removes the heat generated by the nuclear reaction. This helium is the same gas that is used as the working fluid in the power conversion unit; hence, the PBMR is a direct gas cycle.

The main barrier to release of radioactivity is the graphite in the fuel sphere and the silicon carbide coating. Considering the very large number of fuel spheres making up the core, it will be necessary to ensure adequate quality is manufactured into all fuel spheres to have a high confidence in the performance of this important barrier.

Planned plant availability is higher due to the continuous refueling scheme used. This scheme also ensures there is never a large amount of excess reactivity within the core. Continuous removal of spent fuel is completely automated, with subsequent fuel handling via an automated pneumatic system.

The vendors maintain that no physical process is capable of producing a radiation hazard outside the site boundary. The PBMR does not require any of the traditional nuclear safety systems that actively protect current generation reactors against radiation release.

Other safety features include:

- the use of stable graphite as a moderator
- the use of Helium as coolant (Helium remains in a gas phase, so there is no change in thermal hydraulic properties, and Helium has a low neutron cross section, which means no change in reactivity due to the presence of the reactor coolant)
- the existence of a low core power density and good thermal conductivity of graphite (which means cooling is passively assured and temperatures are acceptable even on loss of all forced cooling)
- the lack of or need for early insertion of control rods is not needed in any accident

Operators control multiple PBMR reactor modules from a single computer-based control room. The PBMR is designed specifically for load-following operation within specified limits. This means that the amount of electrical power output can be varied to match the current power demand. This is different than a typical base-load NPP. Also, the PBMR can withstand a 100% load rejection without a reactor trip, which adds stability and reduces transients that contribute to risk.

Its small size may have been viewed as a regulatory disadvantage because most former licensing regulations required separate licenses for each unit at a site. If each PBMR module at a site were licensed separately, additional regulatory activity would be required.

## SWR-1000 (Siedewasser Reactor-1000)

Siedewasser Reactor is German for boiling water reactor. The SWR-1000 is a Framatome ANP (FANP) design for an advanced BWR. The reactor's passive safety features include:

- increased water inventory in the reactor pressure vessel
- core flooding pools inside the containment
- emergency condensers within the core flooding pools
- a water inventory in a shielding/storage pool above the containment, permitting heat removal from the containment for 3 days without makeup water

Should a severe accident occur, the core material would be retained inside the reactor pressure vessel (RPV) by cooling the RPV exterior. For this purpose, the bottom of the drywell is flooded using water from the core flooding pools. Also, the containment atmosphere is injected with nitrogen to prevent hydrogen combustion. Passive heat removal from the containment is ensured via the containment cooling condensers. Additionally, the SWR-1000 uses passive pressure pulse transmitters that are small heat exchangers that operate on the same principle as the emergency condensers. Upon a drop in reactor water level, pressure builds up on their secondary sides. This pressure is then used to activate safety functions, without any need for signals from the reactor protection system.

## Evolutionary Pressurized Water Reactor (EPR)<sup>6</sup>

The EPR is a 1600 MWe 4-loop evolutionary PWR, developed by FANP, which incorporates a combination of technologies from the French N4 and the German KONVOI (late model PWR) reactors. As of the writing of this document, the EPR is undergoing pre-application review by the NRC with the expectation of a submittal for design certification and a combined license (CCL). One EPR, called the European Pressurized Water Reactor, is being installed in Finland. Areva announced plans to seek design certification under 10 CFR 52 for a US version of the EPR called the Evolutionary Pressurized Water Reactor. The reactor containment building has two walls, an inner pre-stressed concrete housing and an outer reinforced concrete shell, both 1.3 meters thick. In a core meltdown event, there is an area inside the containment where the molten core will be collected, retained, and cooled.

The major safety systems comprise four independent sub-systems or "trains" with each train being capable of performing the complete safety function and located in a separate Safeguards Building. The design includes increased grace periods for operator actions by designing components (e.g. pressurizer and steam generators) with larger water inventories to limit transients. The major safety systems are an in-containment refueling water storage tank (IRWST), accumulators for injection, medium head safety injection (MHSI), Low Head Safety Injection (LHSI), emergency feed water system (EFWS), and an extra borating system (EBS) for anticipated transient without scram (ATWS) mitigation. These systems are more typical of current generation active safety systems rather than the new passive safety systems used in some new reactor designs.

---

<sup>6</sup> In many reports this design is also referred to as the European PWR.

The plant is operated from the control room where all operating data is centralized. The control room is located in one of the four safeguards buildings and is totally computerized, having the most up-to-date digital technology, giving operators full control over all parameters important to plant operation. The optimized human-systems interface is less sensitive to human errors.

The EPR design incorporates the French concept for the next generation of nuclear power plants; namely, that there must be “no need for emergency evacuation outside the immediate vicinity of the plant, only limited sheltering, and no long-term restrictions in the consumption of food,” even in the case of a core melt accident. However, due to the high projected power rating and the resulting narrow margins, the EPR’s designers dismissed in-vessel melt retention by outside vessel cooling. Instead, an ex-vessel strategy is used to avoid a molten core attack on the structure concrete. The key feature, called a “core spreader”, mitigates the interaction between the melted core and the concrete and prevents basemat penetration. Much of the melted core control is passive, but active cooling systems also are involved, e. g., the Severe Accident Heat Removal System (SAHRS).

The EPR core design (with a thermal power of 4250 MW) consists mainly of UO<sub>2</sub> fuel but has a capacity for mixed oxide (plutonium/uranium nuclear fuel) (MOX) recycling of 50%.

#### *3.1.2.2 Potential Issues*

The design characteristics with potential implications for human performance are summarized in Table 3-3 for the six U.S. near-term deployment designs.

The main issues identified were:

- Passive Safety Systems
- Modular Construction
- Modular Plants
- Continuous Fueling
- Graphite Cores
- Increased Power Operations
- Post-core-melt Mitigation
- Availability of Operating Experience of Generation III Reactors

As noted earlier, these six near-term new plants will rely mainly on digital I&C systems and fully computerized control rooms. However, since the implications of I&C and HSI technology trends are discussed in detail in Sections 3.2 and 3.3, respectively, they will not be addressed in this section.

**Table 3-3 Design Characteristics for Near-term Reactor Designs With Potential Human-performance Issues**

Design Characteristics with Possible Human Performance Issues	Reactor Types						
	ABWR	AP 1000	ESBWR	GT-MHR	PBMR	SWR-1000	EPR
Passive systems	x	x	x	x	x	x	x
Modular plants				x	x		
Modular construction	x	x	x	x	x		
Continuous fueling					x		
Graphite core				x	x		
Increased power operations	x		x				x
Post-core-melt mitigation							x

Passive Safety Systems

Supporting emergency management, many new reactor designs have passive safety systems. Since they depend on physical processes, they are not as amenable to routine testing as active systems. Thus, operators may not become as familiar with their use as they are with current generation active systems. They may not know from actual operational experience how to verify their proper automatic initiation and operation when they are called upon to perform in a real event. For example, there may not be the same initiation signals to start systems that can be observed. The flow rates and temperatures may be much lower and perhaps not as easily verified. The operational aspects of monitoring and verification of passive system success will need to be defined along with any operator actions necessary to initiate or back up passive systems should they fail to operate as designed.

Modular Construction

In the past, plant personnel have participated in the onsite construction, component level testing of installed components, and pre-operational testing of completed systems. This provided the personnel with a thorough knowledge of plant structures, systems, and components. Fabrication of plants at factory locations rather than the site may limit plant personnel's knowledge of systems and components. The implications of this approach from a safety perspective are not known.

Modular Plants

In this context, modular plants refer to a number of small reactors that are operated from a common control room and which may share common infrastructure and resources. These plants may be in a variety of states (e.g., shutdown, startup, and standby) or operating at

various power levels. Multi-module operations may be very different from today's single reactor operations and the safety implications and issues will need to be better understood. Regarding control of modular units, Wood et al. (2003) noted:

The challenge is to address operability issues of the shared and common systems when the first module is declared operational and the follow-on modules are still under construction. Because of the advances in I&C technology, common data networks that transmit and utilize large amounts of information will serve as integrated data links rather than the traditional direct point-to-point wiring. Thus, the control and monitoring operations of these modules must be fully operational and not susceptible to interference from construction and testing activities in the non-operational modules. Research is needed to address basic guidelines that may include modifications to the data highway and control room design to optimize the construction sequencing. This may result in a control room that is less optimal for human factors at all levels than would otherwise be possible if all the modules simultaneously completed construction. In addition to licensed operation, an option to consider is the use of a dedicated commissioning room in which a module would be commissioned and then "transferred" to the shared control room. (p. 59)

Modular plants may create additional opportunities for the "wrong unit/train" errors that have been noted persistently over the years at dual unit NPP sites.

### Continuous Fueling

Although continuous fueling may share some features with on-line refueling (as in CANada Deuterium Uranium (CANDU) designs), it is a new and less familiar concept in the U.S. The need to manage this concurrent activity while the plant is operating will have to be taken into account in the plant's concept of operations; and, therefore, in its approach to staffing, function allocation, and task design.

### Graphite Cores

Under some circumstances, graphite cores are flammable and could create radiologically hazardous fumes. Guarding against these hazards may involve additional safety procedures and monitoring systems for which safety review may be needed.

### Increased Power Operations

Some near-term deployment designs produce more power than today's plants. They have more and/or larger equipment and may, therefore, operate closer to threshold limits. This phenomenon has been seen in some BWR reactor vessel internals as a result of power upgrades in the current fleet of nuclear power plants. Such designs could place higher demands on operators to ensure that equipment performs properly and that parameters are maintained within their specified limits.

### Post-core-melt Mitigation

One aspect of accident management that has received increased attention after Three Mile Island (TMI) is the behavior of the melted core material after all efforts to prevent core damage fail. Activities addressing this issue include modeling, training, procedures, accident management strategies, emergency planning, and design improvements. Notable among the new reactor designs is the EPR strategy to avoid the need for emergency evacuation outside

the immediate vicinity of the plant. This is accomplished by designing advanced mitigating systems for managing a damaged core. Some of these systems are passive, but others are active and rely on operator monitoring and actions. Operator actions at this stage of a severe accident may raise new human-performance issues. This operation will certainly be outside the operational experience of current plants and may need new and better simulation capabilities.

### Availability of Operating Experience of Generation III Reactors

An additional issue not related to specific reactor design characteristics is the need for operating experience of Generation III reactor designs and the lessons learned that can be derived from it. While a number of these plants have been operating outside the US for many years, (e.g., ABWRs in Japan, the Advanced Gas Cooled Reactor (Sizewell B) in the United Kingdom (U.K.), and the N4 in France) very little information is available pertaining to their actual operating experience. One exception is the report by Wood, et al. (2003) related primarily to I&C issues.

This information is very important to the development of future research and as an input to the development of regulatory approaches for the safety review of new technology. Operating experience should be obtained from vendors, utilities, and regulatory authorities. It should address a broad range of topics that reflect the HFE aspects of the plant, including:

- types of automation implemented
- user interfaces to automation
- user interfaces to plant monitoring and disturbance management
- soft control of equipment
- computer-based procedures and computerized operator support aids
- task performance such as maintenance, equipment tagout, and testing using computer-based interfaces
- management of software upgrades and modifications
- operator-modifiable features, such as setpoint adjustment, temporary alarms, and temporary displays
- digital safety systems
- training technology
- approaches to assuring system security
- experience with events
- identification and treatment of risk-important personnel actions
- regulatory strategies for design review

### **3.1.3 Generation IV Reactor Designs**

The international nuclear industry is looking ahead to the development of new reactor design concepts to meet energy needs thirty years from now and beyond. This has been called the Generation IV initiative (see Figure 3-1). The vision for Generation IV plant designs includes ambitious goals (discussed below).

To meet these goals, new and innovative approaches will be needed to the human interaction with the plant (Miller et al. 2002). In all likelihood, this will lead to significant changes in the concept of operations, including:

- the relative roles of human and automation in plant monitoring and control
- the design of HSI
- the tools provided for personnel to plan tasks, interact with each other, and conduct their operational evolutions.

An important aspect of human-system interaction will be the use of advanced I&C technologies that will emerge as Generation IV technology develops (see Section 3.2 for a discussion of I&C technology).

While the precise implications of Generation IV reactor technology for human performance and safety are yet unknown, it is possible to infer some general considerations based on the goals and design features of candidate designs.

Key sources of information contributing to this section include: DOE (2002a), DOE (2002b), DOE (2003), and Risk and Safety Technical Working Group (2002).

### 3.1.3.1 Generation IV Design Goals

Challenging technology goals for Generation IV nuclear energy systems have been defined in the Generation IV roadmap (DOE, 2002b). Table 3-4 summarizes these goals. By striving to meet the technology goals, new nuclear systems are expected to achieve long-term benefits that may increase the role of nuclear energy worldwide. There may also be potential human performance considerations associated with meeting these goals. Any issues that may be associated with these goals apply to all Generation IV designs.

**Table 3-4 Generation IV Reactor Design Goals**

<b>Goal</b>	<b>Key Attributes</b>
Sustainability	<ul style="list-style-type: none"> <li>• provide sustainable energy generation that meets clean air objectives and promotes long-term availability of systems and effective fuel utilization for worldwide energy production</li> <li>• minimize and manage their nuclear waste and notably reduce the long-term stewardship burden; thereby, improving protection for the public health and the environment</li> </ul>
Economics	<ul style="list-style-type: none"> <li>• a clear life-cycle cost advantage over other energy sources (includes as sub-goals both construction and production costs)</li> <li>• a level of financial risk comparable to other energy projects (includes as sub-goals construction costs and duration)</li> </ul>
Safety and Reliability	<ul style="list-style-type: none"> <li>• excel in safety and reliability</li> <li>• very-low likelihood and degree of reactor core damage</li> <li>• eliminate the need for offsite emergency response</li> </ul>
Physical Protection	<ul style="list-style-type: none"> <li>• increase the assurance that they are a very unattractive and the least desirable route for diversion or theft of weapons-usable materials, and provide increased physical protection against acts of terrorism</li> </ul>

### 3.1.3.2 *Potential Human-performance Issues Related to Generation IV Goals*

The main issues identified were:

- Managing Human Error in Operations and Maintenance
- Managing Design and Construction Errors
- Simplified Maintenance Practices
- Reduced Staffing
- Quantitative Human Performance Criteria
- Physical Protection, Security, and Safety

#### Managing Human Error in Operations and Maintenance

To meet the Generation IV design goals for economy and safety/reliability during the production phase of plant lifetime, designs have to minimize human errors and consequent equipment failures that lead to unplanned outages and added repair costs. Insofar as plant safety and reliability depend on the reliability of human behavior, there may be implications for many aspects of human performance (e.g., function allocation, task analysis, staffing and qualifications, interface design, procedure design, training). In particular, designs may incorporate error tolerance features to minimize human errors and the consequences of any errors that occur (see O'Hara, Stubler, & Kramer, 2000, for an example related to soft controls). Safety reviews will have to specifically address error tolerant design activities and features. This will require the development of comprehensive approaches to error tolerance. For new designs with no operating experience, it will be especially important to have a good risk analysis, to define risk-important human actions, and then to address those actions in all aspects of the design.

#### Managing Design and Construction Errors

Achieving Generation IV goals will require design and construction errors to be minimized. Finding such errors can significantly increase the cost and time to complete construction. If not found, they create safety problems for the newly operating plant. One of the lessons learned from the current LWR fleet is that people made design errors in many engineering disciplines that impacted many different aspects of the plant (Lloyd, Boardman, & Pullani, 2000). Table 3-5 provides examples of design errors. Many such errors were discovered and corrected at various points in the plants life cycle: design, design verification, construction, pre-operational testing, startup testing, and during the several decades of plant operation. Some design errors are still being identified, many years after startup.

**Table 3-5 Examples of Design Errors**

- NRC Bulletin 96-03: Potential Plugging Of Emergency Core Cooling Suction Strainers By Debris In Boiling-Water Reactors
- NRC Bulletin No. 93-02: Debris Plugging Of Emergency Core Cooling Suction Strainers
- NRC Bulletin No. 92-01: Failure Of Thermo-Lag 330 Fire Barrier System To Maintain Cabling In Wide Cable Trays And Small Conduits Free From Fire Damage
- NRC Generic Letter 98-02: Loss Of Reactor Coolant Inventory And Associated Potential For Loss Of Emergency Mitigation Functions While In A Shutdown Condition
- Generic Letter (GL) 89-10, Safety-Related Motor-Operated Valve Testing and Surveillance.
- NRC Information Notice 2002-29: Recent Design Problems In Safety Functions Of Pneumatic Systems
- NRC Information Notice 2002-06: Design Vulnerability In BWR Reactor Vessel Level Instrumentation Backfill Modification

The NRC has ongoing activities related to such errors including: Generic Communications with the industry, the Licensee Event Report (LER) data base, and lessons learned programs. In addition, NRC licensees and vendors perform this function through their Corrective Action Programs as conditions of their licenses, and 10 CFR Part 21 notifications.

Construction errors can occur both in modular/factory construction and in the onsite field construction. The issues associated with these two aspects would be different.

A particularly important aspect of the design for new plants is the reliance on software. The design, coding, and testing of software programs are important areas with significant safety implications.

Design and construction errors should be eliminated as much as possible from new reactor designs. One approach is to evaluate the past few decades of design error experience with a view to improving the design and initial test program processes in industry. Past corrective actions may have been too narrowly focused to identify and correct the broader generic problem. Research may be needed to address means to catalogue such errors, identify root causes where possible, and develop NRC review guidelines with the intent of avoiding, detecting, and correcting similar errors in new NPP designs.

#### Simplified Maintenance Practices

Generation IV goals suggest that vendors are likely to submit designs for plants that are easily maintainable to ensure quick and inexpensive repairs when needed. This may result in maintenance being more quickly performed by operations personnel without the checks and balances done by maintenance departments. This may also impact the knowledge, skills, and abilities required of operations staff and increase their workload. The changes in maintenance practices that result may have to be evaluated to determine that they do not negatively impact plant safety. New review guidance may be needed to support these reviews.

## Reduced Staffing

Due to a variety of factors, such as increased automation, design simplicity, and changes in operational practices, Generation IV plants may incorporate staffing approaches that are significantly different from those for current plants and include reductions in the number of personnel needed to manage the plant (this issue is discussed further in Section 3.3.1).

## Quantitative Human Performance Criteria

At present, there are no means by which to quantify human performance impacts of design features without actually measuring that performance. However, this requires a nearly complete design, trained operators, and a high-fidelity process model or the actual plant. The Generation IV roadmap report noted that one main objective of research in human factors should be to characterize a plant's design features that influence human performance in terms of quantitative criteria to enable effective comparisons of various Generation IV plant options. If such a measure were to be useful to compare options, it would have to be measurable at various points in the design process. The technical basis for such a measure and its application may have important safety implications.

## Physical Protection, Security, and Safety

Goals for providing increased physical protection against acts of terrorism raise the issue of ensuring that the added physical protection activities and design do not negatively impact safety, reliability, and plant or equipment availability.

### *3.1.3.3 Design Descriptions*

Design features and characteristics relevant to human performance are described below for selected Generation IV reactor designs slated for deployment further in the future than those mentioned above:

- Gas-cooled Fast Reactor (GFR) System
- Lead-cooled Fast Reactor (LFR) System
- Molten Salt Reactor (MSR) System
- Sodium-cooled Fast Reactor (SFR) System
- Supercritical-water-cooled Reactor (SCWR) System
- Very-high-temperature Reactor (VHTR) System

## Gas-cooled Fast Reactor System

The GFR system features a fast-neutron spectrum and closed fuel cycle for efficient conversion of fertile uranium and management of actinides. A full actinide recycle fuel cycle with on-site fuel cycle facilities is envisioned. The fuel cycle facilities can minimize transportation of nuclear materials and will be based on either advanced aqueous, pyro-metallurgical, or other dry processing options. The reference reactor is a 600-MWth/288-MWe, helium-cooled system operating with a high helium outlet temperature of 850°C (1562°F), using a direct Brayton cycle gas turbine for high thermal efficiency.

Several fuel forms are being considered for their potential to operate at very high temperatures and to ensure retention of fission products: composite ceramic fuel, advanced fuel particles, or ceramic clad elements of actinide compounds. Core configurations are being considered based on pin-or-plate-based fuel assemblies or prismatic blocks. The design is expected to use passive safety systems.

The GFR system addresses sustainability through its closed fuel cycle and excellent performance in actinide management. It addresses improvements in safety, economics, and in proliferation resistance and physical protection. It is primarily envisioned for missions in electricity production and actinide management, although it may be able to also support hydrogen production. Given its research and development (R&D) needs for fuel and recycling technology development, the GFR is estimated to be deplorably by 2025.

### Lead-cooled Fast Reactor System

The LFR system features a fast-neutron spectrum and a closed fuel cycle for efficient conversion of fertile uranium and management of actinides. A full actinide recycle fuel cycle with central or regional fuel cycle facilities is envisioned. The reactor is liquid-metal cooled by lead or lead/bismuth in a natural circulation mode. Options include a range of plant ratings, including a long-life, factory-fabricated core design of 50–150 MWe that features a very long refueling interval, a modular system rated at 300–400 MWe, and a large monolithic plant option at 1200 MWe. The modular units could be turnkey-type plants.

The fuel is metal- or nitride-based, containing fertile uranium and transuranics. The most advanced of these is the lead/bismuth design, which employs a small core with a very long core life (10 to 30 year). The reactor module is designed to be factory-fabricated and then transported to the plant site. The reactor is cooled by natural convection and sized between 120 and 400 MWth, with a reactor outlet coolant temperature of 550°C (1022°F), possibly ranging up to 800°C (1472°F), depending upon the success of the materials R&D.

The system is specifically designed for the distributed generation of electricity and other energy products, including hydrogen and potable water. The LFR system addresses sustainability by using a closed fuel cycle and it is proliferation-resistant. The safety is enhanced by the choice of a relatively inert coolant. It is primarily envisioned for missions in electricity and hydrogen production and actinide management with good proliferation resistance. Given its R&D needs concerning fuel, materials, reactivity effects of the Pb in the core area, and corrosion control, the LFR system is estimated to be deployable by 2025.

### Molten Salt Reactor System

The MSR system features an epithermal to thermal neutron spectrum and a closed fuel cycle tailored to the efficient utilization of plutonium and minor actinides. A full actinide recycle fuel cycle is envisioned. In the MSR system, the fuel is a circulating liquid mixture of sodium, zirconium, and uranium fluorides (and possibly also lithium, beryllium, or thorium fluorides). The molten salt fuel flows through graphite core channels, producing a thermal spectrum. The graphite serves as the neutron moderator. The heat generated in the molten salt is transferred to a secondary coolant system through an intermediate heat exchanger, and then through another heat exchanger to the power conversion system. Actinides and most fission products form fluorides in the liquid coolant. The homogenous liquid fuel allows addition of actinide feeds

with variable composition by varying the rate of feed addition. There is no need for fuel fabrication. The reference plant has a power level of 1000 MWe. The system operates at low pressure (<0.5 mega-pascals) and has a coolant outlet temperature above 700°C (1292°F), affording improved thermal efficiency. Temperatures up to 850°C (1562°F) are envisioned, which will support hydrogen production. As temperature increases to 1000°C (1832°F) the efficiency of H<sub>2</sub> production improves.

The MSR has passive safety systems with a fail-safe drain design and passive cooling. It addresses sustainability through its closed fuel cycle and performance in waste burn-down. It is primarily envisioned for missions in electricity production and waste burn-down. Given the R&D needs for system development, the MSR is estimated to be deployable by 2025.

### Sodium-cooled Fast Reactor System

The SFR system features a fast-neutron spectrum and a closed fuel cycle for efficient conversion of fertile uranium and management of actinides. A full actinide recycle fuel cycle is envisioned with two major options. One option is an intermediate size (150 to 500 MWe) sodium-cooled reactor with a uranium-plutonium-minor-actinide-zirconium metal alloy fuel, processed in collocated facilities. This would be a modular type of facility. The second option is a medium to large (500 to 1500 MWe) sodium-cooled fast reactor with mixed uranium-plutonium oxide fuel, supported by a fuel cycle based upon advanced aqueous processing at a central location serving a number of reactors. The outlet temperature for both is approximately 550°C (1022°F). The primary focus of the R&D is on the recycle technology, economics of the overall system, assurance of passive safety for planned passive safety systems, and accommodation of bounding events.

The plant uses a three-cycle system with: low-pressure primary cycle sodium; intermediate cycle, non-radioactive sodium; and water-steam in the secondary plant. The intermediate non-radioactive sodium system reduces the hazard should there be a significant sodium-water interaction accident.

The SFR system addresses sustainability (DOE 2002b) through its closed fuel cycle and design that addresses actinide management, including resource extension. It is rated good in safety, economics, and proliferation resistance and physical protection. It is primarily envisioned for missions in electricity production and actinide management. The SFR system is the nearest term actinide management system. Based on the experience with oxide fuel, this option is estimated to be deployable by 2015.

### Supercritical-water-cooled Reactor System

The SCWR system features two fuel cycle options: the first option is an open cycle with a thermal neutron spectrum reactor; the second option is a closed cycle with a fast-neutron spectrum reactor and full actinide recycle. Both options use a high-temperature, high-pressure, water-cooled reactor that operates above the thermodynamic critical point of water (22MPa, 374°C) (3200 psia, 706°F) to achieve a thermal efficiency approaching 44%. The fuel cycle for the thermal option is a once-through uranium cycle. The fast-spectrum option uses central fuel cycle facilities based on advanced aqueous processing for actinide recycle. The fast-spectrum option depends upon the materials' R&D success to support a fast-spectrum reactor.

In either option, the reference plant has a large 1700-MWe power level, an operating pressure of over 22MPa (3200 psia), and a reactor outlet temperature of over 374°C (over 705°F). Passive safety features similar to those of the simplified boiling water reactor are incorporated. Owing to the low density of supercritical water, additional moderator is added to thermalize the core in the thermal option. It is noteworthy that the systems and components of the plant are considerably simplified because the coolant operates at such a high temperature and pressure. Specifically, there is no pressurizer or steam generator as in PWRs, and there are no steam dryers, steam separators or recirculation pumps as in BWRs.

The SCWR system addresses economics (DOE 2002b) through high thermal efficiency and plant simplification. If the fast-spectrum option can be developed, the SCWR system also addresses sustainability. The SCWR system is primarily envisioned for missions in electricity production, with an option for actinide management. Given its R&D needs in materials compatibility, the SCWR system is estimated to be deployable by 2025.

### Very-high-temperature Reactor System

The VHTR system uses a thermal neutron spectrum and a once-through uranium cycle. The VHTR system is primarily aimed at relatively faster deployment of a system for high temperature process heat applications, such as coal gasification and thermo-chemical hydrogen production, with high efficiency.

The reference reactor concept has a 600-MWth helium-cooled core based on either the prismatic block fuel of the Gas Turbine–Modular Helium Reactor (GT-MHR) or the pebble fuel of the PBMR. Both plants would use a modular design. It also uses graphite in the core for moderation. The primary circuit is connected to a steam reformer/steam generator to deliver process heat. The VHTR system has the potential for high coolant outlet temperatures above 1000°C (1832°F). These may need to be reduced to the 900 to 950°C (1652 to 1742°F) range due to materials issues. It is intended to be a high-efficiency system that can supply process heat to a broad spectrum of high temperature and energy-intensive, non-electric processes. The system may incorporate electricity generation equipment to meet co-generation needs. The system also has the flexibility to adopt Uranium/Plutonium fuel cycles and offers enhanced waste minimization. The VHTR requires significant advances in fuel performance and high temperature materials development, but could benefit from the developments proposed for earlier prismatic or pebble bed gas-cooled reactors. Additional technology R&D for the VHTR includes high-temperature alloys, fiber-reinforced ceramics or composite materials, and zirconium-carbide fuel coatings.

The VHTR system addresses economics by its high hydrogen production efficiency. Safety and reliability are addressed by the inherent safety features of the fuel and reactor. It addresses proliferation resistance, physical protection, and sustainability by its open fuel cycle. It is primarily envisioned for missions in hydrogen production and other process-heat applications, although it could produce electricity as well. The VHTR system is the nearest-term hydrogen production system, and is estimated to be deployable by 2020.

These new reactor designs were reviewed to identify characteristics with potential effects on human performance. The information available about Generation IV designs is less well developed and less specific than that for near-term designs. Unfortunately, for the current purpose, the descriptions do not provide many (if any) details regarding control room

configuration and staffing (which are available for many of the designs scheduled for near-term deployment). Nevertheless, it can be assumed that technological advances coupled with Generation IV design goals may continue the trend toward digital I&C and highly computerized control rooms, and that Generation IV plants may incorporate features similar to those planned for the more innovative near-term designs (e.g., advanced interface concepts and different approaches to staffing).

#### *3.1.3.4 Potential Design Related Issues*

Potential HFE issues for Generation IV designs are summarized in Table 3-6 and discussed below. The main issues identified were:

- Passive Safety Systems
- Modular Plants
- Different Reactivity Effects
- Larger Number of Systems
- New Hazards

#### Passive Safety Systems

Like the near-term deployment designs, all of the Generation IV designs reviewed incorporate passive safety systems. Thus, the same issues that were discussed in relation to those designs apply to Generation IV designs as well.

#### Modular Plants

Like the GT-MHR and PBMR, a number of the designs feature smaller, prefabricated cores, which are well suited to scalable, modular plant designs. Thus, the same human performance concerns associated with near-term modular design may apply here as well.

**Table 3-6 Characteristics of Generation IV Reactor Design With Potential Human-performance Issues**

Design Characteristics with Possible Human Performance Issues	Reactor Types					
	GFR	LFR	MSR	SFR	SCWR	VHTR
Passive Systems	x	x	x	x	x	x
Modular Plants		x		x		x
Different Reactivity Effects		x				
Large Number of Systems			x			
Load Following Operations		x				
New Hazards:						
Hydrogen		x	x	x		x
Liquid sodium				x		
Liquid fuel			x			
Liquid metal		x				
High temps		x	x		x	x
High temperature gas	x				x	x
Supercritical water		x			x	
Graphite core			x			x
Large plant				x	x	
High pressure					x	

Different Reactivity Effects

Some of the designs incorporate unique features. In the LFR design, the presence of lead in the core area may result in reactivity effects that are different from light water reactors. For example, the LFR will have little neutron thermalization and lower Doppler effects. Also the temperature coefficient of reactivity will be less negative and the neutron lifetime shorter. These all tend to quicken the dynamics related to core power and transient operations. Operator control of reactor power and overall reactor safety is dependent on their understanding of these reactivity effects. Generally, complex physical interactions or dynamic behavior in principal plant processes can place added demands on human performance (Papin, 2002). Thus, designs incorporating truly innovative reactor technologies will have to include features aimed at limiting the additional challenges (e.g., training, automation, design of I&C systems, and controls and displays). These effects and features may have to be studied for their safety impact.

### Larger Number of Systems

Some of the near-term designs are larger than typical current plants. An example is the MSR, which has a large number of subsystems and equipment. This may result in increased complexity from the operators' perspective and place higher demands on operators to ensure that equipment performs properly.

### New Hazards

A distinguishing characteristic of Generation IV designs is the new hazards that may be associated with the reactor technology. These new hazards include hydrogen, liquid sodium, liquid fuel, liquid metal, much higher temperatures/pressures than LWRs, use of high temperature gas, supercritical water, and graphite in the core. The latter issue was also discussed in Section 3.1.2.2, Graphite Core. The hazards must be understood and addressed in safety systems used to mitigate the hazard, in procedures, and in operator training.

### **3.1.4 Summary of New Reactor Design and Technology Related Issues**

In this section, potential issues for three generations of reactor designs were discussed: modernization of Generation II plants with digital I&C and computer-based HSI technology, Generation III plant designs, and Generation IV plant concepts. Some of the same issues were identified for both the Generation III and IV plants, e.g., modular operations, and others are logically related, such as new hazards and graphite core. The issues identified for reactor design and technology are:

- Personnel Acceptance of Technology
- HSI Design Deficiencies
- Unanticipated Impact of Technology
- Increase in Complexity and Opacity
- Understanding How HSIs are Really Used
- Changes in HSI Demands and Training Requirements
- Knowledge Gap Between Utility Organization and Supplier
- Modular Construction
- Modular Plants
- Continuous Fueling
- Increased Power Operations
- Post-core-melt Mitigation
- Availability of Operating Experience of Generation III Reactors
- Passive Safety Systems
- Larger Number of Systems
- Different Reactivity Effects
- New Hazards (including the Graphite Core issue in Section 3.1.2.2)
- Managing Human Error in Operations and Maintenance
- Managing Design and Construction Errors
- Simplified Maintenance Practices
- Reduced Staffing
- Quantitative Human Performance Criteria
- Physical Protection, Security, and Safety

### 3.2 Digital Instrumentation and Control Technology

The I&C systems and associated HSIs for new reactors are expected to take full advantage of digital computer and communication technologies and related advances in areas such as smart sensors, diagnostics and prognostics, advanced control and computational capabilities, and higher levels of automation. Because of the rapid pace of change in these technologies, it is difficult to precisely predict what the systems will be when they are implemented in new plants 20 years from now. However, there are some emerging trends that provide insights into these systems, their capabilities, and their potential impact on human performance. Before the issues associated with I&C technology are discussed, a brief overview of modern digital I&C systems is provided.

Modern digital I&C systems include more functionality than their analog predecessors. The I&C system, together with plant personnel, is in effect the “central nervous system” of the plant. Through its subsystems, the I&C system senses basic parameters, monitors performance and system health, integrates information, and makes adjustments to plant operations as necessary. It also responds to failures and off-normal events, thus ensuring goals of efficient power production and safety. Current risk assessments have shown that I&C systems and personnel performance are some of the most risk-important aspects of plant operations.

From a functional perspective, an I&C system is made up of the following subsystems:

- *Sensor subsystems* - Nearly every aspect of plant processes use some form of physical measurement. These physical measurements take the form of sensors and instruments with signal conditioning that detect physical parameters in the plant, such as neutron flux, temperatures, pressures, flow, valve positions, electrical current levels, and radiation levels. New nuclear energy production technologies will require new and different types of sensors and instruments to measure physical processes. This includes sensors that will be required to work in high-temperature environments and measure process parameters that are quite different from those measured in LWRs in operation today.
- *Monitoring subsystems* - These subsystems monitor the signals and other information produced by sensors and evaluate that information to determine whether and what type of response may be 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 systems or processes. Prognostics refers to methods for using sensor data to estimate the rate of physical degradation and the remaining useful life of equipment, predicting time to failure, and applying this information to more effectively manage a facility’s assets and to schedule maintenance on an as-needed basis.
- *Automation and Control subsystems* - Digital control systems provide the capability to implement more advanced control algorithms than those that have been used in U.S. nuclear power plants to date. Current plants 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 schemes that combine multiple control methods in a multimode or hierarchical system to achieve optimum performance. Application of these advanced techniques will lead to more integrated control of plant

systems and processes (versus separate, non-interacting control loops) and greater complexity. More modern control systems also provide the capability of more interaction and cooperation between automation and personnel, which essentially makes “man and machine” team players in the accomplishment of plant control functions.

- *Communications subsystems* - Information flow throughout the I&C system and to devices being monitored and controlled is provided through a variety of communication systems that 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 are configured in a flexible network architecture and have greatly expanded functionality, increasing the effectiveness of plant maintenance by providing field access to instruction manuals and diagnostics, enabling “smart” transducers to signal their service condition to the plant engineering staff.
- *HSI subsystem* - Plant personnel monitor and control the plant using resources such as information displays, alarms, controls, and support systems (including diagnostic and prognostic information). These systems work with personnel to help them understand the plant’s condition and diagnostic problems and to help them take necessary actions. Due to its significant role in human performance, issues associated with HSIs are considered separately in Section 3.3.

In the midst of information and digital technology growth, these systems represent some of the greatest potentials for advancement in functionality, reliability, and processes within plant operations. Advanced I&C systems enable precise monitoring of plant performance, thus providing better data to plant control systems. The I&C system enables plant personnel to more effectively monitor the health of the plant, identify opportunities to improve the performance of equipment and systems, and anticipate, understand, and respond to potential issues and problems. Improved controls provide the basis for optimized performance, operating more closely to performance margins, and the improved integration of automatic and human response enables them to work cooperatively in the accomplishment of both production and safety goals. The I&C system also monitors the plant processes and various barriers that prevent potential release of radioactive material to the public. The use of advanced I&C systems directly impacts the performance of the entire plant and, consequently, the economics, safety, and security of future reactor designs as well.

The discussion below is organized according to two broad topic areas related to I&C trends, each of which has human-performance issues: Advanced functional capabilities and managing digital I&C systems. Key sources of information contributing to this section include: DOE (2000), Dudenhoeffer et al. (2007), Miller et al. (2002), Wood et al. (2003), and Wood et al. (2004).

### **3.2.1 Advanced Functional Capabilities**

Advanced functional capabilities are organized into the following topics and issues:

- Sensors and Condition Monitoring
- Digital Communication Networks
- Diagnostics and Prognostics
- Advanced Controls

- Computation and Simulation
- Level of Automation
- Information Systems Design
- Computer-supported Collaboration
- Monitoring of Plant Personnel

### Sensors and Condition Monitoring

In plants today there are relatively few discrete sensors being used, even fewer using auctioneering, averaging, or signal validation techniques. When the operator suspects a problem or has an indication of a failure in the instrumentation, it is relatively straightforward to troubleshoot or diagnose the problem. However, future plants are likely to have instrumentation systems that incorporate many more individual pieces of information at the lowest level, with layers of increasing integration and interpretation of this data, leading ultimately to highly processed information that is presented to the plant personnel. Trends in sensors and measurement system technologies that may affect human performance in new reactors include:

- *Smart sensors* – greater intelligence is being built into individual sensors, allowing more self-checking and self-calibration, and also providing the capability for multiple variables to be measured and combined to improve condition monitoring
- *Sensor proliferation* – sensors are being made smaller (e.g., micro electro-mechanical sensors or MEMS), less expensive, and with greater communication capability (e.g., wireless sensor networks), leading in the future to a proliferation of many very small sensors that collectively provide more robust condition monitoring of plant systems and equipment
- *Sensor “data fusion”* – data from multiple sensors are integrated together to form higher-level information on the condition of equipment and systems (see also the Diagnostics and Prognostics topic area below)

Human-performance issues associated with these new capabilities include determining the level of understanding of this functionality that will be needed by personnel to properly interpret and interact with condition monitoring systems, how they will be able to judge the quality of the information provided, and how they will deal with failures in these more complex systems.

Another trend is for reduced calibration, maintenance, and testing requirements for sensors. This may have significant economic benefits, but, at the same time, may lead to a greater detachment of personnel from the actual equipment and local conditions in the plant. Use of video and audio, which will be facilitated by high-bandwidth communication systems, may help address this issue.

### Digital Communication Networks

Advanced digital I&C systems make use of extensive communication networks to collect data from sensors, transmit control signals to plant equipment, provide intercommunication among processors involved in monitoring, control and protection (with suitable means to ensure the interconnections do not compromise safety functions), and communicate with human-system interfaces, such as workstations and overview displays. The communication systems are typically arranged in a hierarchy and with a degree of functional segmentation. For example,

they may incorporate local (e.g., fieldbus) networks for field devices, one or more high-speed control networks, protection or safety-critical networks, and information networks or layers to support operator workstations and digital historians. Advanced systems can be expected to include the ability for these different segments or layers to intercommunicate, but with protection or firewalls built in to address potential failure modes, particularly for safety-critical networks.

Communication networks for new plants also may need to integrate information from multiple modules or units on a single site, and allow for communication with off-site personnel who support personnel at the plant. Also, as digital media and communication technologies further evolve, bandwidths may increase, allowing greater amounts and types of information to be carried over the networks (e.g., more extensive communication of video and audio information as mentioned above).

For new reactors it is likely that, in addition to operational information, maintenance, engineering, and management information will also be communicated over the digital communication networks. Technical and administrative information also will be carried over the communication networks as plants evolve toward “paperless” operations.

These trends may have human performance implications. For example, the availability of all of this information on the digital communication systems may facilitate more integrated approaches to:

- plant performance monitoring and reporting
- scheduling and planning of maintenance activities
- other tasks performed by operations, maintenance, engineering, and management or supervisory personnel

Also, these advances will make the digital communication systems in new reactors more extensive, more integrated, and much more complicated than those used in plants today. As digital communication technologies and applications advance, greater fault tolerance capability will be built into these systems. They may have automatic reconfiguration or “self-healing” features that automatically manage the expected changes in plant configuration (e.g., taking a unit or module down for maintenance, taking equipment out of service) and faults or failures that occur in the I&C equipment or communication systems themselves. This raises issues related to human performance such as:

- the level of involvement of plant personnel in network management and reconfiguration
- the potential difficulty in maintaining situation awareness about the condition of the complex communication networks and the quality and timeliness of the information being received from the systems
- the need for personnel to troubleshoot and diagnose system degradation when failures occur
- the need to take manual corrective actions or implement workarounds to deal with these situations

## Diagnostics and Prognostics

Diagnostics refer to techniques for identifying and determining the causes of faults in the plant systems or processes. Prognostics refer to methods for using sensor data to estimate the rate of physical degradation and the remaining useful life of equipment, predicting time to failure, and applying this information to more effectively manage a facility's assets and to schedule maintenance on an as-needed basis. Developments in computer technology, smart sensors, data communications, and real-time data analysis capabilities will enable a new generation of diagnostics and prognostics technologies to be implemented in future plants.

Techniques for diagnostics and prognostics include analysis methods such as trending and statistical analysis, data-driven modeling using neural networks or other models that can learn from acquired data, methods based on first-principle models of the equipment or system, and hybrid methods that employ some combination of these or other techniques.

Accuracy and reliability of diagnostics and prognostics are significant issues for human performance. Issues that may need to be addressed include:

- the operator's understanding of these techniques
- the ability to query the system for information on the underlying basis for diagnostic and prognostic conclusions or recommendations
- the degree of trust to be placed in these systems

There are also issues related to training and qualification of operators – the degree to which diagnostics and prognostics capabilities should be relied upon in training and qualification exams, and training that addresses situations in which the operators must make do without them.

Greater use of prognostics may entail different operational strategies. With effective prognostic systems, operators may be more involved in predicting future states of the plant and its systems/equipment and taking action proactively, as opposed to monitoring the current state and reacting to changes or fault indications.

Another change relates to the need to deal with uncertainties in operations and maintenance decision-making. Plant operators and maintenance personnel are currently trained to work primarily according to procedures that are, for the most part, deterministic. In future plants with extensive diagnostics and prognostics capabilities, operators may increasingly be faced with diagnostic results that come with uncertainties, predictions, and recommended actions that carry attendant uncertainty, and risk assessments that are inherently probabilistic (see the "Computation and Simulation" topic for a related discussion on use of risk models). This may need to be addressed in the training, qualification, and licensing of personnel.

## Advanced Controls

Digital computer-based control systems provide the capability to implement much more advanced control algorithms than have been used in plants to date. Current plants rely primarily on single-input, single-output classical control schemes to automate individual control loops.

Some multi-variable control schemes have been applied and some plants incorporate a modest level of integration of control loops. However, more advanced control methods and algorithms have not been applied in nuclear plants, although many have been studied in research programs and some have been applied in other industries. Further advances are anticipated in control schemes, and it seems likely that new reactors may take advantage of more advanced control in order to help meet objectives of increased operability, load following capability, multi-unit or multi-module control, and reduced staffing.

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 schemes that combine multiple control methods in a multi-mode or hierarchical system to achieve optimum performance (see Wood et al., 2003 for a survey of these methods). Application of these advanced techniques may lead to more integrated control of plant systems and processes (versus separate, non-interacting control loops) and greater complexity.

This presents a number of issues related to human performance. First, increased control complexity affects design, operations, maintenance, and engineering support personnel. The design and verification/validation of the control schemes will be considerably more difficult than with classical control. Once designed and implemented, operations personnel will need sufficient understanding of the control schemes to be able to monitor their performance, determine whether they are working correctly, and be prepared to back them up. This leads to both design and human performance challenges. Maintenance and engineering support personnel will likewise be affected by the additional complexity and interactivity of the control schemes.

A second issue is related to implementation of intelligent control schemes that learn or change over time. Use of adaptive control methods and techniques, such as on-line knowledge capture and machine learning, offer the advantage that control performance can be improved over time as the plant is operated. However, this also means that the behavior of the controls will be changing. Operation and maintenance personnel will need to be cognizant of these changes and monitor the effects of the changes on plant performance.

Finally, more integrated control schemes can result in greater difficulty for operators when failures occur. This has already been seen in some operating plants that use integrated control systems in which multiple control loops interact when the system is in a fully automatic mode (e.g., the original Babcock & Wilcox Integrated Control System). Failures have the potential to cause multiple control loops to malfunction, placing the operators in a situation in which they must manually control multiple systems. Also, advanced control schemes may have multiple modes of operation and may automatically switch modes when plant conditions change or failures occur. The operators must maintain an awareness of the current mode of automation, be able to interact effectively with the system during all expected modes, and be prepared to back up the system if required.

In summary, a key issue is how personnel will react to failures of the I&C systems when more complex, advanced control schemes, integrated control, multi-mode control, and adaptive control methods are applied. It will be important for plant operators, maintenance personnel, and engineers to be able to distinguish between and react appropriately to: process anomalies,

sensor anomalies or failures, control adjustments or adaptations made automatically by the system, and control system failures.

### Computation and Simulation

As processing power and computational methods continue to evolve, I&C systems will be able to incorporate more extensive computational capabilities including the ability to run models and simulations faster than real time. Built-in simulation capability, coupled with visualization technologies, animations and virtual reality techniques, offer the possibility for personnel to play out “what-if” scenarios, or to replay events with tests of various hypotheses as part of diagnosis and response planning. These capabilities offer the potential to improve performance, but they also raise issues such as operator confidence in the model results, the ability to separate real and simulated data, and the potential to get lost in simulations.

With the trend toward increased computational and modeling capability plus the general industry and regulatory trend toward increased use of risk models to support decision-making, it seems likely that plant personnel will make more extensive use of on-line risk calculations and predictions to support their decision-making tasks.

### Level of Automation

Given the goals of reduced staffing and more economic operation, plus the advances in digital I&C technologies and general trends in industrial automation, the level of automation in new reactors is expected to be much higher than in today’s plants and the type of interaction between automatic systems and personnel much more varied.

New plants will likely involve an increase in overall process automation. The means for determining the acceptability of a particular level of automation for a given system remains an issue. Design philosophies must take into account the reliability of both the operator and the automation, the potential consequences to performance that may result from human and system failures, and the presence of design features and other factors (e.g., training) that may reduce the likelihood and consequences of these failures. Highly automated systems may perform all required actions unless the operator takes exception. However, to be effective, the operator must be given sufficient information to make an informed decision regarding the appropriateness of the actions proposed by the automated system. The presentation of this information and the means of user-system interaction are key issues. In addition, the operator may have to interact with a decision-aiding system to determine why a particular course of actions is being recommended (see Section 3.3.3 for a discussion of “Interfaces to Automation”). Thus, finding ways to keep the operator involved when high levels of automation are used is a potential issue.

Further, new digital I&C systems offer the possibility to provide new and more flexible types of personnel interaction with automatic processes. Thus, operators may play a variety of roles in the control and management of automated systems. Historically, processes were either manually controlled or fully autonomous. Increasingly, intermediate levels of automation are being implemented to help crews maintain better awareness of the automatic actions and to be in a more informed position when disturbances in the automation arise. One example of these new approaches to automation is “breakpoint automation,” as used in the ABWR. Thus, a task

such as plant start up, is divided into a discrete sequence of steps. Operators authorize the automation to begin a step and monitor its progress. Once completed, the automation stops (a breakpoint) so operators can determine whether it is acceptable to proceed to the next step in the sequence. Thus, the task is shared between operators and automation. Another example is “dynamic allocation.” Functions and tasks are flexibly performed by automation or operators based on the current operational situation. Thus, for example, automation may assume control over lower priority tasks when the operator’s level of workload increases to a point where it would be difficult to perform all their current work. This approach can ensure that operators are able to maintain their attention on high priority tasks because their workload levels remain within acceptable limits. Two important considerations include defining what the specific levels of automation will be, and the means for managing the dynamic changes in allocation. For example, the allocation may be specified by the operator, by the automation (based on predefined conditions), or jointly by both.

Two important issues include defining the levels of function allocation and the means for managing the changes in allocation. For example, the level of allocation may be set by the operator, by the automation based conditional factors, or jointly by them. The Department of Defense (DoD) HFE Technical Advisory Group (2002) recommended more research on real-time dynamic reallocation of function between system and human. They noted the need to understand the effects on users of transitioning between levels of automation, and also suggested that a definitive basis for identifying situations conducive to its use is lacking. Another area of growth is the automation of non-process control tasks that have been typically performed by operators, i.e., monitoring, detection and analysis of off-normal conditions; situation assessment; and response planning.

Maintenance and testing functions also will be increasingly automated, including fault detection and diagnosis, automatic reconfiguration of systems, and automated work order generation for required manual interventions. Engineering and administrative functions also may see increased levels of automation.

In addition, digital systems offer new opportunities to extend automation to the HSI itself. For example, operators may be offered specific displays that are automatically retrieved based upon predefined plant conditions. HSI automation may greatly reduce the workload that operators face to navigate and retrieve displays in the large information systems that will characterize modernized plants (see O’Hara & Brown, 2002).

Advances in I&C technology that impact plant automation include:

- data communication networks (e.g., automated reconfiguration of systems)
- diagnostics and prognostics
- advanced control methods
- computation and simulation (e.g., use of models to support automated functions)
- information management (e.g., automated tools for retrieving information)
- computer-supported collaboration (including collaboration with automated agents or aids)

In addition to the benefits to be obtained from increases in automation, there have historically been a range of human-performance issues that arise when that automation is poorly designed and implemented. Some of these issues include:

- a mental model (understanding) how the plant works is more difficult to develop because automation complicates operations
- situation awareness and alertness are lowered
- complacency can arise from confidence in automation (resulting in failure to properly monitor its performance)
- excessive workload can be created when there is an need to transition from monitoring automation to taking over manual control when the automation fails
- skills in performing automated tasks are degraded due to lack of use

The safety consequences of such issues are a significant consideration when evaluating the increased and more diverse automation anticipated in new plants.

For a detailed discussion of automation-related issues, see Section A.1 of the Appendix.

### Information Systems Design

With the proliferation of low-cost sensors, higher-level information resulting from “data fusion,” diagnostic and prognostic techniques providing condition monitoring results and predictions, and integration of plant technical data (drawings, equipment design data, historical data) with process information, I&C systems become more information-rich. Thus, issues related to information storage and retrieval become important. There is already a tendency for information overload in today’s plants, and it may be a greater problem in new reactors. The information systems likely will bring together process data, configuration data, engineering and maintenance information, results from intelligent agents, plant performance and economic data, data from multiple units/modules, and video and audio data.

Advances in databases, data mining, and information search and retrieval technologies offer potential solutions, but there are also human-performance issues related to different ways of interacting with data and information, shared responsibility for analyzing and interpreting data as information (the responsibility split between human and machine), and the potential for users to get lost in data. These issues have the potential to affect personnel performance.

### Computer-supported Collaboration

A significant problem in current plants is events that are caused by unique plant conditions resulting from the combined effects of different work groups executing their activities. In a new plant, the use of computer supported cooperative work (CSCW) may be used to help minimize these problems. CSCW refers to (1) the use of advanced information systems to supply knowledge within the organization that is needed by different groups to work in the most efficient, safe manner, and, (2) the use of technology to support crew communication and coordination.

With digital I&C systems, extensive communication networks throughout the plant (and links to remote locations) and computer-based interfaces for personnel at all locations, personnel can share information and common views of plant data regardless of where they are located. Advances in CSCW methods and technologies should further enhance the ability of personnel

to collaborate on tasks including monitoring, troubleshooting, diagnosis, and decision-making. This has the potential to affect the performance of both operations and maintenance personnel (see Stubler & O'Hara, 1996, and O'Hara & Roth, 2005, for a further discussion of the application of CSCW techniques to nuclear plant information system design).

Greater use of wireless communications and connectivity with remote locations will increase concerns about the security of the I&C systems and plant control. Users who engage in computer-supported cooperative work will need to identify themselves and have their identities authenticated. Decisions must be made on who is responsible for user authentication. To some degree, all users may have responsibility for authenticating other users with whom they interact, and for discerning any evidence of intrusions into the system.

In addition to human collaborations, with advanced systems employing technologies such as autonomous software agents (software that can make decisions and take action on its own), there will also be collaboration between human users and automated agents or assistants. Issues regarding crew or team coordination and communication, responsibility and authority, acceptance of the machine as a collaborator, and ability for users to understand the basis for an agent's work and query it for more information, will need to be addressed.

Issues related to this technology include:

- the means by which knowledge and information can be generated and distributed among work groups
- the means by which work can be conducted and coordinated within a plant complex (i.e., involving multiple plant modules)
- the principles for use of computer support tools to enable broad group communication and coordination

### Monitoring of Plant Personnel

Digital I&C technology provides the opportunity for systems to monitor personnel performance; for example, actions taken at workstations can be monitored and recorded. The systems can monitor performance and provide "comments" under predefined circumstances, such as when the operator makes a potential input error. Systems can also monitor physiological parameters to detect conditions such as fatigue. Technology also is available for location tracking that potentially will allow the plant monitoring and information systems and software agents to know where personnel are located at all times.

This capability may support better coordination, cooperation, and collaborative task performance in new plants, with the human and the machine working much more closely together than has been the case in plants to date.

However, concern over security and intrusion threats, and availability of personnel identification and monitoring technologies may lead personnel to feel they are no longer in charge, and to experience a loss of privacy that may affect recruiting, training, and performance.

### 3.2.2 Managing Digital I&C Systems

Management of digital I&C systems are organized into the following topics and issues:

- More Frequent Changes Due to Obsolescence
- Rapid Learning Curve in Early Stages of Plant Operation
- Change in the Concept of Maintenance
- Ease of Making System Modifications
- Design and Evaluation of Digital Systems and Software
- Operations Under Conditions of Degraded I&C

#### More Frequent Changes Due to Obsolescence

The rapid rate of advancement in I&C technologies has a potential impact on plant personnel. Installed equipment will become obsolete much faster than in current plants, leading to the need to make changes to ensure that it can continue to be maintained and that adequate vendor support will be available. Also, vendors will offer enhancements as their product lines and associated functional capabilities evolve. In the past, plants were reluctant to undertake major upgrades from analog to digital I&C due, in part to regulatory uncertainty associated with approval of such a major change. Individual upgrades to digital I&C (both hardware and software) could be viewed as more gradual, and would likely be performed under the guidance provided in Guideline on Licensing Digital Upgrades (EPRI, 2002) and 10 CFR 50.59 without the need for specific submittals to NRC for their review and approval. Thus, plant I&C systems may continue to evolve over the years with many incremental upgrades.

Therefore, plant personnel will see more frequent changes to the I&C system, including software and hardware, which will impact operations, maintenance and training. Also, the level of involvement of plant personnel in the changes will be an issue; for example, the trend toward automatic or semi-automatic updates of commercial software will need to be considered carefully before it is implemented.

#### Rapid Learning Curve in Early Stages of Plant Operation

Another issue relates to the fact that current plants have been slow to implement new technologies and no new plants have been built for many years. Thus, the U.S. nuclear industry has not had the opportunity to gain much experience with the newer evolving technologies. Automation is one example. In Japan, automation in nuclear plants has evolved over several generations of designs, allowing utilities and vendors to gain experience as relatively small evolutionary steps have been taken. New plants in the U.S. will present a revolutionary change in I&C technology. Thus, an accelerated learning curve should be anticipated that must be accommodated in the early years of operation. Plant personnel must be prepared to deal with shortcomings of the new I&C designs that will be revealed during operation and will require correction.

## Change in the Concept of Maintenance

The overall concept of maintenance is likely to significantly change with advanced digital I&C systems that have more extensive self-diagnostics and self-correction capabilities. Some aspects of this change are discussed here.

*Unique features of digital I&C* - Digital systems have features and capabilities that pose unique challenges for maintenance activities. The importance of these topics is likely to grow as the nuclear industry continues to adopt newer digital technologies to replace existing equipment and upgrade plant performance. A systematic approach is needed to ensure that the human factors considerations of maintenance are adequately addressed. Such a systematic approach should address both the process by which maintainability features are designed into digital equipment and the process by which the digital equipment is maintained, including the development of maintenance interfaces for digital equipment, test equipment and tools, maintenance training, and maintenance procedures. Because digital technology continues to rapidly evolve, these developments must be ongoing to keep pace with the technology.

*Workstation based maintenance* - Troubleshooting will be done through dialog with the system at a workstation, possibly with software agents acting as automated assistants. This is quite different from how I&C maintenance is accomplished in current plants. Operations and maintenance personnel will work cooperatively when performing maintenance, collaborating via the computer. An issue here is operator awareness of maintenance activities when maintenance personnel are working with the systems via workstations. In current plants, operators maintain some level of awareness simply by knowing what cabinets are open and where maintenance personnel are working. With workstation-based maintenance and troubleshooting capability, operators and maintenance personnel will need to each maintain an awareness of the others' activities, and system features should be provided to support this.

*Merging of maintenance and operations functions* - With the advent of more complex automation and information systems, on-site personnel who are charged with operating the plant also will increasingly need to act as the first line of defense when faults are detected or failures occur in the I&C systems. With digital systems, the distinction between I&C maintenance and operation tends to become blurred in the early stages of fault response. This can be seen to some degree in currently operating plants that have upgraded to digital control and monitoring systems. Early actions in response to I&C fault alarms call for operators to check diagnostic indicators and perform relatively simple actions, such as switching between redundant channels.

This task is likely to increase in new plants with fewer staff on site. The on-site personnel will need to make decisions and take initial defensive or corrective actions after faults or failures in the I&C systems. There will be a greater need for workarounds to allow continued operation until additional technical personnel are available at the site or remotely to do more extensive diagnosis and make needed repairs. Complex systems or subsystems will need to be treated as "black boxes" for these initial actions. Skills and training (as well as appropriate design features and system architecture) should reflect this.

For a detailed discussion of maintenance issues, see Section A.8 of the Appendix.

## Ease of Making System Modifications

Conventional hard-wired I&C systems are difficult and expensive to modify and often requires modifications to field cabling and/or replacement of equipment to obtain new or different functionality. However, advanced digital I&C systems provide much more flexibility and are easier to modify. With digital communication networks, adding a sensor may require only local cabling to bring it in as a new “drop” on a sensor network, or no cabling if using wireless communication. Enhancing functionality or adding new functions may be accomplished via a workstation without any physical change to equipment. This easy capability to change increases the potential to impact both safety and security.

Also, new nuclear plants will be expected to operate much more economically than the current generation; thus, meeting or exceeding economic performance goals will be a key driver for these plants. Given this environment, and the ease of modification of the I&C systems, plant operators would be expected to take advantage of experience gained during operation, and identify changes that can be made over time to improve plant performance and reduce costs. Advanced I&C systems may incorporate capability for knowledge capture and machine learning, or adaptive control methods that automatically adjust control schemes based on experience gained in operation. In addition, operations, maintenance, and engineering personnel may be responsible for identifying changes that will enhance performance while maintaining safety. There also will be the opportunity to make changes that improve plant safety based on operating experience.

## Design and Evaluation of Digital Systems and Software

Although the primary emphasis of this discussion is the impact of I&C advances on human performance in operation and maintenance, there are significant issues related to design of advanced digital I&C systems that should not be overlooked. New reactors will employ digital I&C systems relying heavily on software for critical monitoring and control functions. Software and knowledge representation will also form the foundation of the computerized operator support systems and intelligent agents that will be available to the crew in the control room and for test, maintenance, and configuration management functions.

*Increase in complexity* - The complexity of the I&C systems envisioned for new reactors is much higher than for current plant designs, and there is no practical limit to how complex software can be. A program can have many execution paths, which, in combination with process states and human inputs, lead to a very large number of distinct system states. Software is also error sensitive. In typical engineering contexts, small errors have small effects; this is not so with software. It is also difficult to test software. Software may be reliable and formally correct, yet still be unsafe in the context of the system it interacts with. Managing the complexity and the risk associated with potential errors designing critical software or in the overall digital system design requires careful attention to the qualifications and experience of design personnel (as discussed below), and the processes used to control the design, verification and validation, as well as the safety/hazards analysis activities and their results.

*Common-mode failure* - The possibility of correlated failures in software can make it more likely that a fault occurs. Programmed 'components' typically are re-used thereby weakening the protection afforded by redundancy. Even when two software systems are developed

independently, the similarity of industry design and testing approaches leaves them vulnerable to common mode failure.

*Hardware-software interaction* - Although much of the research on safety-critical systems has focused specifically on software, problems that have been experienced with digital systems often relate to hardware-software interaction, digital system architecture or other design issues, and inappropriate applications of digital systems.

*Design team skills* - For the I&C systems of new reactors, evaluations of risk should consider:

- the skills, abilities, training and experience of the designers
- organizational factors
- design processes
- design reviews, verification, validation, analysis and testing

Experience with critical digital systems has shown that the qualifications and experience of the design team are very significant factors, yet most efforts to evaluate and manage digital system risks have been directed primarily toward the process. Note that there will be different requirements for design skills and expertise for different aspects of the I&C systems. For example, a different set of skills is required for designing smart sensors, communication networks, diagnostics and prognostics, computational methods, advanced control algorithms, or human-system interfaces.

*Human error* - One of the biggest issues in software development is human error. Mistakes and oversights occur, but may only manifest themselves in interaction with the process or with other software components; i.e., the software errors often remain latent until a unique set of plant conditions occur and there are system failures or other performance problems. Given these limitations and the fact that new plants will be software based, human error in software development needs to be evaluated.

*Defensive design techniques* - Defensive design techniques are very important in managing risk of digital systems, such as making systems tolerant of design errors that may be present in software or digital system design. Their use in new reactor designs will have to be evaluated.

*Software quality assurance* - There are no well-established standards that can be relied upon to assure safety. Software verification and validation techniques are evolving and need to mature further before they are sufficiently robust to establish firm, objective criteria.

### Operations Under Conditions of Degraded I&C

Digital I&C systems and computer-based HSIs may pose new challenges to the handling of conditions of degraded I&C system components. I&C degradation may be caused by a variety of events, such as instrument failure, computer failures, seismic events, fire and smoke damage, internal flooding, or loss of electrical power. These events may cause a range of failures from individual control room instruments to more significant degradations such as the loss of all displays. A few issues associated with this topic are summarized below.

*Detection of digital system failure* - The loss of hardwired displays and controls is readily apparent to plant personnel. However, the degradation modes and failures in digital systems can be more difficult to detect, especially where failure is not complete. The reason is that much of the information with which the crew interacts will be at a high level as compared to the single sensor-single display relationship that characterizes more traditional equipment. Information displays, for example, will often represent the integration of many lower level data points. The impact of sensor and processing degradation on these higher-level displays is not well understood.

*Transition to back-up systems* - Upon failures of digital systems, crews may have to transition to using the hardwired control and displays and paper procedures. Crew interactions with these technologies are very different from their interaction with digital systems. Digital systems provide a great deal of support to crews in terms of information access and suitability to ongoing task requirements that conventional technology does not. There may also be training implications for using both digital and conventional systems and for the transition between them.

*Teamwork* - Digital systems have a significant impact on the nature of crew members' tasks and their interactions with each other. An example of this was given in Section 3.1.1.2, in the discussion of the issue "Unanticipated Impact of Technology" related to the use of computerized vs. conventional procedures. This may result in a shift to less teamwork, less communication, and more difficulty for crew members to monitor each other's activities. Thus, when crew members are located at individual panels, it is relatively easy to see what they are doing. By contrast, when crew members are seated in front of workstation VDUs, it is much more difficult to know what they are doing. When the digital systems are lost, the crew must shift its activities to once again accomplish the lower-level responsibilities that the digital system performed. In this case, the type of teamwork needed is more similar to that in present-day control rooms. This issue may become more significant as new generations of operators, trained mainly on digital system operations, have to cope with abnormal situations. Current crews are already well trained in the use of conventional equipment and in the associated teamwork requirements. Succeeding generations of operators will become less and less familiar with the conventional equipment.

### **3.3 Human-system Integration Technology**

The discussion in this section is divided into the following broad topic areas:

- organizational factors
- advanced human system interfaces
- computerized support systems

It should be noted that these trends and issues, like the ones discussed earlier, are highly interrelated.

The discussion in this section is based largely on issues identified in the course of extensive NRC research on computer-based HSI technology. A comprehensive list of the issues identified in these reports that are pertinent to new reactors is included the Appendix to this report. The higher-level discussions below are organized around the broad trends and issues listed above.

### 3.3.1 Organizational Factors

The main issues identified were:

- Functional Staffing Models
- Crew Member Roles and Responsibilities
- Training and Qualifications
- Biometrics, Fitness for Duty, and Security
- Safety Culture
- Vendor Diversity and Its Impact on Operational Philosophy

#### Functional Staffing Models

Current plants have a large number of on-site personnel organized into functional groups including operations, maintenance, engineering, administration, and security. Many of the designs slated for near-term deployment in the U.S. do not involve fundamentally different plant staffing concepts; accordingly, changes to the current approaches to staffing are not anticipated. However, since plant staffing and training are very costly aspects of plant operations, staffing will certainly be an area of focus in new plant designs. In addition, nearer-term modular designs and the longer-term goals for economy and safety may give rise to a trend toward different operating concepts and approaches to staffing. In anticipating new approaches, we use the term "functional staffing models" to refer to general approaches to fulfilling these human roles.

To illustrate the diversity of models, some of the candidates that depart from the current model will be presented. One alternative is a decentralized functional groups model. Multiple reactor modules are staffed with a very small number of onsite personnel. Unlike today's operational environment, the on-site crew is made up of technicians who oversee the highly automated operation and occasionally perform minor operations and maintenance tasks. Responsibilities for other activities are handled by off-site specialists who either come to the site when needed (such as for maintenance) or perform their tasks remotely. Significant disturbances may be handled by highly trained crisis management teams. Since these teams do nothing but handling crises, their level of expertise would be superior to what could be attained when a single crew is responsible for both normal and emergency operations (today's model). Due to the low probability of such an accident, the teams are available to handle emergencies at many reactor sites, a role that will be supported by increased plant standardization. This model greatly reduces staffing and training burdens.

There are many alternatives to this model, including:

- greatly reduced staffing (as compared with current plants) supported by a high degree of automation
- multi-unit operations by a single operator
- fully remote unit operations by a single crew

The staffing model chosen is a very significant design decision as it drives many other aspects of the plant design, such as levels of automation, HSI design, and personnel training. Selection of the staffing approach that best meets the goals for the plant will require tools such as modeling techniques and simulation facilities. The safety impacts of such approaches will have to be carefully evaluated.

### Crew Member Roles and Responsibilities

Once a staffing model for a new reactor is identified, crew member roles and responsibilities must be specified, e.g., whether a given crew member is responsible for particular modules, for specific systems across modules, or for certain operating states, evolutions, or transients.

There may also be changes in the degree of procedural vs. knowledge-based reasoning required of personnel in new reactors. The U.K. Safety and Health Executive (HSE) points out that, while customs have evolved in conventional plants as to the use of scenario-based vs. symptom-based procedures, design features (such as passive safety systems) and different concepts of operations may require revisiting this issue in the context of new, more advanced plants<sup>7</sup>.

Tools and techniques to perform function and task analyses for evaluating staffing needs also must to be developed; this issue is discussed later (see Section 3.3.1).

### Training and Qualifications

As technological trends, both near and long term, lead to changes in the organization of crews and crew member responsibilities, there will necessarily be changes in how plant personnel are trained and how their qualifications are defined. For example, to make the best use of some new display designs, operators may need to be trained to think about the plant in functional rather than physical terms. To the extent that this would require a fundamental shift in operational philosophy, it poses near- and long-term issues. In the near term, there is the issue of how the transition to new ways of representing and using information will be accomplished. Operators may be slow to accept such displays. In the longer term, the issue is whether the selection criteria for plant personnel might have to be modified to include different types of cognitive characteristics. Concern has also been expressed that advanced displays may inhibit long-term learning and retention (see O'Hara, Higgins, & Kramer, 2000 for a discussion of this issue). For displays of high-level information, where a large amount of information is consolidated into one or a few graphic images, the training requirements become very important. Operators must understand all aspects of the display and how it reacts to various operational transients, accidents, and instrument failures. The long-term effects of these displays on operator performance and strategies are unknown, but it is clear that training will be a key consideration.

Training considerations are associated with the selected approach to staffing. Qualifications are generally based not only on training but also education and experience. The knowledge and abilities required of different staffing functions need to be defined. Training approaches need to change to provide for distributed training, embedded training, and virtual reality.

---

<sup>7</sup> See the following website for HSE's Nuclear Research Index for Human Factors (retrieved February 14, 2008) - <http://www.hse.gov.uk/research/nuclear/nri/open/humanfactors10.pdf>

Taking a slightly different perspective, the HSE noted that traditional approaches to training assume a degree of homogeneity in the trainees; however, “with the trend toward multi-skilling and de-manning, particularly for plant operators and maintenance personnel, this common approach may be less appropriate”<sup>8</sup>. They suggested that techniques for assessing initial competence, identifying learning needs, and deciding on the appropriate training methods might need to be defined as well.

#### Biometrics, Fitness for Duty, and Security

Continued advances in the area of biometrics will permit the assessment of fitness for duty to be approached from a more functional perspective; e.g., measurement of relevant physiological and cognitive indicators can be compared to baseline criteria to indicate whether personnel are fit to perform their tasks. Biometrics may also play a role in meeting the goals for security in new plants by allowing the identities and movements of personnel within the plants to be monitored and documented. Selection of appropriate parameters and the methods used to monitor them will have to be made, in part, based on human factors input.

#### Safety Culture

There has been an industry trend toward large energy corporations that acquire many diverse plants. An issue that arises is how safety culture is transmitted to personnel at the individual units and determining the impact on safety culture of combining units with different original cultures under a single large operating entity. Longer-term issues may arise defining safety culture in the context of radically different concepts of operations and approaches to staffing (e.g., minimal onsite staffing, specialist crews).

#### Vendor Diversity and Its Impact on Operational Philosophy

Different approaches to designing and operating nuclear power plants have evolved in different parts of the world. Yet, the nuclear power industry is international. Therefore, plants based on designs developed elsewhere might operate well in this country, and vice versa. As a result, in addition to perhaps having different backgrounds, demographics, and population stereotypes than those prevalent in the country or area in the world in which the plant was designed, plant staff may have fundamentally different ideas about how a plant should be operated; e.g., the degree to which systems operate autonomously, or the extent to which responses to abnormalities are proceduralized. The possible safety implications of this issue will have to be addressed.

### **3.3.2 Advanced Human System Interfaces**

In a recent survey of control center operational and technology trends, AECL (2002) noted a trend toward integration of operating information from separate sources into unified task-based presentations to reduce workload, support decision-making and reduce errors. Similarly, the HSE has noted that systems already can provide online access to information about every aspect of the plant and that, in the future, there is likely to be an increase in the potential for

<sup>8</sup> See the following website for HSE's Nuclear Research Index for Human Factors (retrieved February 14, 2008) - <http://www.hse.gov.uk/research/nuclear/nri/open/humanfactors10.pdf>

collecting, accessing, and distributing information<sup>9</sup>. HSE noted the potential for misuse of these capabilities and that attention must be paid to possible drawbacks, functional requirements, and usability. In particular, they emphasized the need to consider human factors aspects of the types of support systems used by comprehensive information systems. Near-term, there may be a continuation of a trend toward integrating information that has typically been presented in separate displays, e.g., integrating alarms into process displays. A result of this trend will be that the classical distinctions between HSI resources, such as alarm, displays, and controls, will become increasingly blurred.

Integration of information is likely to eventually expand beyond the plant per se. In a recent survey of control center operational and technology trends, AECL (2002) noted a trend toward increased availability and responsiveness to market demands by means of high degrees of coordination not only between operations and maintenance activities, but also between these functions and electricity sales opportunities.

As the amount and variety of information available to personnel increases, there will be a need to use the capabilities afforded by computerization to synthesize information, and to design representations of higher-level information about the plant, resulting in interfaces that are more immediately and directly meaningful to operators. Also, in the context of reduced staff, changes to personnel roles, and multiple unit operations, it will be necessary to develop an interface through which plant personnel can obtain information effortlessly, when and where they need it.

Issues associated with displaying and providing access to large amounts of information are discussed below. The main issues identified were:

- Alarm System Design
- Display Design
- Interface Management Design
- Control Design
- Portable Computers and HSIs

### Alarm System Design

Alarm system effectiveness continues to be a problem in today's plants. Under typical normal operations and minor transients the alarm systems function well. However, the alarm avalanche received on major transients and accidents is commonly recognized as a problem area that is being addressed by new designs. Approaches to alarm implementation similarly will be addressed in new plant design. Significant aspects include:

*Improved approaches for alerting operators to unexpected conditions* - Given the importance of alarm systems, efforts to improve the effectiveness of alarm systems undoubtedly will continue in the near term, and designers will continue to concern themselves with how alarms are defined, processed, and presented, and how operators interact with the alarm system (i.e., alarm system controls).

---

<sup>9</sup> See the following website for HSE's Nuclear Research Index for Human Factors (retrieved February 14, 2008) - <http://www.hse.gov.uk/research/nuclear/nri/open/humanfactors10.pdf>

*Alarm definition* - Advanced technology will provide opportunities to obviate the need for alarm processing by taking plant contexts into account when defining the conditions that will be alarmed. That is, if a given condition warrants attention only under certain circumstances, then defining it as an alarm only in those circumstances avoids the need to deal with the alarm in circumstances where the condition is expected.

*Alarm processing* - Advances in I&C provide an opportunity for alarm processing to be more widely applied, and for the processing itself to become more sophisticated. While the feasibility of processing has increased, there are issues bearing on its use that remain unresolved. For example, there is at present little technical basis for choosing among processing techniques or for determining the degree of alarm reduction necessary to make the system usable when a significant disturbance occurs.

*Alarm presentation* - Computerization and digital I&C have already broadened the variety of ways in which information (disturbance-related and otherwise) can be presented to personnel. As technology advances, the types of displays available will increase. For example, providing large, group-view displays no longer presents the technical challenge it once did, and workstation VDUs are becoming more compact and less costly. However, there is only a limited basis for deciding to provide a given type of information via a particular display design. In addition, crew members must be able to readily access detailed information about unexpected conditions, especially those that alarm processing has assigned a high priority, and the design of effective hierarchical structuring and 'drill-down' techniques will remain important. Advances in display technology will also broaden the palette for presenting and coding indications of unexpected conditions. For example, it can be assumed that future designs will follow a trend seen in other domains and make better use of audio signals, and may also employ speech messages for indicating abnormalities.

*Alarm control* - The operators' interaction with the system will, of necessity, change from the traditional silence, acknowledge, reset, and test (SART) approach to one including a larger set of features. For example, additional interfaces may be required for features such as operator-defined alarms, operator adjustment of limits, and operator control of processing. Operators may also need to acknowledge an automatic changeover to different processing or silencing mode that is automatically invoked when alarm volume is high.

In the longer term, the functions of the alarm system probably will be integrated into a comprehensive information system, one of the functions of which is to detect and then to direct operators' attention to degraded or unexpected conditions; i.e., alarm systems may not exist as separate entities. Such a system might comprise:

- condition-monitoring
- on-line monitoring and assessment using advanced instrumentation and computational technology
- use of "data mining" tools in real-time to support the analysis of plant performance data and documentation
- predictor displays, fast-time simulation, and prognostics

Certain contemporary problems with alarm systems (e.g., the question of separating status indications from alarm displays) will cease to be a concern if there are no longer dedicated alarm displays. However, similar types of concerns regarding the processing and presentation of information will continue to exist. For example, directing crew members' attention effectively is likely to entail complex processing of information about deviation from normal conditions, and there is likely to be a point beyond which the amount or complexity of processing may reduce crew members' situation awareness by insulating them from process-related data.

For a detailed discussion of alarm system issues, see Section A.2 of the Appendix.

### Display Design

Digital systems provide the potential for very significant advances in display of information that simply were not possible with analog equipment. However, this capability is largely untapped in current systems because of the lack of established techniques for identifying high-level displays. Most information displayed in modern control rooms is fairly low level. Plant information is presented on VDUs using conventional display formats, such as mimic displays and trend graphs. These displays are essentially digital replicas of the information layout that exists in older control rooms - with some enhancements. In new plants, the digital infrastructure will allow information to be displayed at much higher levels that more clearly reveal fundamental principles that the plant systems serve, such as mass and energy balances. Other forms of information presentation and display are possible to help personnel understand the plant situation and to more effectively detect and understand developing failures. However, because these displays are not simply computerized instances of time-tested conventional instrumentation, there is little guidance for their design, and their effectiveness under various conditions has not been tested.

While more advanced displays offer potential improvements to performance as noted above, new approaches to information display are needed for another reason. While organizing controls and displays around plant systems may have been adequate for conventional CRs, it may pose difficulties in computer-based CRs. For example, a system-based organization may be rather easy to understand, but may require excessive work for display retrieval when the system-based organization of displays does not match operator task requirements (this specific issue is elaborated in the discussion of "Interface Management Design" in the next section). A related issue concerns the density of information to be presented on a display. Packing more information into individual displays can help insure that information needed simultaneously by personnel is presented together, and by providing more information in one display, the need to access additional displays is reduced. On the other hand, information dense displays are usually considered undesirable from a human factors standpoint because operators may have difficulty finding the information they want on a "crowded" display. This tradeoff needs to be better understood.

Finally, it will be possible in the control rooms of new plants to distribute information among a variety of computer-driven devices, including large wall panel displays, VDUs at consoles, and 'walk-up' displays at control panels. The allocation of information across workstations and display devices will be an issue, as will the number of individual workstations and display devices that are needed in the control room. One of the most frequent complaints of operators in existing computer-based control rooms is that they need additional VDUs. In part, this is due

to the fact that designers often decide how many monitors will be placed in the control room before they know what information operators need or how it will be presented, thereby installing too few monitors to view all the required information. It will be necessary to thoroughly explore the operators' information requirements and the advantages and limitations of higher-level displays in order to support informed decisions about the needed display resources.

For a detailed discussion of display design issues, see Section A.3 of the Appendix.

### Interface Management Design

The primary tasks performed by nuclear-power-plant operators are process monitoring and control. In a computer-based system, operators also must perform secondary tasks such as retrieving information and configuring workstation displays. These are called "interface management tasks." In listing current operating trends, (AECL, 2002) noted that the increasing volume of operating information and support resources will result in increased dependence on computer-based applications, 'requiring a shift in design emphasis to support information use rather than just information accessibility.' There are a number of sub-issues to the interface management problem.

#### *Information Access*

As noted earlier, an increasingly large portion of the information needed by operators is accessed via computerized interfaces. The effort required to obtain needed information and to carry out tasks depends on the design of these interfaces. If a large amount of information from disparate sources is needed, personnel may be forced to make performance tradeoffs, especially during demanding tasks, if the demands involved in accessing information are too high (O'Hara & Brown, 2002). For example, under demanding conditions, personnel may not use the flexibility designed into the display system because the effort associated with configuring it might detract from their primary task, i.e., controlling the process. Alternatively, personnel may need to expend effort to access information; thereby, lessening the amount of attention they can apply to planning and carrying out tasks. As computerized information systems become increasingly comprehensive and central to operators' tasks, the issue of information access cost comes to the forefront.

The costs associated with accessing information also affect monitoring, possibly decreasing the frequency and accuracy with which personnel routinely assess the status of plant systems. One cause for the negative effects is that primary and secondary tasks often demand the same resources. For example, if the same kinds of actions are required for both manipulating the interface and controlling a system, then one task may suffer as resources are directed to the other, especially during periods of high demand. However, if different resources are required for these two tasks, then it is less likely that one task will interfere with the other; consequently, a higher overall level of performance may be maintained.

Personnel are less likely to configure an interface if they do not expect the benefits to outweigh the associated costs (e.g., time and effort). Just as the display design can increase the cost of accessing information, the design of interface-management features may also increase such costs. As a result, personnel may be less likely to perform routine monitoring if the controls are difficult or awkward to operate (e.g., poorly placed relative to the operator or associated

displays). For example, a display device that has a touch interface located outside of the operator's immediate reach may be monitored less often than one within easy reach. In addition, actuation may not be as reliable when using a touch-screen, e.g., a technician may have to press a button multiple times to select a desired display). Accordingly, the design of effective computer-based displays and controls that minimize demands placed on personnel in obtaining information will be an issue.

### *Flexibility*

Computer-based HSIs offer significant interface flexibility. Since designers cannot anticipate the information needs associated with all possible circumstances, or the interaction styles preferred by different user, flexibility allows situation- or user-specific tailoring so the displays more closely match the needs or preferences of the user. However, there are tradeoffs between the benefits of flexibility and the costs it imposes on operators. These costs include the workload associated with using flexible features, and the difficulty in accomplishing tasks owing to the diminished predictability of the interface. There also may be human-performance costs when other crew members must view or use HSI components that have been modified by others, for example, when operators share HSI components or when a shift supervisor observes operators' actions. The advantage of interfaces that are not flexible is that they do not have to be thought about a great deal. The disadvantage is that they cannot be tailored to give better support to operators' task- or situation-specific needs. Thus, as greater flexibility becomes possible, issues will arise as to how much is desirable, in what circumstances, and for what purposes. A flexible user-interface feature should address the need to optimize operator performance under specific conditions. Flexibility without proper analysis can expose the operator to configurations that may impair performance, such as by increasing the likelihood of errors or delays.

HSI flexibility typically refers to features that can be directly modified manually by users. However, with advances in computerized monitoring of the process (and of operators' actions), flexible interfaces may also become increasingly likely to incorporate automation. Users can determine the need for a change in the HSI, and then take actions to carry out the change. Some direct user modification features for displays include features for moving display pages or soft controls to particular display devices, and features for creating operator-defined trend displays. A direct user-modification feature for controls may allow an operator to provide inputs as a single, compound command, rather than as individual commands in response to a series of prompts. The disadvantages of direct user modification of the HSI include the following:

- additional learning requirements for new users
- increased difficulty for casual users in making modifications (e.g., supervisory personnel may experience difficulty setting up or viewing user-defined trend graphs)
- trade-offs in time and effort associated with setting up a flexible feature and completing a task
- difficulty in over-the shoulder viewing of flexible features (e.g., by supervisory personnel)
- difficulties in coordinating the use of a flexible feature among multiple personnel

As indicated above, flexible interfaces that incorporate automation may adjust the HSI based on plant conditions, user behavior, or both. Advanced automation may allow the interface to adapt (1) for specific individuals, based on their preferences or past behavior and performance, or (2) to meet changing needs of the user based on current task demands. A computer-based model of the user may be employed to predict the user's interface management needs and support adjustments of the HSI. This model may contain a profile of the user's characteristics and a program for determining interface management needs. Increasing computer-mediation of operator actions and the development of integrated data collection functions will allow the implementation of these systems in future plants.

For a detailed discussion of interface management design issues, see Section A.7 of the Appendix.

### Control Design

Operators' actions (both to control plant processes and the HSIs) will continue to be increasingly mediated by computer systems. The types of control interfaces differ from those typically found on traditional control boards, and will likely continue to change. In addition to keyboards and keypads, computer-based systems incorporate controls implemented on visual display devices, and these may have novel features. The removal of the constraints of conventional controls and input devices can allow the design of highly flexible and functional controls; however, designers of such controls do not have the benefit of accumulated experience about the types of actions they best support, and the types of errors that may occur in their use. Specific issues that may emerge from this trend are described below.

*Input and feedback methods for continuous-variable inputs* - Industry experience has shown that the entry of numerical values is error prone, especially when performed using a keyboard or keypad. However, the popularity of the keyboard as an input device suggests that it may have some advantages (such as speed) compared to other methods, such as arrow keys and soft sliders. Feedback regarding the magnitude of entered values (provided, for example, by digital readouts or bar charts) can support the detection and correction of input errors, but there is little information available regarding the relative advantages of combinations of input and feedback methods.

*Keyboards versus incremental input devices* - Many soft controls provide the operator with the choice of changing control values via arrow buttons or via a keyboard. Like continuous-variable inputs, keyboard entry is prone to error, e.g., large-magnitude input errors may result from typing errors. Lacking better information on the error rates associated with data entry via keyboards versus incremental input devices, questions remain on the appropriate use of particular input devices.

*Consistency of soft controls* - When systems incorporating soft controls are installed as a series of independent modifications rather than an integrated effort, the overall HSI may contain a variety of soft controls. Under these circumstances, operators make frequent switches between different styles of interaction. It is reasonable to expect that this would not be the case for future new plants but rather that the computerized controls would be designed consistently. However, studies of computer-based systems have suggested that consistency can lead to slips, where operators think they are operating one control, but actually they are operating the wrong control.

The probability of this type of error will increase if there is a high degree of consistency without sufficient cues to enable operators to readily distinguish between similar-looking controls.

*Sequential plant control and interface management tasks* - Many plant control tasks are sequential, and different tasks can have similar but different sequences. For example, some pumps require that the downstream valve be closed prior to starting the pumps. Other pumps require that it be opened. The types of errors (e.g., interruption errors and capture errors) that can occur when such sequences are performed using hardware control are well known, and there are established methods (e.g., procedural or hardware) for avoiding them. Controls that are implemented in software and presented on computer displays and are typically accessed sequentially, i.e., one after another. The sequential nature of their use and that of the control tasks themselves may interact, possibly resulting in an increase in the likelihood of performing actions in the wrong sequence, or starting one task sequence and finishing with another.

*Soft controls and display space* - If, as expected, the portion of operators' activity (e.g., monitoring, process control, interface management, and communication) that is computer-mediated continues to increase, the amount and type of computer-driven display space available becomes a potential concern. For example, if space is limited, controls may be made visible only while they are being operated to avoid obscuring other data displayed on the same device. However, this may exacerbate the kinds of sequence-related errors referred to above because the controls are not continuously visible, the operators lack cues that would remind them that a sequence of actions has not been completed. Increasing the number of display devices can reduce conflicts between demands for short-term control actions and long-term monitoring actions. Placing controls on dedicated display devices can also improve access time by reducing the need to perform display navigation tasks in addition to allowing operators to more easily keep track of tasks that have been temporarily suspended. Nevertheless, there are practical limits to the amount of space that will be available in the interface, and trade-offs between providing dedicated display devices and general-purpose display devices will continue to be an issue.

*Speech-mediated interfaces* - As noted above, secondary tasks, such as those involved in accessing information, may negatively affect operators' effectiveness at their primary tasks. One reason for the negative effects of secondary tasks is that they draw on the same cognitive resources as the primary tasks at the same time. For example, if the same cognitive resources are required for both manipulating the HSI and controlling the plant, then during periods of high demand, one task may suffer as resources are directed to the other. However, if different cognitive resources are required for these two tasks, then it is less likely that one task will interfere with the other, and, consequently, a higher overall level of performance may be maintained. The use of speech interfaces has been explored because they offer an alternative information channel that may lessen the competition for resources.

Speech may be used either as an input medium (the interface reacts to operators' utterances) or as a means of presenting information (via a computer-driven voice). Speech input may allow operators to avoid having to interrupt their primary tasks to call up and use menus and tools for accessing information. Implementation of speech input will depend on continued improvements in speech-recognition technology and sufficient recognition. Spoken presentations allow operators to receive information without having to change or obscure what is shown on their primary display, or shift their attention to other display devices. In new plants, speech may offer

an alternative means of conveying status information that in conventional control rooms is often presented by means of 'alarms.'

The use of speech in either of these ways has a potential benefit beyond that associated with the reduction of competition for resources. When operators interact with systems via computer interfaces, their fellow crew members are less able to infer what they are doing; i.e., operators' actions are less 'visible.' If, on the other hand, parts of the interaction are mediated by speech, the ongoing verbalizations may partially compensate for the loss of visibility, and increase crew members' general awareness of each others' actions.

For a detailed discussion of control design issues, see Section A.4 of the Appendix.

### Portable Computers and HSIs

One often thinks of HSIs as being in fixed locations, such as in a control room or local control station. The increasing portability of computers allows HSIs to be brought where they are needed. Operators and maintenance personnel will be able to communicate and work cooperatively with the information system and automation even when they are not in the control room or at a fixed workstation. For example, clothing is being developed today that will integrate communication and computer interfaces to facilitate mobility and connectivity. However, the information and control design is significantly impacted by the size constraints imposed by portability. Maintaining performance and safety with these new devices will have to be demonstrated.

### **3.3.3 Computerized Support Systems**

The main issues identified were:

- Interfaces to Automation
- Computer-based Procedures
- Computerized Operator Support Systems
- Intelligent Agents

#### Interfaces to Automation

As was discussed earlier, the extent and nature of automation may significantly change (see Section 3.2.1). Designing the displays needed by operators to monitor and interact with new automatic systems will be challenging since little guidance is available to support their design or review. There is a lack of guidance for design review as well.

#### Computer-based Procedures

Plants have many types of procedures, e.g., administrative, operating, emergency, surveillance, test, and maintenance. Systems are available to present procedures in computerized form and to provide support for their use. Owing to the advantages of computerization (e.g., support for procedure maintenance and configuration management), the trend toward the CBPs can be expected to continue.

As sensor input and control capabilities are made available to computerized systems, it becomes feasible for CBPs to incorporate greatly expanded functionality and so they may come to resemble complex automated systems. There may be no technological limit to the extent of such procedural automation, especially when looking to long-term deployments. The role of the operating crew and the 'procedures' will be defined by the concept of operations.

Studies of current computer-based procedures suggest there are human-performance issues associated with CBPs (O'Hara, Higgins, Stubler, & Kramer, 2000). Some specific issues that need to be addressed are summarized below.

*Personnel role in procedure use* – Plant personnel must be able to independently assess the appropriateness of procedures to the current situation. However, CBPs have the potential to work against this independence and minimize the user's role. For example, should CBPs only automate data gathering and lower-level activities, or should they also automatically evaluate procedure-step decisions? The analysis of procedure step logic (i.e., the comparison of actual parameter values to the reference value identified in procedures using the logical relationships described in the step) is an important capability of CBP systems. However, when the step logic or the actual data analysis required for evaluating the step logic is incomplete, both the procedure and the operator may incorrectly assess the situation. A related issue concerns how to guard against this situation, and how to specify when the evaluation of step logic should be left to the operator's judgment. Thus, the question arises as to how much of a procedure's function should be automated to ensure that personnel can independently assess the results (O'Hara, Higgins, Stubler, & Kramer, 2000).

*Narrow field of view* – Typically, access to computer-based displays and controls tends to be serial, rather than parallel; thus, operators only see a little of the procedure at one time. The narrow field of view is potentially significant in that it may limit the operators' ability to flip forward and back through the procedure, or to consult multiple procedures at the same time. Because only a portion of the procedure can be observed at one time, operators may lose a sense of where they are in relation to the total set of active procedures. The available display space may be inadequate to support simultaneous viewing of multiple procedures and associated plant data. The sheer burden of interface management in navigating and retrieving many displays can interfere with the operators' ability to obtain an overview of the plant's situation.

*Structure of procedure content* – The computerization of procedures may provide opportunities for new and different approaches to the structure of procedure content that can improve efficiency and reduce errors in procedure use. The impact of such changes on procedure use will be an important issue.

At the same time, the appropriateness of techniques that evolved for paper presentation may be an issue. For example, it is not clear whether flowchart procedure presentations are acceptable in computer media where the limited screen view and need for scrolling may make them less effective. Similarly, studies have generally found that reading extended text from VDUs is visually fatiguing. Further, too little information presented at each procedure step can cause operators to lose a sense of where they are, while too much detail may be a distraction. The level of abstraction in which procedure step results are presented will impact the operators' situation awareness.

*Operator awareness* – Use of CBPs may alter operators' awareness of the state of the process. For example, if plant indications are accessed by the CBP, the operator may not feel the need to look at other sources of information and may miss important indications that are not present in the CBP. Operators may also uncritically accept the CBP's assessment of the plant's condition. The nature of CBP use itself may diminish the chances that errors in the selection of a course of action or the execution of step logic will be detected (see below).

*Team performance* – In the control room, the operating crew is a team in which the members must share information and coordinate their tasks to satisfy specific goals or mission requirements. This requires a common understanding of the status of the system and an understanding of each other's actions and intentions. CBPs have the potential to limit this knowledge (Roth & O'Hara, 2002). For example, it may not be necessary for the user of a CBP that integrates display and control capabilities to request information from or give control orders to other crew members. This can lessen the collective awareness of the state of the process and eliminate an important means of detecting when a procedure is off track, i.e., is not accomplishing the appropriate operational goal.

*CBP failure in complex situations* – Ensuring the transfer from CBPs to backups (e.g., paper procedures) has been identified as an important consideration in the design of CBPs, especially those used in emergency conditions. As the scope and functionality of CBPs increase in the future, the ability to cope with loss or degradation of CBP capabilities becomes a greater concern. The transition from a computerized system to a backup may be easily accomplished when the procedural context is simple, such as when operators are in the first few steps of a procedure. However, the transition may be quite complex if operators are deep into the procedures. Other factors that make the transition complex are: when multiple procedures are open, many steps are completed, and when the CBP is monitoring many steps of continuous applicability, time-dependent steps, and parameter-dependent steps. How operators will manage failures in such complex situations is unknown. Operators' familiarity with paper-based procedures will also be an issue. To date, there have been only limited opportunities to evaluate transitions from CBP to paper-based backups, and these have involved crews that were highly practiced with the paper-based versions of the procedures. In future plants, crews may train principally with the CBP system, and thus be at a greater disadvantage in the event of a failure.

For a detailed discussion of procedure design issues, see Section A.5 of the Appendix.

### Computerized Operator Support Systems

Computerized operator support systems (COSS) assist personnel in monitoring, decision-making, and planning. Their applications include improving plant performance, condition monitoring, core monitoring, early fault detection and diagnosis, safety-function monitoring, and plant control. While first generation COSSs have been around for some time, the digital I&C infrastructure in new plants will provide a basis on which second-generation systems can be developed. Therefore, the use and scope of these systems in the control room can be expected to increase. In addition, because effective testing and maintenance are major drivers for the safety, reliability, and economics of nuclear power, the application of COSS technology to maintenance decision-making, and planning, is likely to increase as well. Computerized

systems to support maintenance will support 'just-in-time' maintenance, and will minimize the time spent on maintenance, the impact on production, risk, and personnel exposure.

Plant information can feed predictive models and fast-time simulations to provide plant personnel with much better decision support than previously was possible. However, human-performance issues have been identified that have limited the effectiveness of current COSSs; these include: poor integration with personnel task performance, complexity of COSS information processing, lack of transparency of the COSS decision process, inadequate explanatory information to address personnel verification needs, absence of communication facilities to permit personnel to query the system or obtain a level of confidence in the conclusions that have been drawn. To design effective COSSs and integrate them into plant work practices and procedures, these issues must be resolved.

For a detailed discussion of COSS design issues, see Section A.6 of the Appendix.

### Intelligent Agents

Intelligent agents are computer functions that perform information processing tasks for operators in a semi-autonomous or fully-autonomous manner. They are adaptive to changing plant conditions and their overall role can be much broader and independent from personnel. Intelligent agents will provide significant support for on-line monitoring, fault detection, situation assessment, diagnosis, and response planning through the use of advanced sensing and computational technology. The potential benefits of intelligent agents must be weighed against operator burdens associated with supervising these agents, and any potential problems that may result from their inappropriate application.

## **3.4 Advances in HFE Methods and Tools**

Human factors methods and tools that are applied to the design and evaluation of complex systems are constantly evolving as newer approaches are developed. It is anticipated that future nuclear systems will reflect the application of newer methods, especially for Generation IV plants. In this section, the trends in HFE methods and tools are examined. Their implications apply not only to NRC review criteria, but to the methods the staff use to conduct reviews, and the types of analyses and data that are included in submittals made by applicants.

### **3.4.1 Current HFE Methods and Tools**

The main issues identified were:

- Operating Experience and Lessons Learned
- Development of New Function Allocation Methods
- Development of New Task Analysis Methods
- Development and Application of Knowledge Engineering Techniques
- Human Reliability Analysis Methods for Advanced Systems
- Design Process for Higher-level Interfaces
- Guidance for the Review of Intelligent HSIs
- Validation of Integrated Systems

- Methods to Support the Early Consideration of Human Factors in Plant Design
- Collection, Analysis, and Use of Real-time Human Performance Data
- Modeling and Measurement of Effective Team Performance
- Evaluating the Effects of Advanced Systems

### Operating Experience and Lessons Learned

Operating experience review is a key element of the NRC's *Human Factors Engineering Program Review Model* (NUREG-0711) (O'Hara et. al, 2004). While the development and use of operating experience is often considered an important design activity, formal methods are needed to ensure that it is collected, that human performance insights related to it are recorded, and the lessons learned extracted.

A key issue relates to the recording of operating experience for the development of HFE insights. Improvements along these lines were one of the main recommendations of a recent OECD workshop (OECD Workshop, 2003). It has further been noted that lessons learned tend to focus on negative aspects of performance (Papin, 2002). One impediment to including human factors considerations at the earliest stages of design is the lack of a basis for taking into account the positive aspects of human action (especially knowledge-based action) in plant operations. As a result, the basis for considering 'positive' performance shaping factors is limited, and it is more difficult to make the case for considering human factors in early design decisions.

Thus, improved methods for collecting and evaluating operating experience are needed.

### Development of New Function Allocation Methods

Generally accepted methodologies to conduct function analyses are lacking. However, this is a very important issue for new reactors. As the degree of plant automation is expected to increase and become more widely applied, the need is great for accepted methodologies in the context of advanced nuclear plants. Traditional function and task analysis methods are not oriented towards advanced systems where crews interact mainly through computers and with intelligent systems.

### Development of New Task Analysis Methods

One area that is rapidly evolving is task analysis. It actually comprises a family of techniques. One technique is not adequate because individual tasks can be very different from one another. Some tasks are sequential and well defined, like plant startup. Other tasks are ill defined and not sequential, like fault-detection, troubleshooting, and situation assessment. Different task analysis methods are better suited to different objectives. For example, link analysis is a method of determining the layout of equipment and consoles based on task demands. Operational sequence analysis is a method of examining the detailed behavioral aspects of tasks that are fairly well defined and sequential. Hierarchical task analysis is a method of decomposing higher-level functions to the information and controls that personnel need to perform their tasks. Cognitive task analysis (CTA) is a method for examining tasks that are ill-defined and dependent on the expertise of the user. In combination, these methods provide important tools for identifying task requirements.

Recent advances in work analysis, cognitive task analysis, and cognitive engineering are especially applicable to supervisory control tasks. These methods are particularly well suited to analyzing the nature of expertise and as the nuclear industry loses expertise, these methods, along with knowledge engineering methodologies will be increasingly applied in the industry (see next topic on knowledge engineering).

At present, there is a lack of guidance on the appropriate application of such methods to the analysis of safety-related tasks. As these approaches are relatively new, their methodologies are not formalized yet. Guidance for the review of task analyses employing these methods is needed.

### Development and Application of Knowledge Engineering Techniques

Knowledge engineering involves techniques for identifying and documenting the knowledge of subject matter experts. When this knowledge is coupled with simulation and analysis tools, a powerful knowledge base is created upon which to improve operations and maintenance. This information can be applied to the development of more intelligent interfaces in the near-term (such as intelligent alarm processing and analysis), and to intelligent agent design in the long term. Efficient methods to obtain and store such knowledge in integrated databases are needed. In addition, review criteria are needed to evaluate HSIs developed using the knowledge elicited from experts.

### Human Reliability Analysis Methods for Advanced Systems

Human reliability analysis (HRA) will continue to be an important tool in the performance of safety evaluations using probabilistic risk assessment (PRA), especially as safety reviews become more risk-informed. However, current HRA methods may not be applicable to new designs incorporating increased automation, alternative concepts of operations, and intelligent interfaces. The conduct of HRA will be further hampered by the lack of databases upon which to estimate base-case human error probabilities.

### Design Process for Higher-level Interfaces

While interfaces incorporating higher-level, functionally-oriented displays may be a promising advance, there are no well-defined processes for conducting the analyses needed to specify them. There has been little research that carefully assesses the various aspects of these interfaces, e.g., information requirements, effect of organization of information along functional lines, display representation, and use of analytical redundancy. The ability of such interfaces to support the successful handling of unplanned-unanticipated events under actual operational conditions needs to be demonstrated.

### Guidance for the Review of Intelligent HSIs

Based on current trends, it is likely that HSIs will continue to become more intelligent. The knowledge and reasoning bases of these systems will be diverse, e.g., application of knowledge engineering or use of formal analysis rules. At present, the NRC's *Human-System Interface Design Review Guidelines* (NUREG-0700) (O'Hara et. al, 2002) does not have sufficient guidance to address the review of the technical bases for intelligent HSIs.

## Validation of Integrated Systems

In addition to addressing specific aspects of HSI design or plant operations, the NRC is also concerned with evaluating integrated human-machine systems (O'Hara, Stubler, Brown, & Higgins, 1997). This is especially important in the context of new reactors, since the designs will be more complex and the interfaces will incorporate more functions than in conventional designs. NRC HFE guidance, e.g., NUREG-0711, includes HFE tests ranging from HSI design evaluations to integrated system validation as part of a design review and design certification efforts.

While they identify the considerations for the conduct of validation, more clearly defined and detailed methodological criteria for validation and the full range of system test and evaluation activities are needed to review licensee submittals. A technical basis exists upon which review guidance on methodology can begin to be developed; e.g., see Golan et al. (1996) on maximum entropy econometrics, O'Hara (1999) on the application of quasi-experimental methods, and Snow et al. (1999) on comparing new designs with baselines.

## Methods to Support the Early Consideration of Human Factors in Plant Design

Papin (2002) advocates addressing human factors issues early in the design process, rather than restricting consideration to design and evaluation of HSIs. Decisions about the human role in management of future plants should be guided by the positive contributions humans can make to safety and reliability and not restricted to minimizing the negative effects on risk. Papin suggests that human factors considerations for a design in its early stages can be evaluated in the absence of information required for formal analysis, by characterizing its complexity and dynamic aspects. Based on identifying and analyzing the constraints and interactions associated with the technical means for achieving safety objectives, a 'complexity scale' can be created. This indicator can be calculated globally, or for individual safety functions. Assuming that lower complexity and lessened time constraints translates into better human performance, the indicator provides a basis for comparison among design alternatives and for illustrating the value of particular new design features (e.g., passive operations). This and similar indicators should be applied to existing or new projects in an advanced phase of the design and validated from operating experience, feedback, data and/or detailed probabilistic safety assessment (PSA or HRA) results. Further developments along these lines could be useful in forming design tradeoffs that involve taking human performance into account at levels more basic than the HSI (i.e., process and plant systems, instrumentation and control systems).

## Collection, Analysis, and Use of Real-time Human Performance Data

Computer-mediation of human actions in future plants will allow the development of data logging capabilities that can be integrated into display, control, and communications interfaces to automatically gather and analyze human interaction data. This, in turn, will support the development of HFE tools that could be used in assessing human performance and predicting performance shortfalls. Based, in part, on the same data, as well as evolving understanding of cognitive aspects of operator tasks, it will also be possible to develop methods for measuring and modeling cognitive performance. Likewise, computer mediation of actions may allow a more detailed view of crew interactions than previously available, and this also could support

measurement and modeling of team performance (DoD HFE TAG, 2002), an issue discussed below.

### Modeling and Measurement of Effective Team Performance

Nuclear plant personnel work as crews to accomplish their functions and tasks. Understanding team performance will be significant in future plants that may involve alternative concepts of operations, use of intelligent agents, and applying technology to support teamwork, such as computer-supported cooperative work. Research is needed to identify what constitutes good and effective teams and how teamwork is affected by technology. In addition, measures of effective team performance are needed and can be applied to system design and evaluation, including integrated system validation.

### Evaluating the Effects of Advanced Systems

Methods and criteria for advanced system acceptance need to be addressed from both research and regulatory-review perspectives. One might specify that such systems should improve performance; on the other hand, the requirement might be only that performance should not be degraded. In either case, methods would be needed for evaluating their effects on crew performance under a wide range of scenarios and complex situations.

### **3.4.2 Trends in HFE Methods and Tools**

Perhaps more challenging than addressing gaps in current methods is forecasting how HFE methods and tools are changing. In this section the current trends in HFE methods and tools are considered to anticipate how these changes may affect safety reviews. The main issues identified were:

- Participatory Ergonomics
- Rapid Prototyping
- Rapidly Changing HSI Technology
- Changing Testbeds
- Human Performance Models
- Performance-based Methods

### Participatory Ergonomics

With the rapid development over the past decade of standards for user-centered design and concepts of usability engineering, recognition is becoming more widespread, in that it is important to obtain input from users early and often during a design project. This is sometimes called "participatory ergonomics."

While this is an important development and fully consistent with NUREG-0711, an accepted view has yet to emerge of specifically what contribution users should make, or how such input should be solicited. Thus, user input is sometimes obtained as part of a design review and sometimes the users essentially design the interfaces. The latter is the situation with some of the control room modernization programs currently underway. This approach can have safety

implications. While users have significant contributions to make, they do not necessarily know principles of good interface design.

A clearer technical basis for where and how users should participate in the process is needed for future design projects and regulatory reviews of them.

### Rapid Prototyping

The use of rapid prototyping tools enables design to become much more iterative and fast paced. Rapid prototyping is often performed with system users as a means of soliciting feedback, making HSI modifications, and repeating the cycle until the design is completed. This is quite different from the more traditional approach of performing careful information requirements analysis, applying HFE guidelines, and conducting evaluations in a much less iterative manner.

As a new approach, acceptable methods of rapid prototyping have yet to be developed and the methods of documenting the design basis of HSIs developed this way are not established. Similarly, review guidance for evaluating designs developed in this manner does not currently exist.

### Rapidly Changing HSI Technology

HFE guidelines are one of the technical bases for designing systems, conducting verifications, and performing regulatory reviews. In the development of NUREG-0700, key concepts for the technical basis for guidance development are internal and external validity. These forms of validity help provide assurance that HFE guidelines are technically sound and reflect appropriate scientific knowledge of the design characteristics that affect human performance. However, as HSIs become more computer-based, they can be expected to change far more rapidly than was the case with analog HSIs. This is true of digital systems in general. As the evolution of new design concepts accelerates, there will not be sufficient technical basis on which to develop HFE guidance. Thus, designs will be developed and evaluated using methods and tools that go beyond guidelines. This will necessitate a change in regulatory review approaches that rely on HFE guidelines for reviewing the detailed aspects of HSI design.

### Changing Testbeds

HFE tests and evaluations often use testbeds like full-mission simulators. However, new technologies are being developed that provide flexible alternatives that can be used for design and evaluation. For example, virtual reality (VR) can be used as an alternative to physical mockups or simulators. For example, VR was used to evaluate control room layout issues during the Oskarshamn control room modernization project in Sweden. It can be anticipated that this trend will continue and the application of new testbeds will become more widespread.

An important question to be addressed is the validation of VR models and the methodology for their use. VR is accomplished by many different technologies, and the value of different approaches may differ.

## Human Performance Models

There is a significant push in the human factors community to develop human performance models that can be applied to design and evaluation projects. Operator availability is limited, and the means to collect data can be expensive, such as using full-mission simulators. Models, therefore, can be an attractive alternative. Human behavioral modeling techniques, such as task network modeling and discrete event simulation, have been developed and tested by the U.S. Army and Navy, and some of these techniques have been accredited by the U.S. Department of Defense for use in HFE analyses during system design and engineering (Allender, 1995).

The NRC developed models to support staffing evaluations using task network modeling techniques (NRC, 2005). These techniques are attractive in that they permit "human performance" data to be generated without the need to collect data using actual operators (Laughery & Persensky, 1994; Laughery, Plott, & Persensky, 1996; Lawless, Laughery, & Persensky, 1995). Partly as a result of these encouraging results, modeling was identified as a means of evaluating exemption requests from 10 CFR 50.54(m) (NRC, 2005).

As the sophistication of the models improve, their application will be extended to more complex design and evaluation situations. For example, the cognitive workload associated with an information system design may be estimated using a cognitive model of human information processing.

Before its use in a regulatory review, whether by the NRC staff or as part of an applicant submittal, the validity of the modeling and its results must be assured. The type of questions to be addressed include:

- What type and amount of data from actual trials with operators is needed to build models?
- Are the models of sufficient fidelity to use in regulatory evaluations?
- Is modeling "cost-effective" relative to alternative analytical approaches?
- What is the value added component of modeling, e.g., what can be accomplished with the models that extends beyond what can be practically accomplished with actual trials?
- What is the relative role of results from actual human trials and results produced by models?

## Performance-based Methods

There is a trend in design evaluation toward performance-based methods, in contrast to design verification methods (such as comparing a design using HFE guidelines). It will be necessary to establish NRC acceptance criteria and review procedures for independently assessing performance-based evaluations.

## 4 ISSUE SUMMARY AND ORGANIZATION

Using developments and trends in the areas of reactor technology, I&C technology, and human-system integration technology, numerous potential human-performance issues related to new reactors were identified. In addition, trends in the area of HFE methods and tools were identified as well. Since the organization of issues is technology driven rather than by categories that are meaningful to HFE, the issues were organized in a way that is more meaningful to human factors engineering. Such an organization should provide a better overall framework with which to discuss long-term research needs. A "concept of operations" framework was used to provide that organization.

### 4.1 Defining Concept of Operations

As noted in Section 2.1, Approach, a framework was sought to help organize the human-performance issues and to ensure all important topics were addressed. The framework used was that of a "concept of operations." Concept of operations documents are increasingly being used in a wide array of industries to address the vision of how humans are integrated into a system. They are especially appropriate in the early stages of design in order to identify design goals and expectations relative to human performance. As a concept of operations covers all facets of personnel interaction with a complex system, it provides a good organizational framework for a wide variety of issues.

Concept of operations plays a significant role in the NRC's review of the human factors aspects of NPPs. NUREG-0711 defines it in Section 8.4.2, Concept of Operations. Criterion 1 states that:

A concept of operations should be developed indicating crew composition and the roles and responsibilities of individual crew members based on anticipated staffing levels. The concept of operations should:

- Identify the relationship between personnel and plant automation by specifying the responsibilities of the crew for monitoring, interacting, and overriding automatic systems and for interacting with computer-based procedure systems and other computerized operator support systems.
- Provide a high-level description of how personnel will work with HSI resources. Examples of the types of information that should be identified is the allocation of task to the main control room or local control stations, whether personnel will work at a single large workstation or individual workstations, what types of information each crew member will have access to, and what types of information should be displayed to the entire crew.
- Address the coordination of crew member activities, such as the interaction with auxiliary operators and coordination of maintenance and operations should be addressed.

However, while concept of operations is used in NRC HFE review guidance, we examined the current literature to more precisely define and update what a "concept of operations" means and how it can be used to organize the issues.

The idea of a concept of operations is a fundamental component of systems engineering and in the design of any complex system (Fairley & Thayer, 1977). In many industries, design

guidance suggests that a “concept of operations” document be used to help guide the development of requirements, detailed design, and system evaluation. For example, a documented concept of operation is usually required in military projects (DoD, 1985; DoD, 1995) and is a recommended practice in the aerospace industry (AIAA, 1992). The Federal Highway Administration recently completed a study on developing and using a concept of operations for transportation management systems (DOT, 2004).

The concept of operations for a new system begins to be defined before the design work actually starts. At that point, the concept reflects the goals of the organization procuring a new system that were formulated by the desire to improve on an existing system and to correct problems discovered through operating experience. These goals may include:

- incorporating new technological capabilities, such as increased automation
- reducing staffing or operational costs
- minimizing recurring errors and otherwise improving human performance

In large-scale system development, these goals may be explicitly incorporated in the request for proposal.

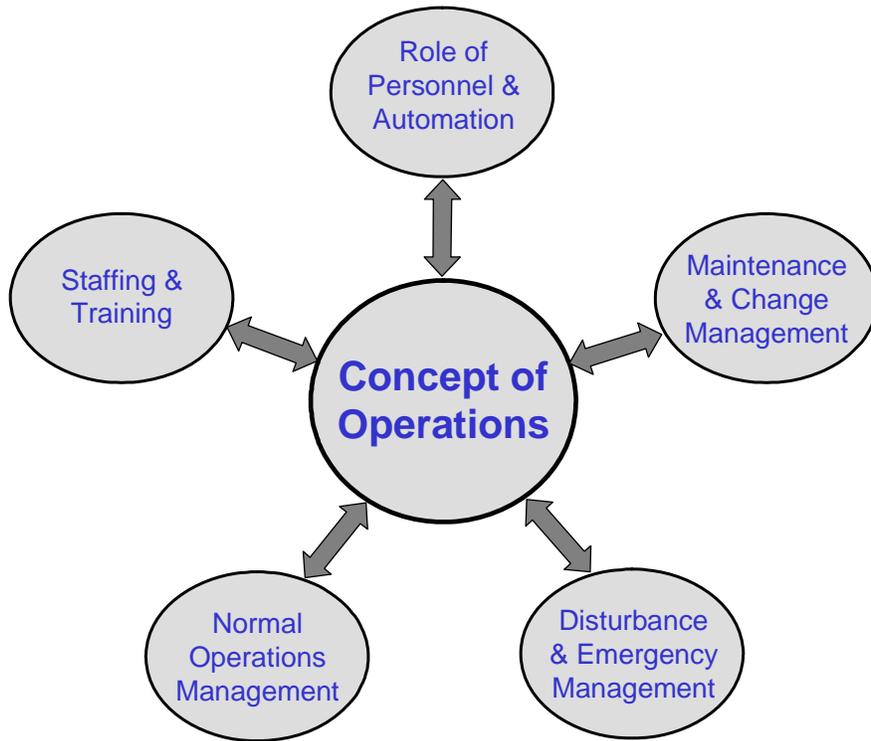
NUREG-0711 recognizes such goals and addresses them as part of Element 1 - HFE Program Management in Section 2.4.1, General HFE Program Goals and Scope. The first two review criteria state:

- (1) *HFE Program Goals* - The general objectives of the program should be stated in "human- centered" terms, which, as the HFE program develops, should be defined and used as a basis for HFE test and evaluation activities.
- (2) *Assumptions and Constraints* - An assumption or constraint is an aspect of the design, such as a specific staffing plan or the use of specific HSI technology, which is an input to the HFE program rather than the result of HFE analyses and evaluations. The design assumptions and constraints should be clearly identified.

Design organizations refine and more precisely define the concept of operations through analyses, requirements development, and evaluations. Concept designs are developed for achieving the desired concept of operations.

A concept of operations reflects top-down and bottom up considerations. From the top, the concept reflects the high-level goals for system operations. From the bottom, the concept rests on the technological infrastructure needed to support it. A characterization of the concept of operations was developed that is divided into five dimensions (see Figure 4-1). The dimensions are:

- Role of Personnel and Automation
- Staffing and Training
- Normal Operations Management
- Disturbance and Emergency Management
- Maintenance and Change Management



**Figure 4-1 Concept of Operations Dimensions**

The dimension, *Roles of Personnel and Automation*, addresses the relative roles and responsibilities of personnel and plant automation and their relationship. The definition of human roles and responsibilities in a system is the first step toward human-system integration, from which all other aspects of the concept of operations and system design flow. This dimension is usually specified to some level before design work begins and is refined using a variety of evaluation techniques, such as operating experience review, function and task analysis, and testing.

The *Staffing and Training* dimension addresses approaches to staffing the plant, including staffing levels and personnel qualifications. For example, new reactor goals include reduced staffing. In addition, this dimension includes the ways in which teams will be structured and the types and means of interaction between team members and other people, such as the coordination of crew member activities and the means by which checks and supervision are accomplished. The training needed to achieve these aspects of the concept of operations is also addressed.

The *Normal Operations Management* dimension addresses the concept of how the plant will be operated by personnel to follow its normal evolutions, such as start-up, low power, full power, and shutdown. Specifically, the concept of how personnel will interact with plant functions, systems, and components to accomplish their main tasks of monitoring and controlling the plant through these normal evolutions. This includes concepts for the resources provided to conduct their activities, e.g., the human-system interface (HSI), procedures, and supporting infrastructure. For example, the following concepts for how personnel interact with HSI resources may be specified:

- information distribution, e.g., the types of information which individual crew member access and the types of information that are displayed to the entire crew
- distribution of HSIs between the main control room and local control stations
- configuration of personnel workplaces, such as a single large workstation or individual workstations
- the type of high-level control strategies to be achieved

The dimension, *Disturbance and Emergency Management*, addresses concepts for how degraded conditions, disturbances and emergencies will be handled, and how responses to such situations will be determined. For example, as part of the concept of operations, a system developer must decide how operations are expected to change when the computer network goes down. Are personnel going to shut the plant down until the condition can be fixed, will they maintain the plant in its current state, or will they do something else? That decision has a significant impact on the types of backup resources that must be provided, the procedures that must be written, and the training personnel must receive.

The *Maintenance and Change Management* dimension addresses concepts for system maintenance, installing upgrades, and configuration management. For example, a great deal of maintenance in advanced systems will typically be performed at a workstation through software changes. This is a significant change from current practices. Another example is the management and control of operator initiated changes. New software systems typically have features that enable user to make changes, again, a marked departure from current practices where all modifications are controlled by engineering change procedures.

In the design of a new system, the concept of operation should consider and address each of these dimensions.

This model of a concept of operations was used as an organizing framework for the results presented in the next section.

## **4.2 Organization of Human-performance Issues into High-level Topic Areas**

Many of the issues that were identified relate to the concept of operations dimensions. Thus, each of the five dimensions served as a high-level research topic. However, some of the research issues were not associated with these topics. Hence, they were grouped into two additional topics: "Plant Design and Construction" and "HFE Methods and Tools." Thus, we identified seven high-level topic areas in all.

Table 4-1 shows the relationship of the original list of individual research issues and the seven high-level topic areas. The topics to which an issue belongs are shown by shading the cell in the topic's column. Some issues were related to more than one topic; this is indicated in the table by shading more than one cell.

Table 4-2 reorganizes the issues into the seven high-level topic areas (shown in bold). Some topics were further divided into sub-topics (shown by underline) to better identify clusters. Volume 1 of this report provides a descriptive summary of each high-level topic.

**Table 4-1 Relationship of Issues to High-level Topic Areas**

Detailed Issues	High-level Topic Areas						
	RPA	S&T	NOM	DEM	MCM	D&C	HMT
<b>Reactor Technology</b>							
Personnel Acceptance of Technology		X					
HSI Design Deficiencies			X	X			
Unanticipated Impact of Technology			X				
Increase in Complexity and Opacity			X				
Understanding How HSIs are Really Used			X				
Change in HSI Demands and Training Requirements		X					
Knowledge Gap Between Licensee Organization and Supplier						X	
Modular Construction						X	
Modular Plants			X				
Continuous Fueling			X				
Increased Power Operations			X				
Post-core-melt Mitigation				X			
Availability of Operating Exp. of Gen. III Reactors			X				
Passive Safety Systems				X			
Larger Number of Systems			X				
Different Reactivity Effects			X				
New Hazards				X			
Managing Human Error in Operations and Maintenance			X	X	X		
Managing Design and Construction Errors						X	
Simplified Maintenance Practices					X		
Reduced Staffing	X	X					
Quantitative Human Performance Criteria							X
Physical Protection, Security, and Safety			X				
<b>I&amp;C Technology</b>							
Sensors and Condition Monitoring			X				
Digital Communication Networks			X				
Diagnostics and Prognostics				X			
Advanced Controls			X				
Computation and Simulation			X				
Level of Automation	X						
Information Systems Design			X				
Computer-supported Collaboration			X				
Monitoring of Plant Personnel	X						
More Frequent Changes Due to Obsolescence					X		
Rapid Learning Curve in Early Stages of Plant Operation		X					
Change in the Concept of Maintenance					X		
Ease of Making System Modifications					X		
Design and Evaluation of Digital Systems and Software						X	
Operations Under Conditions of Degraded I&C				X			

High-level Topic Areas							
Detailed Issues	RPA	S&T	NOM	DEM	MCM	D&C	HMT
<b>Human-System Integration Technology</b>							
Functional Staffing Models		X					
Crewmember Roles and Responsibilities		X					
Training and Qualifications		X					
Biometrics, Fitness for Duty, and Security			X				
Safety Culture			X				
Vendor Diversity and Its Impact on Operational Philosophy			X				
Alarm System Design			X				
Display Design			X				
Interface Management Design			X				
Control Design			X				
Portable Computers and HSIs			X		X		
Interfaces to Automation			X				
Computer-based Procedures	X		X				
Computerized Operator Support Systems	X		X				
Intelligent Agents	X		X				
<b>HFE Methods and Tools</b>							
HRA Methods for Advanced Systems							X
Design Process for Higher-Level Interfaces							X
Validation of Integrated Systems							X
Participatory Ergonomics							X
Methods to Support the Early Consideration of Human Factors							X
Rapidly Changing HSI Technology							X
Operating Experience and Lessons Learned							X
Development of New Function Allocation Methods							X
Development of New Task Analysis Methods							X
Dev. and Application of Knowledge Engineering Techniques							X
Guidance for the Review of Intelligent HSIs							X
Collection/Analysis/Use of Real-Time Human Perf. Data							X
Modeling and Measurement of Effective Team Performance							X
Evaluating the Effects of Advanced Systems							X
Rapid Prototyping							X
Changing Testbeds							X
Human Performance Models							X
Performance Based Methods							X

Notes:

RPA = Role of Personnel and Automation; S&T = Staffing and Training, and Teamwork;  
 NOM = Normal Operations Management; DEM = Disturbance and Emergency Management;  
 MCM = Maintenance and Change Management; D&C = Plant Design and Construction; and  
 HMT = HFE Methods and Tools.

**Table 4-2 Organization of Issues into High-level Topic Areas**

---

**Role of Personnel and Automation**

Increase in the Extent and Diversity of Automation

- Level of Automation
- Computerized Operator Support Systems
- Computerized Procedures
- Intelligent Agents
- Monitoring of Plant Personnel

Consequences of Increased Automation

- Reduced Staffing

**Staffing and Training**

Approaches to Staffing

- Functional Staffing Models
- Reduced Staffing
- Crew Member Roles and Responsibilities

Training Implications

- Training and Qualifications
- Change in HSI Demands and Training Requirements
- Rapid Learning Curve in Early Stages of Plant Operation
- Personnel Acceptance of Technology

**Normal Operations Management**

General Knowledge Limitations

- Availability of Operating Experience of Generation III and III+ Reactors
- Unanticipated Impact of Technology
- Understanding How HSIs are Really Used

Specific Changes to Operations

- Modular Plants
- Different Reactivity Effects
- Increased Power Operations
- Continuous Fueling
- Physical Protection and Safety
- Biometrics, Fitness for Duty, and Security

Advances in HSIs Technology

- Interfaces to Automation
- Sensors and Condition Monitoring
- Digital Communication Networks
- Alarm System Design
- Information System Design
- Display Design
- Control Design
- Advanced Controls
- Computerized Operator Support Systems
- Computerized Procedures
- Computation and Simulation
- Interface Management Design
- Portable Computers and HSIs
- Computer-supported Collaboration
- HSI Design Deficiencies

Complexity

- Increase in Complexity and Opacity
- Larger Number of Systems
- Intelligent Agents

### Organizational Factors

- Vendor Diversity and Its Impact on Operational Philosophy
- Safety Culture
- Managing Human Error In Operations And Maintenance

### **Disturbance and Emergency Management**

- New Hazards
- Passive Safety Systems
- Post-core-melt Mitigation
- Diagnostics and Prognostics
- Operations Under Conditions of Degraded I&C
- HSI Design Deficiencies
- Managing Human Error in Operations and Maintenance

### **Maintenance and Change Management**

#### Rapid Pace of Technology Change

- More Frequent Changes Due to Obsolescence
- Ease of Making System Modifications

#### Impact on Maintenance Practices

- Change in the Concept of Maintenance
- Simplified Maintenance Practices
- Portable Computers and HSIs
- Managing Human Error in Operations and Maintenance

### **Plant Design and Construction**

- Managing Design and Construction Errors
- Design and Evaluation of Digital Systems and Software
- Modular Construction
- Knowledge Gap Between Licensee Organization And Supplier

### **HFE Methods and Tools**

#### Analysis Methods and Tools

- Methods to Support the Early Consideration of Human Factors in Plant Design
- Operating Experience and Lessons Learned
- Development of Function Allocation Methods
- Development of Task Analysis Methods
- HRA Methods for Advanced Systems
- Development and Application of Knowledge Engineering Techniques

#### Design Methods and Tools

- Rapidly Changing HSI Technology
- Participatory Ergonomics
- Rapid Prototyping
- Design Process for Higher-Level Interfaces

#### Test and Evaluation Methods and Tools

- Evaluating the Effects of Advanced Systems
- Guidance for the Review of Intelligent HSIs
- Validation of Integrated Systems
- Changing Testbeds
- Performance Based Methods
- Collection, Analysis, and Use of Real-Time Human Performance Data
- Modeling and Measurement of Effective Team Performance
- Human Performance Models
- Quantitative Human Performance Criteria



## 5 HUMAN PERFORMANCE ISSUE PRIORITIZATION

### 5.1 Overview

The issues were evaluated and prioritized using a Phenomena Identification and Ranking Table (PIRT) methodology. In this application, the phenomena are the issues identified in Section 3. This section describes objectives, methodology, and results of the evaluation and prioritization method.

### 5.2 Objective

The objective was to prioritize the human factors research issues and identify those of greater importance with respect to regulatory activities.

### 5.3 Methodology

#### 5.3.1 Subject Matter Experts

Fourteen independent subject matter experts (SMEs) participated in the exercise. The SMEs had knowledge of human factors, I&C, plant operations, and HFE and PRA analysis methods.

The SMEs represented a cross section of the industry and included regulators, vendors, utility personnel, and researchers. All SMEs were knowledgeable of the nuclear industry although several work in other industrial domains. The SMEs were affiliated with the following organizations.

- NRC – Office of Nuclear Reactor Regulation
- NRC – Office of Nuclear Regulatory Research
- Canadian Nuclear Safety Commission
- Electric Power Research Institute
- TXU Power
- CDF Services, Inc.
- Atomic Energy of Canada, Limited
- AREVA Nuclear Power, Inc.
- Pacific Northwest National Laboratory
- Idaho National Engineering Laboratory
- Halden Reactor Project
- Science Applications International Corporation
- Alion Science and Technology
- Federal Aviation Administration

#### 5.3.2 Issue Evaluation Procedures

Based on pilot testing of the methodology, the following issues were screened out of the SME evaluations based on consistently low ratings:

- Monitoring of Plant Personnel
- Change in HSI Demands and Training Requirements
- Rapid Learning Curve in Early Stages of Plant Operation
- Personnel Acceptance of Technology
- Biometrics, Fitness for Duty, and Security
- Portable Computers and HSIs
- Larger Number of Systems

The SMEs evaluated the issues in two phases. In Phase 1, each SME was sent:

- A draft of NUREG/CR-6947 (O'Hara, et al., 2008)
- A draft of this BNL technical report providing a detailed discussion of the issues
- An evaluation form that contained instructions and rating dimensions

The SMEs evaluated the issues according to the instructions and returned the completed forms to the project staff. The responses were then evaluated and the results compiled.

In Phase 2, a meeting of the SMEs was held. All but three of the SMEs were able to attend. The overall purpose of the meeting was to discuss those issues for which agreement was low so that SMEs could provide their rationale and basis for their ratings. They were given the opportunity to modify their ratings or any of the issues based on these discussions.

For the purposes of evaluation, the issues were divided into two groups. The first group was referred to as the human-performance issues and included the following high-level topic areas:

- Role of Personnel and Automation
- Staffing and Training
- Normal Operations Management
- Disturbance and Emergency Management
- Maintenance and Change Management
- Plant Design and Construction

Human-performance issues were evaluated on two primary dimensions: safety significance and immediacy (how soon an issue needs to be addressed).

#### *Safety Significance*

Each issue was evaluated in terms of its *potential* to compromise plant safety. SMEs were asked to consider whether:

- The issue increases the probability of occurrence of an accident?
- The issue increases the consequences of an accident?
- The issue increases the probability of occurrence of a malfunction of equipment important to safety?
- The issue increases the consequences of a malfunction of equipment important to safety?

- The issue creates the possibility of an accident of a different type than any evaluated previously in the industry?
- The issue creates the possibility of a malfunction of equipment important to safety when the malfunction is of a different type than any evaluated previously in the industry?
- The issue reduces the margin of safety?

Safety was then evaluated on the following three-point scale:

1. High likelihood of safety significance - An answer of “yes” to any of the questions listed above led to a rating of “1.”
2. Probably safety significant - If no “yes” responses were given to any of the above questions and at least one was answered “probably,” a rating of “2” was given. A “2” could also be given if the issue represented a significant departure from the status quo and an impact on safety was suspected.
3. Low likelihood of safety significance - A rating of “3” was provided if the answer to all of the above questions was “unlikely.”

In addition to the safety rating, SMEs were asked to provide a brief description of the basis for their evaluation.

#### *Immediacy*

This evaluation dimension identified how soon an issue needs to be addressed. This dimension was evaluated using the following two-point scale:

1. Near-term - Guidance is needed for licensing activities within the next five years.
2. Longer-term - Guidance is not needed for licensing activities within the next five years.

HFE Methods and Tools issues were also evaluated on two primary dimensions: importance to regulatory effectiveness and immediacy.

The second group was the high-level topic area of HFE Methods and Tools. Since this group consisted of methods rather than aspects of NPP design or operations, it had to be evaluated somewhat differently.

#### *Importance to Regulatory Effectiveness Evaluation*

Each issue was evaluated in terms of its likely importance to effective regulatory review. Human factors methods and tools that are applied to the design and evaluation of nuclear power plants are constantly evolving as newer approaches are developed. The designers of new plants are already utilizing these methods and tools which will result in changes to the types of analyses and data that are included in submittals made by applicants. Since HFE reviews conducted in accordance with Chapter 18 of the SRP (NRC, 2007) evaluate the design processes used, these developments have implications for the review criteria needed as well as the methods

used by the staff to conduct reviews. This dimension was evaluated using the following three-point scale:

1. High importance
2. Moderate importance
3. Low Importance

#### *Immediacy*

The methods and tools issues were evaluated for immediacy using the same two-point scale used for the human-performance issues.

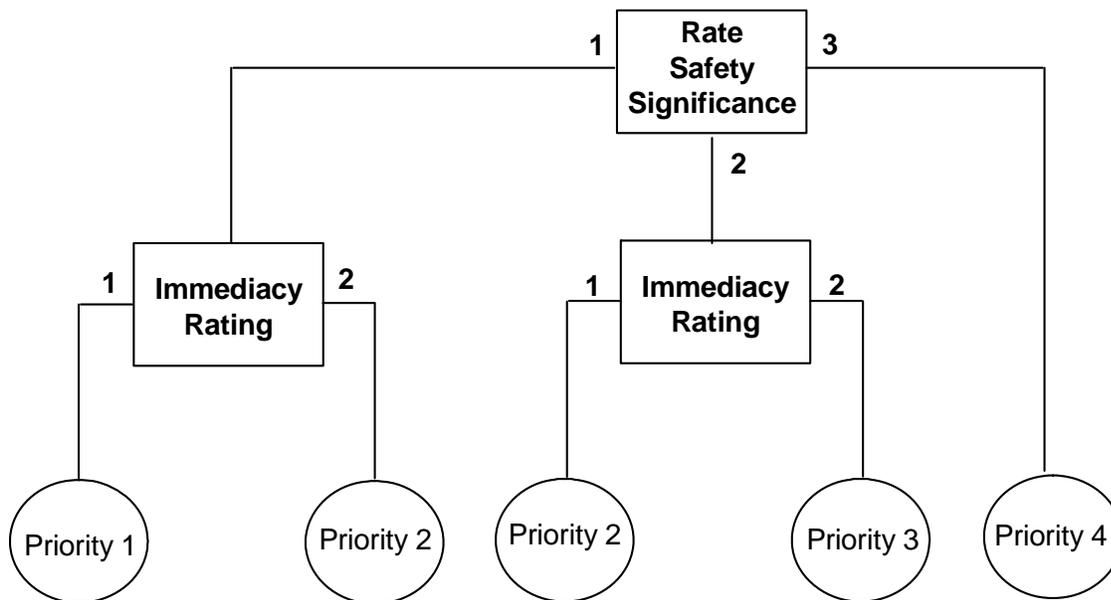
### **5.3.3 Issue Prioritization**

The SME ratings were used to determine each issues priority. This was accomplished in two steps. First, a “summary rating” for each evaluation dimension was calculated. With respect to safety and regulatory effectiveness significance dimensions (rated on a three-point scale), the average of all SME ratings was calculated for each issue. For the purposes of assigning a “summary rating” for each issue, the following criteria were used:

1. An average of 1.5 or less was assigned a summary rating of ‘1’
2. An average of 2.0 or less was assigned a summary rating of ‘2’
3. An average of greater than 2.0 was assigned a summary rating of ‘3’

Issues were assigned a summary rating for the immediacy dimension (rated on a two-point scale) based on which response was most frequent (1 or 2). In the case of ties (i.e., 7 each), a summary rating of ‘2’ was assigned.

In the second step, the ratings were combined using the logic shown in Figure 5-1 to place each issue in one of four priority levels. Priority 1 issues being the most important and Priority 4 issues the least important.



**Figure 5-1 Issue Prioritization Based on Ratings of Safety Significance and Immediacy**

## 5.4 Results

### 5.4.1 Priority Groupings

The number of issues in each of the categories was:

- Priority 1: 20 issues
- Priority 2: 17 issues
- Priority 3: 17 issues
- Priority 4: 10 issues

The issues in each of the four priority categories are listed in Table 5-1. Within each priority category, the issues are listed according to their average significance, with the most significant first.

**Table 5-1 Organization of Issues into Priority Categories**

**Priority 1 Issues**

- Level of Automation
- Operations under Conditions of Degraded I&C
- Design and Evaluation of Digital Systems and Software
- Operating Experience and Lessons Learned
- Validation of Integrated Systems
- Performance-Based Methods
- Information System Design
- Computer-based Procedures
- Interfaces to Automation
- Modeling and Measurement of Effective Team Performance
- Design Process for Higher-Level Interfaces
- Control Design
- Alarm System Design
- Evaluating the Effects of Advanced Systems
- Training and Qualifications
- HRA Methods for Advanced Systems
- Methods to Support the Early Consideration of Human Factors in Plant Design
- Sensors and Condition Monitoring
- Interface Management Design
- Increase in Complexity and Opacity

**Priority 2**

- Guidance for the Review of Intelligent HSIs
- Safety Culture
- Intelligent Agents
- Managing Design and Construction Errors
- Unanticipated Impact of Technology
- Display Design
- HSI Design Deficiencies
- Development of New Task Analysis Methods
- Computerized Operator Support Systems
- Physical Protection, Security, and Safety
- Availability of Operating Experience of Gen. III Reactors
- Change in the Concept of Maintenance
- Digital Communication Networks
- Participatory Ergonomics
- Computation and Simulation
- Diagnostics and Prognostics
- Understanding How HSIs are Really Used

**Priority 3**

- Reduced Staffing
- Managing Human Error in Operations and Maintenance
- Ease of Making System Modifications
- New Hazards

- Crew Member Roles and Responsibilities
- Human Performance Models
- Continuous Fueling
- Modular Plants
- Different Reactivity Effects
- Advanced Controls
- Simplified Maintenance Practices
- Changing Testbeds
- Post-core-melt Mitigation
- Increased Power Operations
- Development of New Function Allocation Methods
- Rapidly Changing HSI Technology
- Functional Staffing Models

#### **Priority 4**

- Computer-supported Collaboration
- Knowledge Gap between Licensee Organization and Supplier
- Development and Application of Knowledge Engineering Techniques
- Collection/Analysis/Use of Real-Time Human Performance Data
- Passive Safety Systems
- More Frequent Changes Due to Obsolescence
- Quantitative Human Performance Criteria
- Rapid Prototyping
- Vendor Diversity and Its Impact on Operational Philosophy
- Modular Construction

#### **5.4.2 Bases for Priority 1 Issues**

Twenty issues were classified as Priority 1, the most important category. Based on information obtained from the SMEs, both from their evaluation sheets and during the meeting discussions, the technical basis for classifying each of these issues as Priority 1 is briefly discussed below. These bases are often closely tied to the issue discussions provided in Section 3. The basis discussions below are meant to illustrate the key aspects of each issue that led to SMEs' giving it a Priority 1 evaluation.

In the issue discussions, links between related issues were often identified. These links are identified as well.

The issues are organized by the high-level topic area in which they belong. It is interesting to note that issues from all but one high-level topic area (Maintenance and Change Management) were represented in the Priority 1 group. The two areas in which most of the issues fell were Normal Operations Management, largely due to advanced HSI technology issues, and Methods and Tools.

#### **Role of Personnel and Automation**

*Level of Automation* – Since automation helps to define the role of the personnel and can be applied to essentially any task, it can affect performance of any of the generic primary tasks. Its

most significant impact is on situation assessment, especially when automation's activities are not clearly visible to operators. Level of Automation is closely coupled to the issues of "Interfaces to Automation" and "Computer-based Procedures", both of which are discussed below. It is also closely tied to the "Development of New Function Allocation Methods", since these methods are used to help determine what aspects of plant operations should be automated.

### Staffing and Training

*Training and Qualifications* – The activities involved with training and qualifications development provide the foundation for personnel to perform their new roles in advanced plant designs and for understanding the new I&C and HSI technology. Thus, training and qualifications development will have broad effects on primary tasks and team performance.

### Normal Operations Management

This area was dominated by issues related to advanced HSI technology. In general, the issues are related to technologies that form the core HSIs used by personnel in the performance of their task.

*Interfaces to Automation* – As the levels of automation in new plants will be varied, the HSI design for interacting at the different levels of automation is a significant aspect of new plant design that is quite different from current designs. HSIs serve to help operators maintain awareness of the automation and monitor its effects. In addition, the HSIs will provide the means for operator to direct automation and interact with it.

*Sensors and Condition Monitoring* – The availability of new sensors and condition monitoring capabilities will have a direct impact on monitoring, detection, and situation assessment. The complementary concerns of information overload (due to the proliferation of sensors) and potential masking of raw data indications due to data integration were identified as important aspects of this issue.

*Alarm System Design* – Since alarm systems monitor the plant and often are the initial means by which plant disturbances are brought to the operator's attention, its design directly affects monitoring, detection, and situation assessment. One specific concern identified is the potential exacerbation of the alarm 'overload' problem resulting from the additional alarms associated with digital systems. The challenges and difficulties of effective alarm system design are highlighted by the fact that human-performance issues related to alarm system design persist in the nuclear industry and many other industries despite efforts to address them.

*Information System Design* – Information is at the core of human performance and the primary determinant of monitoring, detection, and situation assessment. Poor information systems design will significantly impair these cognitive functions. Related considerations are information overload and the extent to which secondary task 'costs' are incurred while accessing information.

*Computer-based Procedures* – Since NPP personnel actions are largely governed by procedures, their design directly affects response-planning tasks. As procedure functions are

increasingly automated, many of the human-performance issues associated with automation pertain to them as well. Other HFE concerns associated with computerized procedure use are usability, navigation, and error detection.

*Control Design* – Operators directly impact the plant through the actions they take at the controls, thus their design directly impacts response implementation tasks. Advanced controls (such as controlling plant processes, systems, and components through screen-based controls) will also affect the secondary task demands associated with accessing and manipulating them. The design of controls is related to the issue of “Operations Under Conditions of Degraded I&C”, since the controls available to personnel may change depending on the type of degraded condition that exists.

*Interface Management Design* – The design of the interface management features of the HSI have a direct impact on operator workload. Performing interface management tasks require operators to divert attention and effort away from their primary tasks, thus the primary task may be negatively impacted.

*Increase in Complexity and Opacity* – Computer-based HSIs are generally based on software that processes lower-level data into higher-level information. Such processing can make the HSI more complex to understand, much more than is the case with “one sensor - one display” approaches typically used in analog control rooms. This can impact situation awareness as it might not be clear to the operators how the information is being processed. Since training on these systems will be a key consideration, this issue is linked to the “Training and Qualifications” issue discussed above.

#### Disturbance and Emergency Management

*Operations Under Conditions of Degraded I&C* – Since the I&C system is the primary means by which personnel obtain information about the plant, its degradation will have a significant impact on the operator’s ability to monitor the plant, detect disturbances, assess the plant situation, and implement their responses. While major I&C failures are likely to be recognized by personnel, more subtle degradations may be overlooked which could lead to the wrong assessment of the plant condition. Another consideration is the need to use backup HSIs in the event of I&C failure.

#### Plant Design and Construction

*Design and Evaluation of Digital Systems and Software* - Design of a digital system has the potential to affect any of the generic primary tasks in highly-computerized plants. Incomplete or inadequate design and evaluation methods may lead to a failure of the I&C system to achieve its mission. Since most of the tasks performed by plant personnel rely on data and information from the I&C system, a poorly designed system can undermine human performance.

#### HFE Methods and Tools

*Operating Experience and Lessons Learned* - Operating experience provides an important basis for establishing the acceptability of new technology, as well as providing the basis for the development of industry guidance, good practices, and regulatory review guidance. Acquiring

this experience and extracting its lessons should be a proactive activity and better analysis may be needed because human performance aspects of experience are too often missed. Thus, this issue is directly tied to “Availability of Operating Experience of Generation III Reactors.”

*HRA Methods for Advanced Systems* – While HRA and PRA are important design and regulatory tools, there are a number of significant deficiencies in current methods when HRA is conducted for new reactors. Deficiencies that need to be addressed include: the lack of methods for dealing with passive systems, the need for better models and quantification, and the need for better human error databases.

*Methods to Support the Early Consideration of Human Factors in Plant Design* – Human performance is an important aspect of plant safety and defense-in-depth. However, it is difficult to evaluate designs in the early conceptual stages for their compatibility with human performance. The availability of such methods may also support early identification of designs that might be more susceptible to human error than others.

*Design Process for Higher-Level Interfaces* – The rapid pace of technology change has resulted in different approaches to HSI design and a wide variety of design solutions. However, the processes used to design them often are not as well defined as was the case for analog HSIs. Regulatory approaches to reviewing the bases for the new designs will be needed.

*Evaluating the Effects of Advanced Systems* – The need to evaluate the effects of advanced systems on human performance, both from design and regulatory perspectives, is an important consideration. Reliable and valid evaluation approaches and criteria will be needed that can address the features and functions of advanced systems. This is closely tied to “Performance-Based Methods” and “Validation of Integrated Systems,” discussed below.

*Performance-Based Methods* – Evaluation methods based on measured performance is an important component in achieving review methods that are neutral with respect to specific technologies that are used in design.

*Validation of Integrated Systems* – Integrated system validation is one specific case of the use of performance-based methods. Evaluating the integrated human-machine system to ensure it meets performance requirements is important to determining the safety of the design. While methods for validation are available, additional work is needed to improve those methods, especially in the area of acceptance criteria.

*Modeling and Measurement of Effective Team Performance* – While teamwork is essential to effective human performance and plant safety, it is generally a neglected aspect of test and evaluation. Understanding teamwork and how to measure it is even more important than the advent of expected staffing reductions and increased application of automation. Team performance is particularly important in the distributed control environment envisioned in future plants.

## 6 SUMMARY AND CONCLUSIONS

This study identified sixty-four potential human performance research issues related to the HFE aspects of the integration of new technology into NPPs. The research issues were organized into seven high-level research topics. The issues were then evaluated and 20 were identified as Priority 1 – the most significant category. These topic areas and the related human performance considerations are potential research issues that could be used to develop guidance.

There are several recurrent themes that cut across many of the topics and issues identified. They are: complexity, roles of personnel and automation, management of human error, and the design and evaluation process. While each was identified as a topic or issue, their pervasiveness deserves mention.

The first recurrent theme is complexity. Although NPP designers are seeking greater simplicity, the HFE aspects of the plant are likely to be more complex than in today's plants. Increases in sensing capabilities, information processing support, intelligent agents, automation, and software mediated interfaces increase the “distance” between personnel and the physical plant. Although these technologies are potentially beneficial, they may sometimes add to complexity for the personnel operating and maintaining the plant.

A second theme is the role of personnel and automation. Many of the issues identified were related to increases in automation and reductions in staff. Increased automation cuts across many aspects of plant operations and maintenance from process control, to decision support, to HSI management, to routine tasks such as keeping logs. Decisions regarding staffing impact the requirements for automation, i.e., all other things being equal, fewer staff can lead to the need for greater automation.

Another theme is the management of human error. Although several specific human error issues were identified, many other issues contained aspects that involve human error. Because the safety implications of human error are well established, management of errors in plant design, software development, construction, maintenance, and operations will be a significant consideration for new designs. Methods to minimize human error, in all aspects of a plant's lifecycle, will be important as will providing personnel with the means to detect and correct errors when they do occur. Designing to minimize and manage errors is part of a fault tolerant design strategy that should be a major focus as new NPPs are designed and built in the U.S.

A fourth theme is the importance of the design and evaluation process. Currently, NRC HFE reviews are process oriented, which is a positive step toward addressing new NPP issues. A process orientation enables acceptance criteria to be relatively technology neutral. This will be extremely important in new NPP reviews because the diversity of reactors, HSIs, and concepts of operation will expand significantly. Because analysis, design, and evaluation methods and tools are rapidly changing, modifications and improvements to the review methods and criteria are necessary.

The “Plant Design and Construction” topic is a relatively new consideration. With the rapid

advance of technology, a more focused approach to this aspect of the design process, especially in minimizing human errors that impact aspects such as software design and plant construction, may be warranted.

Our results also have implications for the NRC's current HFE-related regulations and design review guidance documents. There are at least three aspects of the current guidance that should be evaluated further:

- First, the wording of the regulations and guidance often reflects LWR technology. However, non-light water reactors are viable candidates for near-term deployment, as well as longer-term Generation IV designs. Thus, changes will be needed to address non-LWR designs.
- Second, the regulations and guidance reflect current concepts of operation used in today's plants. For example, the current definition of crew member roles and responsibilities reflect the staffing approaches used in older, less automated plants. Another example is that safety monitoring reflects current approaches and LWR technology, such as in the safety parameter display system requirements. Some new plants may employ new concepts of operation and implement new technologies that may not fit the current review criteria.
- Third, the HFE review process and its guidance may have to be modified to accommodate new design and evaluation approaches, such as the use of human performance modeling for HSI evaluation in place of data collected from actual operations crews. The current review guidance is based on a systems engineering process that itself is changing as new design and evaluation methods and tools become available.

The information obtained in this research can support the development of a long-term strategy and plan for addressing human performance in these areas through regulatory research. Continuing industry developments in the area of human performance will be monitored to identify new and emergent issues so that they can be integrated into the plan as appropriate.

In conclusion, new plants will offer the potential for improvements in performance and safety. However, there are challenges ahead, especially as personnel and technology are integrated into final designs. Although these advances will pose challenges for vendors and licensees, they will present challenges to safety reviewers as well. Addressing these issues will provide the technical basis from which regulatory review guidance can be developed to meet these challenges.

## 7 REFERENCES

- AECL (2002). Control Centre Operational and Technology Trends Survey. April 08, 2002.
- AIAA (1992). *AIAA recommended technical practice - Operational Concept Document Preparation Guidelines*. Reston, VA: American Institute of Aeronautics and Astronautics.
- Allender, L., Kelley, T., Salvi, L., Lockett, J., Headley, D., Promisel, D., Mitchell, D., Richer, C., & Feng, T. (1995). Verification, Validation, and Accreditation of a Soldier-system Modeling Tool. In *Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting* (pp. 1219-1223). San Diego: Human Factors and Ergonomics Society.
- DoD HFE TAG (Human Factors Engineering Technical Advisory Group) (2002). Human Factors "Hot Issues III." May 13, 2002. <<http://hfetag.dtic.mil/>>
- DoD (1985). *Operational Concept Document (DI-ECRS-8x25 (specified in DoD Std.- 2167)*. Washington DC: U.S. Department of Defense.
- DoD (1995). *Software Development and Documentation Standard (MIL-STD-498)*. Washington DC: U.S. Department of Defense.
- DOE (2000). *Nuclear Energy Research Advisory Committee Subcommittee's Long-Term Nuclear Technology Research and Development Plan*. Washington, D.C.: U.S. Department of Energy.
- DOE (2002a) *A Roadmap to Deploy New Nuclear Power Plants in the United States by 2010*. Washington, D.C.: U.S. Department of Energy.
- DOE (2002b) *A Technology Roadmap for Generation IV Nuclear Energy Systems*. Washington, D.C.: U.S. Department of Energy.
- DOE (2003). *The U.S. Generation IV Implementation Strategy Preparing Today for Tomorrow's Energy Needs*. Washington, D.C.: U.S. Department of Energy.
- DOT (2004). *Developing and Using Concept of Operations in Transportation Management Systems*. Washington, D.C.: U.S. Department of Transportation.
- Dudenhoefter, D., Holcomb, D., Hallbert, B., Wood, R., Bond, L., Miller, D., O'Hara, J., Quinn, E., Garcia, H., Arndt, S., & 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.
- Electric Power Research Institute, (2002). *Guideline on Licensing Digital Upgrades (EPRI 102348 Revision 1)*. Palo Alto, CA: Electric Power Research Institute.
- Fairley, R. & Thayer, R. (1977). *The Concept of Operations: The Bridge from Operational Requirements to Technical Specifications*. *Annals of Software Engineering*, 3, 417-432.

- Forsberg, M. (2004). The Ringhals HSI and Control Room Modernization Program: The Practical Application of a Contemporary User and HF Based HSI Design Process. In the *Proceedings of the ANS International Meeting on Instrumentation, Control, and Human Machine Interface Technology*. La Grange Park, Illinois: American Nuclear Society, Inc.
- Golan, A., Judge, G. & Miller, D. (1996). *Maximum Entropy Econometrics: Robust Estimation with Limited Data*. New York: Wiley.
- Gunnarsson, T. & Farbroth, J. (2004). The Control Room Upgrade in the Oskarshamn 1 Modernization Project. In the *Proceedings of the ANS International Meeting on Instrumentation, Control, and Human Machine Interface Technology*. La Grange Park, Illinois: American Nuclear Society, Inc.
- Harmon, D. & Kerch, S. (2004). A Vendor's Perspective on Control Room Modernization. In the *Proceedings of the ANS International Meeting on Instrumentation, Control, and Human Machine Interface Technology*. La Grange Park, Illinois: American Nuclear Society, Inc.
- Higgins, J. & Nasta, K. (1996). *HFE Insights for Advanced Reactors Based Upon Operating Experience* (NUREG/CR-6400). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- Kozak, A. & Malcolm, S. (2004). Development of the Advanced CANDU Reactor Control Center. In the *Proceedings of the ANS International Meeting on Instrumentation, Control, and Human Machine Interface Technology*. La Grange Park, Illinois: American Nuclear Society, Inc.
- Laughery, R. & Persenksy, J. (1994). Network Modeling of Nuclear Operator Procedures. In *Proceedings of the HFES - 38th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.
- Laughery, R., Plott, B., & Persenksy, J. (1996). Micro Saint as a Tool to Determine Necessary Nuclear Power Plant Operating Crew Size. In *1996 ANS International Meeting on Nuclear Plant Instrumentation, Control and Human Interface Technology*. LaGrange Park, IL: American Nuclear Society.
- Lawless, K., Laughery, R. & Persenksy, J. (1995). *Using Micro Saint to Predict Performance in a Nuclear Power Plant Control Room: A Test of Validity and Feasibility* (NUREG/CR-6159). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- Lloyd, R., Boardman, J. & Pullani, S. (2000). *Causes and Significance of Design-Basis Issues at U.S. Nuclear Power Plants* (NUREG-1275, Vol. 14). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- Miller, D., Quinn, T., Arndt, S., Bond, L., Jarrell, D., O'Hara, J., & Wood, R. (2002). *Report of the Instrumentation, Controls and Human-machine Interface (IC&HMI) Technology Workshop*. Washington, D.C.: U.S. Department of Energy.

- NERAC (2000). *Long-Term Planning for Nuclear Energy Research: Long-Term Nuclear Technology Research and Development Plan*. Washington, D.C.: U.S. Department of Energy - Nuclear Energy Research Advisory Committee.
- Nuclear Energy Institute (2000). *Guidelines for 10 CFR 50.59 Implementation* (NEI 96-07, Rev.1). Washington, D.C.: Nuclear Energy Institute.
- NRC (2005). *Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.54(m)* (NUREG-1791). 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. (1999). A quasi-experimental model of complex human-machine system validation. *International Journal of Cognition, Technology, and Work*, 1, 37-46.
- 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., Brown, W., Persensky, J., Lewis, P., Kramer, J., Szabo, A. & Boggi, M. (2008). *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., & 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., 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., Higgins, J., Stubler, W. & Kramer, J. (2000). Automation of Emergency Operating Procedures: Finding the Right Balance. 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., Higgins, J., Stubler, W. & Kramer, J. (2000). *Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6634). 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. (Chapter 7, pp. 139-159).
- O'Hara, J., Stubler, W., Brown, W. & Higgins, J. (1997). *Integrated System Validation: Methodology and Review Criteria* (NUREG/CR-6393). 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.
- 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.
- Papin, B. (2002). Integration of Human Factors Requirements in the Design of Future Plants. *Proceedings of the Enlarged Halden Program Group Meeting – GOL (NOR)*. 09/2002.
- Persensky J. & O'Hara. J. (2005). *Insights into the Role of the Operator in Advanced Reactor Systems*. Washington, DC: U.S. Nuclear Regulatory Commission.
- Risk and Safety Technical Working Group (2002). *Generation IV Roadmap – Crosscutting Risk and Safety R&D Scope Report*. Washington, D.C.: U.S. Department of Energy.
- 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.
- Snow, M., Reising, J., Barry, T., & Harstock, D. (1999). Comparing New Designs with Baselines. *Ergonomics in Design* (October), 28-33.
- Stubler, W., Higgins, J., & Kramer, J. (2000). *Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6636). Washington, D.C: U.S. Nuclear Regulatory Commission.
- 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.

Whitsitt, D. (2004). Comanche Peak Digital Upgrade Project. In the *Proceedings of the ANS International Meeting on Instrumentation, Control, and Human Machine Interface Technology*. La Grange Park, Illinois: American Nuclear Society, Inc.

Wood, R., Antonescu, C., Arndt, S., Britton, C., Brown-VanHoozer, S. Calvert, J. Damiano, B., Easter, J., Freer, M. , Mullens, J., Neal, J., Protopopescu, V., Shaffer, R., Schryver, J., Smith, C. Tucker, R., Uhrig, R., Upadhyaya, B., Wetherington, G., Wilson, T., White, J., & Whitus, B. (2003). *Emerging Technologies in Instrumentation and Controls* (NUREG/CR-6812). Washington, D.C.: U.S. Nuclear Regulatory Commission.

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



*Appendix - Detailed HSI Issues Description*

---

**Appendix Contents**

<b>A.1</b>	<b>Advances in Automation</b> .....	<b>102</b>
<b>A.2</b>	<b>Alarms</b> .....	<b>104</b>
<b>A.3</b>	<b>Information Systems</b> .....	<b>105</b>
<b>A.4</b>	<b>Controls</b> .....	<b>110</b>
<b>A.5</b>	<b>Procedures</b> .....	<b>113</b>
<b>A.6</b>	<b>Computerized Operator Support Systems</b> .....	<b>119</b>
<b>A.7</b>	<b>Interface Management Issues</b> .....	<b>120</b>
<b>A.8</b>	<b>Maintenance</b> .....	<b>134</b>
<b>A.9</b>	<b>References</b> .....	<b>138</b>



## **A.1 Advances in Automation**

Automation was identified in NRC research (O'Hara, Stubler, & Higgins, 1996) as an important emerging issue; however, it was not specifically addressed in guidance development efforts. New digital I&C systems offer the possibility to extend and improve the automation of plant control, and to provide new and more flexible types of personnel interaction with automatic processes; this potentially could improve integration of automatic and human task performance. In addition, digital systems offer new opportunities to extend automation to the human-system interface itself. For example, operators may have the capability to identify specific displays that are automatically retrieved upon predefined plant conditions. Such automation may greatly reduce the workload that operators face to navigate and retrieve displays in the large information systems that will characterize modernized plants.

Operators may play a variety of roles in the control and management of automated systems. Historically, processes were largely either manually controlled or fully autonomous, in which the operator's active role is minimal. Increasingly, intermediate levels of automation are being implemented to support crews to maintain better awareness of the automatic actions, and to be more informed when disturbances in automation arise.

### **A.1.1 Philosophy**

Changes in automation can have a major effect on the role of plant personnel, so it is important to ensure that functional requirements for control have been defined, and that the function allocations take advantage of human strengths and identify those functions that would be negatively affected by human limitations. Such an approach has not been typically followed. Instead, allocations are predominately technology driven, thereby failing to ensure a coherent role for human resources in the plant and resulting in personnel problems summarized below. A user-centered consideration is whether a function should be automated with respect to the human operator's ability to perform as part of the overall plant; i.e., whether the combination of human and system task allocation best serve the overall productivity and safety of the system.

### **A.1.2 Level of Automation**

Designers need a basis for determining the acceptability of a particular level of automation for a given system (intermediate levels of automation). This involves taking into account the reliability of both the operator and the automation, the potential consequences to performance that may result from human and system failures, and the presence of design features and other factors (e.g., training) that may reduce the likelihood and consequences of these failures.

### **A.1.3 Operator Involvement with Higher Levels of Automation**

The automation may perform all required actions and perform them unless the operator takes exception. This approach aims to reduce the operator's range of activities and level of workload by operating for long periods of time without input from the operator. Because little action is required. This can lead to a lack of operator involvement and loss of situational awareness. Thus, a critical design consideration is finding ways to keep the operator involved when using high levels of automation.

#### **A.1.4 Design for Operator Interaction with Automation**

The displays needed for operators to monitor and interact with advanced automatic systems will pose considerable challenges. A better understanding of advanced display design options is needed to support the design of effective displays to mediate human interaction with these more advanced automatic systems. Automation may operate autonomously, but require consent from operators before instituting certain critical procedure steps or phases of operation. This approach keeps the operator involved and aware of system intents while providing opportunities for the operator to intervene if the intended action appears inappropriate. However, to be effective, the operator must be given sufficient information to make an informed decision on the appropriateness of the actions proposed by the automated system. The presentation of this information and the means of user-system interaction are key considerations. In addition, the operator may have to interact with a decision-aiding system to determine why a particular action is being recommended.

#### **A.1.5 Dynamic Function Allocation**

A system may change the allocation of functions between the operator and the automation based on the situation (e.g., an automated system may assume control over lower priority functions as the operator's level of workload increases). This approach can ensure that operators are able to focus attention on functions that are the most important to plant performance, and that the level of workload remains within their capabilities when demands for monitoring plant conditions and executing control actions impose high demands. Two important considerations include defining the levels of function allocation and the means for managing the changes in allocation. For example, the level of allocation may be set by the operator, determined by the automation-based conditional factors, or determined jointly by the operator and the automation.

#### **A.1.6 Opportunities for Human Error**

New opportunities for human errors have emerged. For example, mode errors are an increasing phenomenon associated with automated systems. Automated systems often have a variety of modes in which the inputs used by the automated system and the outputs provided by the automated system are different. Operator inputs may have different effects depending upon the characteristics of each operating mode. Errors result when operators make inputs thinking the system is in one mode when it is in another.

### **A.2 Alarms**

The issues in this section were identified in Brown, O'Hara, and Higgins (2000); O'Hara, Brown, Hallbert, Skråning, Wachtel, and Persensky (2000); and O'Hara, Brown, Higgins, and Stubler, (1994).

#### **A.2.1 General Issues**

### **A.2.1.1 Operator-centered Alarm System Design**

The large number of alarms occurring during a NPP transient overloads the operator's information processing ability. Since fault detection performance decreases as cognitive workload increases, the operator will have a great deal of difficulty handling the flood of alarms associated with process disturbances. The main problems are associated with the limitations of working memory (limited capacity and short duration) and the limited availability of attentional processing resources. As a result, under high workload situations such as NPP transients, signal detection and recognition capability is reduced. The operator samples rather than completely scans alarm information. The operator's information-processing system attempts to handle high workload situations heuristically, which reduces the overall load on the information processing system, but can also lead to human error. In light of these aspects of human information processing and the large amount of alarm information presented in a NPP, the operator-centered objectives of the alarm system should:

- support accurate situation awareness
- minimize the time required to take appropriate action by providing the cues required to activate the operator's mental model which is appropriate to the situation (thus, minimizing the higher-level processing and the information processing burden)
- minimize cognitive workload
- minimize operator error
- support operator-scanning patterns, which may change as workload increases

An understanding is needed of how these objectives can be accomplished.

### **A.2.1.2 Role and Definition of Alarm Systems**

The alarm system is the principle source of information for the detection of a specific off-normal condition. However, in conventional NPPs, it is also used to indicate system/function status and, in this role, also supports a feedback function on the success of actions taken by the operator. Observations of operators have shown that the status indication function of the alarm system is important to them. However, the combining of status indication and alarm functions in a single system has contributed to the difficulty operators have with the system under high alarm density conditions. The number of alarms the operator must deal with can be significantly reduced by separating these functions. In advanced control rooms, such a separation can be easily accommodated. In a conventional control room, replacement of the AWS by an advanced alarm system requires consideration of how to handle the status indication functions of the system. Some problems encountered with early attempts to utilize advanced alarm systems possibly stem from the loss of the status indication function. The relationship between alarm and status indication functions needs further research.

### **A.2.1.3 Lessons Learned and Advanced Alarm Systems**

Analytical studies evaluating the alarm characteristics required to meet the functional requirements of alarm systems have identified a number of features that are generally considered important and, if included, can reduce human error-related plant risk. These include, prioritization, alarm inhibit features, first-out alarms (for reactor and turbine trip), reflash, message legibility/intelligibility, and keying alarms to alarm procedures. While these studies were directed to characteristics of conventional alarm systems, the features represent generic alarm system characteristics. However, in spite of the above, there is a limited empirical basis to recommend specific alarm system design features. Thus, the lessons learned from investigations of conventional alarm systems should be carefully examined for their applicability to the design of advanced alarm systems.

### **A.2.1.4 Context-specific Alarm Response Characteristics**

The response of the alarm system can be made context specific to assist operators. For example, during a significant process disturbance, some operator tasks may be automated, such as silencing the auditory warning of lower priority alarms. This possibility can be considered in an effort to make the alarm system more effective under accident conditions. However, operators must be aware of such changes to the alarm system operating mode or mode errors may result. One way to accomplish this would be to have no change occur without operator request or acknowledgment. The candidate alarm functions for context specific variation and their implementation need additional research.

### **A.2.1.5 Hybrid Systems**

The role of alarm systems in hybrid control rooms (i.e., retrofits of advanced alarm systems into existing conventional control rooms) may differ from that in advanced control rooms. In conventional plants, the alarm system exists as an independent system from an SPDS and other plant data displays. Advanced control rooms will have superior data display, integration, and operator aids. This difference could suggest that more should be expected of advanced alarm systems in hybrid plants than expected in advanced plants.

### **A.2.1.6 Alarm Setpoints and the Alerted Monitor**

Process control operators are in a monitoring environment that has been described in signal detection theory terms as an "alerted-monitor system." This is a two-stage monitoring system with an automated monitor and a human monitor. The automated monitor in a NPP is the alarm system, which monitors the system to detect off-normal conditions. When conditions exceed the criterion of the automated monitor, the human monitor is alerted and must then detect, analyze, and interpret the signal as a false alarm, or a true indication of a plant disturbance. Both the human and automated monitors have their own specific signal detection parameter values for sensitivity and response criterion. Sensitivity for the human monitor is strongly affected by alarm system characteristics, including set points, the presence of nuisance and false alarms, and alarm density. A significant issue associated with alerted-monitor systems is that their optimal overall performance is a function of the interaction of both components. Optimizing the signal detection parameters for one component of the system may not optimize performance of the entire two-stage system. An alarm setpoint philosophy frequently employed

is to attempt to optimize the detection of signals by the automated monitor subsystem. The response criterion is set to maximize the number of disturbances detected. However, this increases the false alarm rate for the automated monitor, which may, in turn, cause the operator to lose confidence in the system and adopt a more conservative criterion and can result in poor overall performance. Further research is needed to understand the optimal integration of the automated and human components of the overall alarm system.

#### **A.2.1.7 Second Event Detection**

Crew awareness of second failures is especially problematic, and the alarm processing techniques had mixed success at improving this aspect of performance. The limitation on second event detection may be the result of the typical human problem solving strategies: (1) scanning is initiated by signals from the alarm system and the operator's attention is split between a variety of data gathering activities, (2) the operator "homes in" on a specific group of indicators and makes an initial diagnosis, (3) the operator's attentional resources seek data confirming the hypothesis, and (4) the operator becomes fixated on the hypothesis and can fail to notice changes in the plant's state or subsequent new developments. The operator's awareness of subsequent failures is hampered by limited information processing resources. Since a primary purpose of an alarm system is alerting operators to failure conditions, this problem needs to be addressed further.

### **A.2.2 Processing Methods and Related Issues**

#### **A.2.2.1 Effects of Processing Methods**

The relative merits of processing methods (such as mode dependency, and state dependency) have not generally been evaluated for their effects on operator performance. In studies of combined processing methods, the results of the research on the effect of alarm processing on operator performance were equivocal, and no clear conclusion emerged. The observed differences in results could be due to many factors, such as type of processing used, degree of filtering achieved, method of data display, and familiarization of the study subjects with the system. Alternatively, the results could be transient dependent, e.g., dependent on the specific scenario or on the operator's ability to recognize a familiar pattern. The effects of processing methods and operator control over their implementation, therefore, remain an issue.

#### **A.2.2.2 Design Goals of Alarm Processing Systems**

Many designers of advanced alarm systems set design goals on the basis of achieving some percentage of alarm filtering, e.g., to reduce by a factor of two the number of alarms during major transients. While this might be reasonable for the application of specific processing approaches, the resulting alarm system might not noticeably improve crew performance. To the human information processing system, reducing incoming alarms by a factor of two may not help at all. Ideally, the design goal for alarm filtering would be stated in terms of the degree of alarm filtering required to improve human performance; however, the information currently available provides no basis for that.

### **A.2.2.3 Alarm Information Availability**

Trade-offs were identified in alarm availability techniques (i.e., filtering, suppression, and priority coding). Filtering eliminates the possibility of less important alarms distracting the operators. However, the designer may be removing otherwise useful information. In addition, the designer must be certain that the processing method is adequately validated and will function appropriately in all plant conditions. Suppression provides the potential benefits of filtering by removing distracting alarms. However, since such alarms are still accessible on auxiliary displays, retrieving them may impose additional secondary task workload. Alarm priority coding does not conceal any information from operators. For example, a system might use color coding to distinguish the importance of the alarm messages, allowing operators to perceptually "filter" alarms, using the priority codes, to identify the higher priority alarm messages. This creates the potential for distraction because it presents alarm messages of all levels of importance. Thus, an issue remains as to which method should be used or in what contexts the various options should be exercised.

### **A.2.2.4 Criteria for Prioritization**

Alarm prioritization schemes can be based on several dimensions such as the overall importance to plant safety or the urgency of operator action. Selecting these dimensions will impact the alarm systems characteristics and operator performance. This issue is also related to the functional basis of the alarm system to provide warnings and status indication.

### **A.2.2.5 Alarm Generation**

Alarm generation techniques create new alarms. The generation of alarm conditions and their resulting alarm messages presents an interesting paradox. Alarm systems should facilitate the reduction of errors, which often reflect the overloaded operator's incomplete processing of information (Norman, 1988; Reason, 1987, 1988, 1990). Alarm generation features may mitigate these problems by calling the operator's attention to plant conditions that are likely to be missed. However, the single most significant problem with alarm systems, is the high number of alarm messages simultaneously presented to the operator. Since alarm generation creates additional alarm messages, it may potentially exacerbate the problem.

### **A.2.2.6 Processing Complexity**

Many significant NPP events, such as the TMI accident, have resulted from complex combinations of problems. The behavior of alarm filtering systems in such complex situations must be addressed when any sophisticated, dynamic processing system is utilized. Since the alarm system is the operator's first indication of process disturbances and operators will confirm the validity of alarm signals prior to taking action, it is essential that operators understand what alarm data means and how it is processed. In addition, operators must understand the bounds and limitations of the system.

## **A.2.3 Display of Alarm Data**

### **A.2.3.1 Alarm Allocation to Display Types**

A spatially dedicated, continuously visible (SDCV) display (such as is provided by conventional tiles) generally is found to be superior to a variable message display (as has been typical of some computer-based text message presentations) during high-density alarm conditions. SDCV displays are often thought to provide perceptual advantages of rapid detection and enhanced pattern recognition. The role of integration of alarm information into process displays and other graphic display forms has not received much research and there is little operating experience upon which to draw. While operators appear to prefer graphic displays that integrate alarm and process information, they have not generally been shown to significantly improve performance beyond message lists. Another consideration is that in advanced control rooms, alarm data will be primarily available to the operator at workstation VDUs; thus, alarm information may not be readily available to the entire operating crew. Issues concerning the proper allocation of alarm functions to displays need to be addressed.

### **A.2.3.2 Design of Video Alarm Displays**

The major attraction of computer-based displays is the flexibility to present alarm information in a wide variety of ways. The research on VDU alarm displays has focused primarily on alarm messages. However, given the problems associated with message lists in high alarm density conditions and operator preference for spatially dedicated displays, further work is needed to explore the appropriate use of graphic displays of alarm information (possibly in combination with message lists). The organization of alarms by system and function was preferred by operators and improved their performance. Approaches should be considered to preserve this display approach in VDU alarm displays. In general, the design of VDU displays for presentation of alarms needs further consideration.

### **A.2.3.3 Information Content of Alarm Displays**

When alarms occur, operators must determine whether the signal represents an actual or spurious event. The low probability of significant off-normal events in NPPs, and therefore, low expectancy, can make operator acceptance of certain alarms difficult or slow. After verifying several consistent indicators, the operator will take appropriate action. In broader terms, alarms are sometimes used in groups to diagnose faults. The specific information needed in alarms to accomplish alarm functions and how it should be presented needs additional research. Too little information, makes the alarm system less useful. Too much information, makes it cumbersome to use.

### **A.2.3.4 Hierarchical Displays, Alarm Integration, and Data Layers**

Related to the issue above is the question of how to present alarm information to operators; e.g., as single messages, data layers, or integrated into other displays. One way of reducing the flood of alarms that operators must deal with in process disturbances is to provide alarm information in hierarchical displays; e.g., by integrating lower level alarm information into higher-order alarms. If such a system is to be effective, it must integrate alarms into meaningful units and represent units that the operator would have developed without the system. Another

method is to present the data in layers, with more detailed information in supplemental displays. Such an approach may lower the operator alarm processing workload but it could also increase the operator's interface management workload (Baker, 1985). Thus, while data layering, organization into display hierarchies, and alarm integration should facilitate operator information processing, their implementation may pose challenges for operators that limit their effectiveness. More advanced display techniques for alarm data require further investigation.

#### **A.2.3.5 Use of Auditory Cues**

The auditory characteristics of alarms often are problematic; i.e., they can be startling and distracting. More appropriate and acceptable methods of using tonal cues need to be identified. While the visual features of alarm systems are often overwhelming, the operator's ability to extract information from auditory cues has probably not been fully exploited. For example, zonal auditory cuing (used in many plants already) can facilitate the operator's location of alarms. Auditory cues in advanced alarm systems may not have to provide spatial cues, but may be used to convey other information, such as alarm priority or alarm system/function.

#### **A.2.3.6 Speech Displays**

Whether speech displays can be effectively used in the acoustically crowded NPP control room, must be investigated. The advantages of speech-based alarms in supervisory control tasks is presumed to include their attention-capturing potential, reduction in demands on the visual information channel, ease of understanding the importance and meaning of the message, lack of training required, and public nature of the message. However, studies of these effects have been inconclusive.

### **A.2.4 Alarm System Controls**

Control interfaces for advanced alarm systems have not been systematically investigated. However, the application of computer technology to alarm systems poses several problems.

#### **A.2.4.1 Increased Complexity with Advanced Alarm Systems**

The NPP industry has recommended separate SART (silence, acknowledge, reset, test) controls for conventional alarm systems. The controls of advanced systems may be much more complicated, and will require investigation. While the separate SART philosophy may also apply to advanced systems, additional controls may be required for features such as operator-defined alarms, operator adjustment of limits, and operator control of filtering. The identification and use of these control options is an issue in the design of advanced alarm systems.

#### **A.2.4.2. Role of Automation**

In certain situations, such as accidents, some operator controls may be automated, such as the silencing of lower priority alarms. However, operators must be aware of these changes in the alarm system operating mode or mode errors may follow. One way to accomplish this would be to allow no changes without operator request or acknowledgment. In general, the most appropriate control functions for automation need to be determined along with their

implementation methods. (This issue is related to the Context Specific Alarm Response Characteristics issue identified above.)

#### **A.2.4.3 Implementation of Input and Control Devices in Advanced Alarm Systems**

In advanced control rooms, alarm systems will be integrated with other interfaces, such as process displays or computer based procedures. Thus, alarms may share input interfaces with these HSIs, for example, keyboard entry of temporary setpoints. Other alarm control functions may have dedicated control devices, such as SART controls. The mixture of "soft" and hard controls and dedicated vs. shared interfaces needs to be addressed.

#### **A.2.5 Considerations for the Conduct of Research on Alarm Systems**

Several considerations for alarm system research are identified in this section, including unit of analysis, test condition dynamics, type of simulator, test participants, and performance measurement.

##### **A.2.5.1 Unit of Analysis**

Many of the studies described above contained experimental confounds between the alarm system features employed. That is, the unit of analysis was the comparison between alarm systems differing along several dimensions, rather than individual alarm system features. This complicates the understanding of the effects of individual aspects of alarm systems on crew performance.

##### **A.2.5.2 Test Condition Dynamics**

Most features of alarm systems should be tested in dynamic rather than static conditions; i.e., where alarm states actively change as opposed to fixed and invariant alarm display presentation. There is a role for static mock-ups, but the information processing issues can best be evaluated under dynamic conditions.

##### **A.2.5.3 Type of Simulator**

Validity concerns are associated with alarm system research when it is conducted using alarm system simulators or part-task simulation, rather than full-mission simulators. This is because alarm information is pulled out of the full context of all the other information typically available to operations. Alarms are a part of the plant's information system and operators use alarm information in conjunction with other information available to them to decide on appropriate action. When alarm system information is presented by itself, it becomes the sole focus of the operator's attention and the sole source of information (without the assistance and the distraction of the rest of the control room). Thus, it may not be representative of the way operators use alarm systems in the information-rich context of an actual control room. In a sense, the system's importance is greatly exaggerated. This does not imply that there is no role for alarm simulators in alarm research, only that their limitations must be carefully understood and considered in the context of the questions being addressed.

#### **A.2.5.4 Test Participants**

The use of novice participants in alarm system studies can be problematic since they will approach a simulated task and process information differently than experts. The influences of the expert's mental model and the availability of skill-based processing make the expert qualitatively different from the novice. Again, this does not imply there is no role for novice participants for selected studies. However, where the study attempts to test integrated alarm characteristics in a full-mission context, only expert participants would be appropriate.

#### **A.2.5.5 Performance Measurement**

A methodological weakness in many studies was the absence of a comprehensive performance measurement methodology that focuses on operator cognitive processes as well as operator tasks and system performance. Most of the alarm system studies reviewed focused on the measurement of operator performance in terms of detection time, time required to take appropriate action, and error. While these are indeed important performance parameters, a comprehensive performance measurement approach reflecting the cognitive nature of a supervisory control task is needed. Thus, in addition to primary tasks (e.g., detection of secondary disturbances/malfunctions) and system measures (e.g., critical safety function status), the approach to evaluation of alarm characteristics should include measures of cognitive factors, such as situation awareness, cognitive workload (e.g., load on attentional resources and working memory), and secondary task workload (e.g., managing the HSI). Throughout this discussion, references to potential additional analyses and research have been made. These are summarized below:

- analysis of eye-track data to better understand the use of the alarm system in different scenarios
- inclusion of more extensive alarm processing and further investigation of alarm processing categories to determine their effects on alarm reduction and performance
- examination of alarm displays combining tiles, integrated alarms, and alarm messages (with improved message-list designs), and methods for making smooth and efficient transitions between them
- examination of the role of alarm systems in conventional vs. advanced control rooms (including an examination of "no alarm" and "alarm only conditions")
- research on what makes scenarios easy or difficult for operators to successfully handle and implications for alarm system design

### **A.3 Information Systems**

The issues in this section were identified in O'Hara, Higgins, and Kramer (2000).

#### **A.3.1 Lack of a Well-defined Ecological Interface Design Process**

While the ecological interface design (EID) approach may be a promising advance in the system-engineering process, the development of a well-defined process for conducting an

analysis using the abstraction hierarchy is important to its broader application to the design process.

### **A.3.2 Lack of Specific Representation Guidance**

The research on advanced graphic forms has not yet yielded substantial or definitive bases for designing effective ecological interfaces.

### **A.3.3 Evaluation of Operating Experience**

For those interfaces based on EID that have been installed in operating facilities, there needs to be a thorough assessment of the operating experience, and how it applies to the interfaces. Such experience is important to the formulation of design review criteria to address EID aspects of the HSI.

### **A.3.4 Critical Testing and Evaluation of Ecological Interface Design Concepts**

There is little thorough research that carefully assesses the various aspects of EID; e.g., information requirements, effect of organization of information along functional lines, display representation, and use of analytical redundancy. Studies tend to confound these characteristics, or provide weak assessments of the contribution of these various aspects of EID.

Successful handling of unplanned-unanticipated events with interfaces based on EID, under actual operational conditions in complex systems, has not been demonstrated. Further research is also necessary to more clearly identify which cells of the abstraction-aggregation (A-A) matrix are important to operations.

### **A.3.5 Display Evaluation**

More comprehensive methods of display evaluation are needed. For example, the lack of definitive review guidance will need to be compensated for with dynamic evaluations. The criteria for the evaluations will have to be addressed. For example, signal detection approaches have been recommended; i.e., an examination of hits, false alarms, and misses because some subjects may be less conservative using configural displays under certain situations, so that the hits, as well as the false alarms, increase (Hansen, 1995).

There were ten issues identified in the Design Review area.

#### **A.3.5.1 Task and Temporal Considerations**

The A-A matrix and the EID approach address the plant at a functional level rather than on a task or temporal basis. However, the importance of presenting information consistent with task requirements has been a fundamental basis of the systems approach, and deviations were identified as a problematic aspect of many new plant information systems; i.e., where information is organized around plant systems, rather than operator tasks.

Much of the operators' goal-directed activity is centered around temporal constraints. This is one reason operators like trend displays. The operators' tasks unfold along a temporal continuum with some tasks being performed in parallel and some sequential. This temporal dimension to operations may be lacking from the A-A analysis, except insofar as some time is reflected in higher-level information such as rates.

Additionally, the EID approach seems to be built around functional decomposition of means-ends relationships. It is unclear how well this can be applied to common tasks and disturbances, which are highly proceduralized needs. While it is important to be able to address unanticipated and unplanned events, most things are well planned and the information system needs to support those.

The proper role of task-based information in display design and how it is integrated into the EID approach needs to be addressed.

### **A.3.5.2 Information Volume**

Due to the extensive analytical process used for EID, there is the potential that the process, including the A-A matrix, may identify too much information to be practically displayed. Also, too many display pages may be required to satisfy EID information requirements.

### **A.3.5.3 Display Information Density**

The increase in information may be linked to an increase in the information density of individual displays. While this may minimize the need for interface management tasks, such as navigating to retrieve additional display pages, the density may be associated with lack of salience of important information. Another issue with dense displays is that, for any given operator task, the amount of irrelevant information increases, and from a human performance perspective, performance decreases as the amount of irrelevant data increases (Mitchell & Miller, 1983).

### **A.3.5.4 Operator Use of a Large Span and Variety of Displays**

Operators of advanced NPPs are likely to have to choose from a large variety of displays presented at different levels. Several questions will have to be addressed to ensure the effectiveness of information presentation:

- How does the designer decide how many displays are enough?
- Have the operators been given too much information, either in a single display or in the entire suite of displays?
- Will the operators be able to select the appropriate display for the tasks at hand? Will operators tend to choose a few "favorite" displays, even though they may not be the most appropriate for the tasks?
- If operators do switch displays based on varied tasks, will they pick the proper display?
- What sort of training should be developed to address these concerns?

#### **A.3.5.5 System Complexity and Emergent Features**

It is observed that as the number of vertices in a polygon display increased, the displays became complex, and performance can be reduced. Further, emergent features can be affected by unpredictable interactions between component parts and produce unintended effects that may be misunderstood (Hansen, 1995). This illustrates the issue of increasing the complexity of the underlying domain to which integral and configural displays map. For complex dynamic systems, such as NPPs, not much is known about the dynamics aspect of the emergent features that may be used to represent them. In addition, as the graphic representation increases in complexity, the display grammar will itself become quite complex.

#### **A.3.5.6 Perceptual Resolution**

Configural and integral displays require a perceptual process to take place, such as the recognition of a change in an emergent feature. However, the degree to which a geometric form needs to change before it is perceived as a distortion is not well understood.

#### **A.3.5.7 Configural Display Elements**

Research has suggested that configural displays could be enhanced, especially in support of focused tasks, by (for example) the inclusion of digital information. Research is needed to better understand the effects of display elements on performance, and the effects of their interactions with other display types.

#### **A.3.5.8 Effect of Instrumentation Failures**

The effects of instrumentation failures on EID displays have been recognized as a potentially significant problem. There are several associated sub-issues:

- Can operators detect a failure of instrumentation?
- Can instrument failures result in representations that are interpreted by operators as real process failures; and, perhaps more importantly, can real process failures be misinterpreted as instrument failures?
- If operators do detect a failure, should use of the display be suspended?
- Since the display integrates many parameters into a single display, what is the effect of its loss on operations and how effectively can operators transition to backup displays?

It is worth noting that many designers have implemented advanced features that do address instrumentation failures to some extent. For example, the concepts of redundancy and diversity in instrumentation were shown to be quite powerful when coupled with automatic parameter validation and appropriate notification of operators when instruments fail their validation.

#### **A.3.5.9 Information Organization**

The issues related to display page organization and network organization remain as important research topics.

#### **A.3.5.10 Integration of Ecological Interface Design into Remainder of Interface**

The integration of a new and significantly different EID into the remainder of the standard HSI of a control room is an important consideration that needs attention. There were three operator related issues.

#### **A.3.5.11 Training and Qualification Implications**

Christoffersen et al. (1995) stated that "...to experience the benefits of EID, it seems likely that operators need to be trained to think functionally rather than procedurally. It would seem that this would require a fundamental shift in NPP operation philosophy...it may be that operators have to possess certain types of cognitive characteristics that may not be considered in the traditional selection process in the nuclear industry" (p. 143). Concern has also been expressed that EID interfaces may inhibit long-term learning and retention (Wickens, 1992).

Also, for any display, where the information is sophisticated and a large amount of information is consolidated into one or a few figures, the training requirements become very important. One needs to understand all aspects of the display and how it reacts to various operational transients, accidents, and instrument failures. The long-term effects of EID type displays on operator performance and strategies are unknown.

Also, the training aspects of Design Review Issue 4, Operator Use of a Large Span and Variety of Displays, should be addressed.

#### **A.3.5.12 Operator Acceptance**

The issue of operator acceptance of a new and different type of display (such as one based on EID) is also important, as indicated by the operator comments during experiments. One interesting idea was noted during the Rankine cycle experiments, relative to introducing the displays initially in training and then perhaps gradually introducing them into the plant.

#### **A.3.5.13 Internal vs. External Mental Models**

The issue of the appropriate model(s) to apply as a basis of display design was discussed. How to choosing a model that accurately characterizes the process and its supporting systems, yet appropriately reflects the training, experience, and cognitive capabilities of the users, is an important question. Designing displays that characterize the system in ways that may not reflect the cognitive requirements of plant operators to perform situation awareness (SA), monitoring and detection, response planning and response execution, may degrade performance. Achieving this balance will require additional research.

## **A.4 Controls**

The issues in this section were identified in Stubler, O'Hara, and Kramer (2000).

### **A.4.1 Time Delays and Control Stability**

Given the potential time delays in digital systems and the sequential nature of soft control actions, research is needed to better understand the relationship between time delays and performance stability, especially under emergency conditions. Where delays affect performance, methods to support operator performance should be identified.

### **A.4.2 Input and Feedback Methods for Continuous-Variable Inputs**

Industry experience has shown that the entry of numerical values is error prone, especially when using a keyboard or keypad. However, the popularity of the keyboard as an input device suggests that it may have some advantages (such as speed) compared to other methods, such as arrow keys and soft sliders. Feedback regarding the magnitude of entered values can support the detection and correction of input errors. Two common feedback methods are digital readouts and bar charts. More information is needed regarding the relative advantages of combinations of input and feedback methods. Questions include:

- What are the relative error rates for inputs provided via keyboard, arrow keys, and sliders when they are paired with feedback from digital readouts and bar charts?
- What are the speed versus accuracy tradeoffs between these methods?
- For example, does a keyboard and bar chart combination yield superior performance in terms of both time and errors?
- Do interfaces that combine these features support or inhibit performance (e.g., sliders that incorporate arrow keys)?
- For arrow-button applications, how is operator performance affected by the use of such features as: separate sets of arrow buttons for large and small changes in input values or adaptive-gain features that allow the change produced by a button press to vary as a function of another variable?

### **A.4.3 Confirmation and Warning Messages**

Both confirmation and error messages are prone to problems associated with the level of specification of operator actions. For example, operators may confirm that the desired action is correct but not realize that the goal (e.g., the object being acted upon) may be wrong. Similarly, when receiving an error or warning message, users often are not able to interpret the true cause of the problem.

### **A.4.4 Sequential Plant Control and Interface Management Tasks**

Many plant control tasks are sequential, and different tasks can have similar but different sequences. For example, some pumps require closing a downstream valve before starting the

pumps. Other pumps require opening it. In addition, sequential operators are often involved in the use of soft controls (e.g., the operator must access a selection display, select a component, open an input field, and then enter the input value). Industry experience suggests that the sequential constraints of soft control access can interact with the sequential nature of control tasks. The result can increase the likelihood of capture errors (i.e., starting one task sequence and finishing with another), and of mis-ordered action sequences (i.e., performing actions in the wrong sequence).

#### **A.4.5 Access to One Versus Multiple Input Fields at One Time**

More research may be needed on the potential benefits and costs associated with providing operator access to one input field at a time, versus multiple input fields simultaneously. Some alternative approaches may include displays that provide access to groups of controls, tools for managing multiple open input fields, and methods for gaining serial access more quickly and accurately.

#### **A.4.6 Intelligent Agents**

These are computer programs that perform information processing tasks for the operator in a somewhat autonomous manner. They are currently being developed to perform information management tasks in chemical plants with a user-initiated notification concept. Intelligent agents can help the operator manage suspended tasks. However, the potential benefits must be weighed against operator burdens associated with supervising these agents, and any potential problems that may result from their inappropriate application.

#### **A.4.7 Interaction of Soft Controls with Automation**

Increases in automation of computer-based systems pose greater cognitive demands on operators, especially for understanding and maintaining awareness of their status and behavior. Soft controls play an important role in conveying status information to operators and allowing them to interact with these automated systems. However, automation may also affect the appearance and behavior of controls and displays. Human factors review guidance is needed to address the interaction of soft controls with automation.

#### **A.4.8 Soft Controls and Display Space**

The amount and type of display space provided through the HSI is important for supporting control and monitoring tasks. For example, assigning controls to dedicated display devices can improve access time by reducing the need to perform display navigation tasks. Increasing the number of display devices can reduce conflicts between demands for short-term control actions and long-term monitoring actions. Also, having additional display devices allows operators to more easily track tasks that have been temporarily suspended. Human factors review guidance is needed to address the minimum amount of display space needed to support soft control use and the trade-offs between providing dedicated display devices and general-purpose ones.

#### **A.4.9 Keyboards versus Incremental Input Devices**

Many soft controls used in process control applications provide the operator with the choice of changing control values via arrow buttons or via a keyboard. Keyboard entry may provide some performance benefits. However, industry experience suggests that entry via keyboard is more prone to error. For example, large-magnitude input errors may result from typing errors. Further research is needed to examine the error rates associated with data entry via keyboards versus incremental input devices, especially when combined with features for error prevention, detection, correction, and recovery.

#### **A.4.10 Consistency of Soft Controls in Hybrid Interfaces**

A hybrid HSI may contain a variety of soft controls, especially if they were installed as a series of independent modifications rather than an integrated effort. In a hybrid HSI containing multiple soft control devices, operators are expected to make frequent switches between different tasks with different interfaces. Studies of computer-based systems have produced some conflicting results regarding the effects of consistency. Thus, the goal of trying to maximize consistency between user interfaces may be counter productive if the wrong type of consistency is achieved. Further research is needed to understand the dimensions of consistency that are important for reducing errors and ensuring effective operator performance across a variety of soft controls in a hybrid HSI.

### **A.5 Procedures**

The issues in this section were identified in O'Hara, Higgins, Stubler, and Kramer (2000), and Roth and O'Hara (2002).

#### **A.5.1 Methods and Criteria for the Evaluation of Computer-based Procedure Effects**

Definitive conclusions about the value of CBP systems are hampered by the lack of operational experience with their use, and lack of quality experimental evaluations. The detailed methodological considerations for validation of complex human-machine systems and a conceptual approach to validation were discussed. The methodology focused on (1) establishing the requirements for making a logical and defensible inference from validation tests to predict integrated system performance under actual operating conditions, and, (2) identifying the aspects of validation methodology that are important to the inference process. The technical basis for inference in validation is based upon four general forms of validity: system representation, performance representation, test design, and statistical conclusion.

The studies generally did not perform well-controlled comprehensive evaluations. Such studies should provide valuable data to better understand the impact of CBP effects under a wide range of scenarios and complex situations, using varied personnel and system measures. However, most studies reviewed had methodological weaknesses that limited the conclusiveness and generalization ability of the results. Thus, important questions remain (many are addressed in more detail in the issues below). A good comprehensive evaluation of CBPs and their effects on crew performance has yet to be performed.

The issue of criteria for CBP acceptance needs to be addressed from both research and regulatory review perspective. Many authors specified that such systems should improve performance, while others indicated that performance should not be degraded (implying that equivalent performance with paper procedures and CBPs is acceptable). This is an extremely important distinction because of the impact on performance that would be necessary for CBPs to be required to improve performance.

### **A.5.2 Role of Plant Personnel in Procedure Management**

Procedures are guidance to operators for achieving high-level objectives. While they provide correct guidance most of the time, for the situations analyzed, procedure adaptation may be necessary in some situations. Thus, operators must remain as independent supervisors who manage procedure implementation and independently assess their appropriateness to the current situation. Operators need to understand the overall purpose of the procedures, stay cognitively involved with their progress, and question procedure steps that may be inconsistent with the procedure's overall goals. However, CBPs have the potential to work against this independence and minimize the operator's role. They may increase the tendency to follow procedures without a critical independent perspective, and may even be a deterrent to operator action. Addressing these concerns has both design and training implications.

Another issue that needs to be addressed is how to design and review CBP systems that enable the operators to maintain an independent perspective so they can recognize the procedure's contribution to achieving higher-level safety goals. At the same time, the CBP system should reduce operator workload, automate distracting and lower-level error prone tasks, and monitor crew performance, especially when the crew and CBPs disagree. Equally important is the issue of how to train operators in handling this role while using CBPs. The knowledge required to manage a CBP system may be different from that required to handle conventional procedures. For example, the CBP system may use different analyses to resolve logic steps than the operators use.

### **A.5.3 Team Performance**

Research has shown that CBPs may have a significant effect on crew member roles, teamwork, and communication (O'Hara & Roth, 2005; Roth & O'Hara, 2002). Teamwork is an important element of defense-in-depth. Operators work as a team to support SA, error detection and recovery. The extent to which the roles and communication are changed may be greater than anticipated. Since senior reactor operators (SROs) using CBPs can handle a procedure almost completely on their own, communication between the SRO and reactor operator (RO) may be reduced. While this is not in itself good or bad, its impact on team performance needs to be assessed. When the SRO is using a CBP, board operators have identified the importance of communication to maintaining effective teamwork and expressed a need to be aware of the status of emergency operating procedures (EOPs). Thus, the potential for isolation of the CBP user from the other operators, and changes in the roles and responsibilities of the operators may undermine team performance in emergency conditions. This type of effect on team performance has been noted for many aspects of computer-based HSI technology (Stubler & O'Hara, 1996). The following is a summary of that discussion.

The function of supporting coordination of crew activities addresses the need for crew members to maintain awareness of the activities of other crew members to support teamwork. The control room provides the context within personnel convey, directly and indirectly, their intentions and actions to other crew members. Advanced control rooms, especially those with individual workstations, may tend to isolate operators, making an individual's information and control actions less visible to others; thus, reducing team effectiveness.

Salas et al. (1992) define a team as "...two or more people who interact, dynamically, interdependently and adaptively toward a common and valued goal/objective/mission; who have each been assigned specific roles or functions to perform " (p. 4). In a control room setting, the operating crew is a team in which the members must share information and perform their tasks in a coordinated fashion to satisfy specific goals or mission requirements. This requires a common understanding of the status of the system and an understanding of each other's actions and intentions. The following team behaviors have been identified as important to team performance: identification and resolution of errors, coordinated information exchange, and team reinforcement (Oser et al., 1989). Successful teams actively located errors, questioned improper procedures, and monitored the status of others. In a study of ship navigation (Hutchins, 1990), team performance was discussed in terms of facilitating error checking by others, allowing others to assist when needed, and supporting training in the work setting.

Hutchins found that work environments that evolved over many years using traditional technologies contain characteristics that contribute to team performance. However, when computer-based technologies are introduced, these positive characteristics may be compromised. Hutchins described these characteristics using the terms horizon of observation, openness of tools, and openness of interaction.

*Horizon of Observation* - This refers to the portion of the team task that can be seen or heard by each individual. It results from the arrangement of the work environment (e.g., proximity of team members) and is influenced by the openness of tools and interactions. By making portions of a task more observable, other team members can monitor for errors of intent and implementation, and situations in which additional assistance may be helpful.

*Openness of Tools* - This is the degree to which an observer can infer information about another crew member's ongoing tasks through observation of a tool's use. Open tools show characteristics of the problem domain that provide an observer with a context for understanding what has been done and the possible implications.

*Openness of Interaction* - This is the degree to which the interactions between team members allow others with relevant information to make contributions. Openness of interaction depends on the nature of communication (e.g., discussing actions or decisions in the presence of others) and the style of interaction (e.g., the degree to which unsolicited input is accepted). Openness of interaction is also influenced by characteristics of the work environment (e.g., openness of tools, horizon of observation) that provide other team members with an opportunity to see and hear the interactions.

Conventional control room designs typically provide a broad horizon of observation that facilitates the observation of team activities. In addition, they may be "open tools" in the sense that an observer can infer information about control actions (e.g., which plant system was

involved, which control was operated, and what action was taken) by observing the operator's location at a control panel and the action performed. Interaction may be considered "open" because most interactions involve verbal communication that can be heard from across the control room.

Advanced HSI technologies, such as CBPs, have the potential to impair these positive characteristics. For example, the use of an individual computer-based workstation for CBP operation may reduce the horizon of observation by providing the operator with an individual view of the plant that cannot be readily viewed by others, and may entail less-open styles of communication. Also, the openness of tools may be impaired by implementing methods of user-system interaction that convey less task-related information to observers, compared to conventional tools, such as paper procedures.

#### **A.5.4 Situation Awareness, Response Planning, and Operator Error**

The effect of CBPs on operator situation awareness has not been carefully evaluated. Operators need to maintain several levels of situation awareness when using procedures, including assessment of:

- procedure steps, how procedures are structured, one's location within a procedure or between a set of procedures
- the appropriateness of procedures to achieve high-level procedure goals
- the overall plant situation

Some concern over lowered situation awareness with CBPs was identified (Roth & O'Hara, 1998). Conventional procedures require operators to monitor plant indications. If plant indications are present in the CBP, the operator may not feel the need to look at other sources of information and may miss important indications that are not present in the CBP (Stubler, Higgins, & O'Hara, 1996). The situation awareness of other operators is affected as well. For example, Spurgin et al. (1990) noted that SROs use CBPs as their primary way of following the overall plant condition rather than relying on information from crew members. The other crew members expressed concern about being aware of the EOP status.

The discussion thus far has focused on SA and awareness of plant personnel. Another interesting aspect of situation awareness is the "awareness" of the operators and the CBP of each others' actions (Jeffroy & Charron, 1997). A divergence of each others "understanding" of the situation can occur when operators depart from the recommendations of the CBP. This creates a situation that makes it difficult for operators to recognize the constraints on the CBP system. Hence, they may not understand the information provided, or the effects of their actions on the procedure's interpretation of procedure steps.

Research is needed to address the effects of CBPs on these different levels of situation awareness, the crew's ability to detect errors in the CBP, and response-plan adaptation in the face of procedure failures. In addition, the effect of CBPs on the number and types of operator errors (especially where errors are not defined in terms of verbatim compliance) needs to be examined.

Impacting situation awareness are two related issues: complexity and level of abstraction. Research on COSSs has emphasized that computerized support systems add to plant complexity. Operators need to have a good mental model or understanding of the computer-based system in order to properly monitor and supervise the CBP. Failure to account for this aspect of operations can lead to poor situation awareness and a sense of being out-of-the-loop.

Roth & O'Hara (1998) observed that too little information presented at each procedure step can cause operators to lose a sense of where they are, while too much detail may be a distraction. The level of abstraction in which procedure step results are presented will impact the operators' SA.

### **A.5.5 Level of Automation of Procedure Functions**

The human-performance issues associated with automation have been well documented (see O'Hara, Stubler, & Higgins, 1996, for a discussion of general automation issues). Table 4.1 of the CBP report presented a list of procedure-related functions in terms of several levels of automation. The choices of levels of automation for each, and their implementation will impact operator performance, situation awareness, workload, and errors. For example, Blackman and Nelson (1988) found that when the selection of procedures was automated, operator involvement was reduced. Operators reported that they thought less and acted as switch turners. A better understanding is needed of the tradeoffs between procedure function automation and operator involvement, independence, and supervisory control.

One area of procedure automation is especially noteworthy. One important capability of CBP systems is the analysis of procedure step logic; that is, the comparison of actual parameter values to the reference value identified in procedures using the logical relationships described in the step. When the step logic or the actual data analysis required to evaluate the step logic is under-specified, both the procedure and the operator can incorrectly assess the situation. Therefore, great care has to be taken in the design and evaluation of procedures, especially EOPs, to guard against under specification of step analyses. Where operator judgment is involved, such analyses are better done manually.

### **A.5.6 Keyhole Effects and Use of Multiple Computer-based Procedures**

The characteristic of viewing information through the limited area provided by VDUs has been referred to as the "keyhole effect" (Woods et al., 1990). The consequence of the keyhole effect is that, at any given time, most of the information is hidden from view. Therefore, operators must know what information and controls are available in the computer system, where they are, and how to navigate and retrieve them.

The keyhole effect has been identified as a root cause of many of the known performance challenges (O'Hara & Brown, 2002). If insufficient viewing area is available for operators to perform their tasks, they may have to repeat navigation tasks frequently. A problem related to the keyhole effect is that access to controls and displays tends to be serial; e.g., only a few controls can be accessed at one time. This is in contrast to the parallel presentation of controls and displays in conventional control rooms. The sheer interface-management burden of navigating and retrieving many displays can interfere with the operators' ability to obtain an

overview of the plant situation. If workload is already high, operators may decide not to retrieve all the information they may need, so they can invest their mental resources in their current task.

With respect to CBPs, this issue may become significant when operators are required to be in multiple procedures. Hoecker et al. (1994 & 1996) noted that when the operators are required to access information in parallel, the CBP system can increase workload. Lack of parallel access to information is a limitation of the keyhole effect. Because only a portion of the procedure can be observed at one time, operators may lose a sense of where they are within the total set of active procedures. The available display space may be inadequate to support simultaneous viewing of multiple procedures and the associated plant data.

### **A.5.7 Computer-based Procedures Failure in Complex Situations**

Ensuring the transfer from CBPs to paper procedures has been identified as an important consideration in the design and evaluation of CBP's. This transition may be easily accomplished when the procedure context is simple, such as when operators are in the first few steps of a procedure. However, the transition may be quite complex if operators are deep into the procedures; or when there are multiple procedures open, many steps completed, many steps of continuously applicability, time-dependent steps, and parameter-dependent steps are being monitored by the CBPs. How operators will manage failures in such complex situations is unknown.

### **A.5.8 Hybrid Procedure Systems**

Some CBP systems computerize all plant procedures while others computerize only certain procedures, such as EOPs. The ability to use CBPs effectively when they are designed for emergencies only may be an issue (IAEA, 1994). It has also been noted that CBPs should be consistent with normal, daily operations as well. While one might argue that the EOPs are not used in normal daily operations, it is the computerization of EOPs and the use and functionality of the system that may present difficulty, if it is unlike other systems in the control room.

### **A.5.9 Specific Computer-Based Procedure Design Features**

The relative effects of specific CBP design features on performance were not addressed in most studies reviewed. Most were overall system comparisons, e.g., CBP vs. paper-based procedure (PBP), and not systematic evaluations of individual characteristics. In addition, concern was expressed over generalizing PBP guidance to CBPs.

As an example of this issue, traditional procedure formats may require modifications when implemented on a computer. As noted in Section 4, two primary formats are used for procedures: text and flowcharts. While both have been successful in paper form, Chignell and Zuberec (1993) have questioned whether flowchart procedure presentations are acceptable in computer media where the limited screen view and need for scrolling may make them less effective. Similarly, reading extended text from VDUs, in general studies, has been found to be visually fatiguing. The proper implementation of CBPs in text and flowchart formats may require some additional guidance from that available in paper form. The effects of HSI techniques, such as outline views, navigational aids, and highlighting on text and flowchart formats, needs to be determined.

## **A.6 Computerized Operator Support Systems**

Computerized operator support systems (COSSs) were identified in NRC research (O'Hara, Stubler, & Higgins, 1996) as an important emerging issue; however, it was not specifically addressed in guidance development efforts. COSSs are systems that help operations and maintenance staffs to monitor, make decisions, and plan actions. They support tasks such as:

- plant performance and condition monitoring (e.g., efficiency of main pumps, turbine, and generator)
- core monitoring (e.g., neutron flux)
- early-fault detection and diagnosis
- safety-function monitoring
- plant control
- maintenance monitoring

### **A.6.1 Applications for Enhanced COSS Capabilities**

While first-generation COSS systems have been around for some time, the new digital I&C infrastructure in modernized plants provides a basis on which second-generation systems can be developed. Digital I&C information can be coupled with predictive models and fast-time simulations to provide plant personnel with much better decision support than previously possible. As the ability to provide COSS expands, an issue emerges in identifying, from an operator-performance perspective, the tasks most in need of, and amenable to, computerized support.

### **A.6.2 Impediments to Effective Use**

To be successful, these second-generation COSSs must also overcome some of the obstacles to effective use that characterized earlier systems. Studies of operational experience with COSSs have identified several such issues including; poor integration with personnel task performance, complexity of COSS information processing, lack of transparency of the COSS decision process, inadequate explanatory information to address personnel verification needs, absence of communication facilities to permit personnel to query the system or obtain a level of confident information about the conclusions drawn. These issues need to be addressed so that effective methods for designing COSSs and integrating them into plant work practices and procedures (see below) can be developed.

### **A.6.3 Integration**

Several studies recommended that for COSSs to be effective, they must be well integrated into everyday operations. Further, operators may require more than occasional simulator training to become familiar enough with COSSs to use them. According to the IAEA (1994), operator effectiveness in using the COSS requires that the system be used not only in the very specific conditions for which it was designed, but also in normal operation. For maximum compatibility with the global HSI, it is necessary to integrate the data produced by the COSS into the

procedures used by the operators for normal operations, as well as in the specific abnormal or emergency conditions for which the COSS may have been designed (p. 31).

## **A.7 Interface Management Issues**

The issues in this section were identified in O'Hara and Brown (2002).

### **A.7.1 The Relationship between Interface Management and Primary Task**

In Section 3.3.2, Advanced Human System Interfaces, the topic of Interface Management Design was defined, along with the concepts for primary tasks and interface management (or secondary) tasks. O'Hara and Brown (2002) identified several ways the performance of these tasks can impact each other. However, two basic questions remain unsatisfactorily answered:

- How much time and cognitive resources can be taken from the primary task by the interface management task before primary task performance becomes affected?
- How well can the primary task be performed if interface management tasks are not performed?

Under high workload conditions, operators make decision about when to shift between primary and secondary tasks as part of their workload management strategies. This process needs to be better understood. Under what conditions do operators decide to abandon interface management tasks, and when do they decide that some interface management tasks again are needed? In general, a better understanding of how operators manage or regulate their workload and make performance tradeoffs, especially during complex process disturbances, is required as a technical basis to address the performance limitations of computer-based HSI systems. As a corollary, it is important to identify the strategies operators adopt to minimize the demands of interface management tasks, such as decreasing the inherent flexibility of the HSI, enhancing its appearance and behavior, and increasing the simplicity of its configurations. A related consideration is how to measure the use of these strategies and their effects on plant performance.

### **A.7.2 Cognitive Resources of Primary and Secondary Task Performance**

One of the root causes for the secondary task effects summarized above is that the interface management and supervisory control tasks demand the same cognitive resources. For example, they both rely heavily on visual perception of stimuli, processing of symbolic data, and manual manipulation of a limited set of input devices and formats. The relationship between the cognitive resources required of primary and secondary tasks can affect performance, specifically impacting the operator's ability to engage in dual-task performance where attention is divided between the two types of tasks. For example, if the same cognitive resources are required for controlling the plant, then during periods of high demand, one task may suffer as resources are directed to the other. However, if different cognitive resources are required for them, then it is less likely that one task will interfere with the other, and overall operator performance may be enhanced. Thus, a better assessment is needed of these resources and the role of decoupling the resources required for primary and secondary task performance. For

example, shifting interface management tasks to take advantage of resources that are less in demand (for example, speech as a navigational input) may facilitate dual-task performance.

### **A.7.3 The Relationship between the Keyhole Effect and Display Area**

The keyhole effect causes many challenges associated with computer-mediated interaction with complex systems. The limited display area provided by workstation visual displays (and perhaps group-view displays as well) can impose the burden of navigating and retrieving many displays, and also impede operators' efforts to obtain an overview of the plant situation. Thus, a better definition is needed of the difficulties associated with the keyhole effect.

A question that is fundamental to HSI design reviews is, "How can or should the necessary number of VDUs be determined?" In the authors' experience with both NRC design reviews and with other design efforts, the number of VDUs is usually determined long before the information content of the display system has been designed. No practical guidance appears to exist for determining the needed amount of display space. For example, even simple heuristics such as the ratio of display screens to display pages, do not appear to be used. Instead, the design decision tends to be driven by factors that are not directly related to the information needs of the operator, such as the size of the control console. Given the problems associated with the keyhole effect, there does not seem to be adequate consideration of the display area that will be required in a control room to support crew operations under high workload conditions. Thus, a frequent complaint of operators is that they need additional VDUs in their control room.

The keyhole effect and its relationship to the number of VDUs need to be investigated further. The rationale for determining display area also needs further examination. Consideration of these two issues should lead to guidance for the review of this performance concern.

Criteria are also needed for calculating acceptable limits for the information-access costs associated with displays and display networks. When developing a control room, designers are faced with a tradeoff between concentrating information in a limited number of display devices, or providing it via multiple display devices. Each approach has potential benefits and costs. Using a small number of display devices may be beneficial for reducing the size of control console and panels and reducing the physical distance between display devices. One potential cost is more substantially complex display networks due to the increased number of display pages that must be accessible from each device. These more complex networks may impose greater navigation demands on users for accessing desired displays. The alternative approach is to provide more display devices with fewer pages assigned to each device. For example, each display device may contain a subset of pages (e.g., from a major branch of the display network) that relate to a specific set of operator tasks, rather than the entire network. This approach has the potential benefit of reducing the complexity of the display navigation task since fewer steps may be required to access a particular page, while the displays for tasks that are in progress may be left in place, rather than removed. Previous studies and interviews with operators have shown a clear preference for multiple, dedicated display devices. However, an increased number of display devices entails increased physical navigation between them. Thus, the tradeoff between the number of display devices and the complexity of the network may be modeled as an inverted U-shaped function, in which user performance is optimized for some intermediate level of display devices and network complexity. Outside this optimum

range, performance decreases, as either the number of display devices is increased or the complexity of the display network increases. Rapid and easy access to displays is important for managing multiple concurrent tasks (e.g., operators must be able to check the status of one system while controlling another). Therefore, guidance is needed on this tradeoff - particularly, the points at which performance may become unacceptable, and the factors that may mitigate these effects.

#### **A.7.4 Display Density versus Display Clutter**

Better metrics are needed for defining display clutter and better criteria for determining levels of acceptability. Visual clutter in computer-based displays has long been considered an obstacle to user performance. Visual clutter and the presence of distracting information in a display increases the difficulty of a visual search by requiring the user to focus on many individual items to identify those relevant to a particular task. It increases information access cost by increasing the effort required to search for, and identify, desired items of information. Visual clutter also can increase the distance between such information items, causing task-related information to be located on different display pages, or in separate areas of the same page. This increased distance heightens the demands associated with finding and mentally integrating information.

While it is desirable to minimize or eliminate visual clutter, attention has traditionally been focused on display density - the quantity of information per unit area on a display screen. However, display density is an indirect measure of clutter. Other factors may be more important than density in determining whether content will have negative effects on user performance. The first consideration is whether or not the items in a display are task-related (i.e., used together for tasks). The proximity compatibility principle (Wickens & Carswell, 1995; 1997) states that the information access cost (in terms of time and effort required) is decreased when task-related information is in close spatial proximity, while the presence of information that is unrelated to the task causes display clutter, thereby increasing information access costs. Placing task-related information items together on the same screen, rather than on separate screens, can reduce the need for display navigation. Placing task-related information items closer together within a display can enhance the speed and accuracy of integrating information. Other important considerations include visibility and legibility of information items, ease of locating items, and the ease of accessing and manipulating them (e.g., selecting items with a pointing device).

Techniques that support mental integration of displayed items, such as placing task-related items close together, grouping task-related items, and integrating alphanumeric and graphics into visual objects, may enhance performance while actually increasing display density. Newer display forms, such as integral formats and configural display formats, may greatly increase display density while reducing information access costs and improving user performance (O'Hara, Higgins, & Kramer, 2000). Resolving possible tradeoffs is an issue because there are no clear criteria that take these considerations into account in computer-based display formats, such as integral formats and configural display formats.

#### **A.7.5 Flexibility versus Performance Tradeoff**

Flexibility of the HSI was another root cause of many of the challenges to performance identified in this report. The management and manipulation of flexible user interface features requires

cognitive resources that operators may not want to take from the primary task. Additional research is needed on the tradeoff between HSI flexibility and interface task demands.

Conventional control rooms tend to have inflexible display systems; that is, the indicators themselves cannot be manipulated or configured for their location, content, or presentation format. The display systems reflect the designer's best understanding as to what information operators will need, in what sequence, and in what display format. The display system may be adequate for most tasks, but not exactly right for anyone. Operators may need to transition between multiple displays to get all the information they need for the task at hand.

A desirable aspect of the flexibility of many computer-based systems is that operators can better tailor the displays and workstation resources to meet the requirements of a specific task. It is difficult for designers to anticipate all the operators' information needs and provide displays that meet those needs. Flexibility in the HSI gives operators the ability to perform task-specific tailoring so the displays more closely approximate what is needed.

Flexible user-interface features have been introduced in response to earlier design approaches that assumed a stereotypical user population - a group of individuals having characteristics, needs, preferences, and abilities that were highly similar or nearly identical. These approaches failed to adequately consider the range of performance that may result from differences in expertise, personality traits, demographic characteristics, and physiological attributes. Computer-based technologies provide opportunities for making systems adjustable and adaptable to users and situations. However, designing more personalized systems that many people can use, yet remain responsive to individual needs, is an elusive goal (DoD, 1996).

Users always have tailored the interfaces of their systems to some degree. Two categories of flexibility may be considered in design reviews. Inherent flexibility of the HSI technology includes ways of modifying the HSI that were not specifically intended by its designers. For example, a computer-based display system may use the scroll bar to create a landmark for locating information in large tables (Watts, 1994). Designed flexibility includes features specifically created by the designer to give the user flexibility in using the HSI. For example, a computer-based display system may allow operators to select plant variables and scales to plot operator-defined trends. However, the types of flexible features and their degree are likely to change as computer-based HSI technologies advance.

A further distinction may be made between flexibility features that (1) can be directly modified manually by users, and (2) those that incorporate automation (DoD, 1996). For the former, the user determines the need for a change in the HSI and then carries out the change. Some direct-user modification features for displays include features for moving display pages or soft controls, to particular display devices and features for creating operator-defined trend displays. A direct-user modification feature for controls may allow an operator to provide inputs as a single, compound command, rather than as individual commands in response to a series of prompts. The disadvantages of direct-user modification of the HSI include the following:

- additional learning requirements for new users
- increased difficulty for casual users in making modifications (e.g., supervisory personnel may experience difficulty setting up or viewing user-defined trend graphs)

- trade-offs in time and effort associated with setting up a flexible feature and completing a task
- difficulty in over-the-shoulder viewing of flexible features (e.g., by supervisory personnel)
- difficulties in coordinating the use of a flexible feature among multiple personnel

Flexible HSI features that incorporate automation may adjust the HSI based on plant conditions, user behavior, or both. Adaptive modeling (DoD, 1996) refers to a system's ability to alter the user interface (1) for specific individuals, based on their preferences, past behavior, and performance, or (2) to meet changing needs of the user based on current task demands. A computer-based model of the user is employed to predict the user's interface management needs and support adjustments of the HSI. This model may contain a profile of the user's characteristics and a program for determining interface management needs. This model may be manually updated by a system administrator or accomplished automatically based on the system's monitoring of the user's behavior. Such systems may recognize differences in expertise of users and act accordingly (e.g., providing assistance to novices each time they make mistakes, but assisting experts only upon request).

An example of a flexibility feature that incorporates automation may be a display configuration system that automatically provides the operator with a set of displays tailored to plant conditions. In such systems, automation may serve two functions: identifying the need for a change, and executing it (Sheridan, 1997). Various combinations of these two functions are possible. For example, the automation may identify the need but let the operator execute it, or vice versa: alternatively, the automation may do both. In these cases, additional cognitive burdens are imposed on the operator for anticipating the actions of the automation and understanding the changes afterwards. For example, after the automation has acted, the operator must determine why it acted and whether the result is correct. When these actions are not anticipated by the operator, additional cognitive demands may be involved in shifting attention to the flexible feature and recognizing its actions. Based on the observations of Segal and Wickens (1990) and those of Norman and Bobrow (1975), HSI features that support planning and expectation should be encouraged, but features that draw attention unnecessarily (i.e., cause distractions) may be undesirable. Examples of attentional distractions may include (1) flexible user interface features that require excessive operator attention when they automatically change displays, and (2) interface features that give little feedback when they produce a change thus requiring the operator to divert attention away from what they are doing to determine whether a change has occurred.

There are many factors that affect the use of flexible features by operators. However, users are more likely to employ a particular feature when it provides a potential benefit to task performance, when its benefit is perceived to be worth the effort to execute, and when its use is not prohibited by organizational policies. Sperandio (1978) has described some of the potential benefits of flexibility. They are described in the paragraphs below.

In field investigations of air traffic control, Sperandio observed that controllers shifted their work objectives as the traffic in their air sectors increased; that is, they focused on their higher priority objectives, such as safety, and neglected lower priority objectives. Coincident with the shift in work objectives, the controllers made changes in the types of information they sought and their methods for performing actions. Sperandio observed that information that is pertinent at low

and moderate workload levels may not be usable during high workload levels due to the operators' adjustments in their work methods and objectives. He stated that personnel performance may be negatively affected if the HSI characteristics are unevenly adapted to the controller's strategies. He also stated that the flexibility of computer-based technologies may enhance operator performance by allowing the HSI to provide the right information for the operator's current work methods and work objectives, while removing unneeded information that may become a nuisance. Designing HSI features to accomplish this requires a knowledge of task requirements and strategies used by personnel for modifying work methods in response to changes in external task load.

These findings also are applicable to NPP operations. For example, operators have many objectives when operating a NPP. During plant transients, the primary goal of maintaining safety may override other considerations, such as protection of investment in equipment, and productivity (cost-efficient power generation). Changes in work methods that occur during transients affect the types of information that operators must gather and the means they use for gathering it. Therefore, computer-based HSI technologies should support the gathering and processing of information for a broad range of workloads. The inherent flexibility of computer-based technologies may be beneficial for ensuring that information and control capabilities are provided in ways consistent with the methods used by operators during the various workloads.

The high-level design review principle of Flexibility in Appendix A.4 of NUREG-0700, Rev. 2 (O'Hara et al., 2002) states that flexibility should be limited to situations in which it offers advantages in task performance, but should not be provided for its own sake. This is because there are tradeoffs between the benefits of flexibility, and the costs it imposes on operators. These human performance costs to individual operators include (1) interface management demands, such as the degree to which the workload associated with using the flexible feature diverts cognitive resources from the primary tasks, and (2) the effects that the flexibility have on the primary task (i.e., the degree to which changes to the HSI brought about by flexibility impair the operator's ability to perform the primary tasks). There also may be human performance costs when other crew members must view or use HSI components that have been modified by others. Examples include (1) difficulty in using shared HSI components, and (2) difficulty in over-the-shoulder supervision (e.g., a shift supervisor may have difficulty viewing a display that has been modified by the operator) (DoD, 1996).

Another aspect of the dual-task effects discussed above is that flexible HSI features make interface management tasks more dependent on controlled information processing. Woods (1993) noted the cognitive tradeoffs associated with the flexibility of computer-based interfaces were noted previously. Operators must decide what information they want, how to retrieve it, what HSI to utilize to retrieve it, where and how it should be displayed, and they must coordinate the existing displays with the new information. To the extent that the control room and workstations provide dedicated HSIs with no flexibility, the HSI is highly predictable. If the environment is constant, the mental model of the HSI becomes highly detailed; its location, form, and function of the HSI becomes very predictable. Then, the operator's interface management tasks become highly automated. Flexibility and reconfiguration ability work against predictability and automaticity.

As an example, consider monitoring functions. In conventional control rooms, operators get a good overview of the plant functions and systems through a quick glance at the annunciator tiles. This is possible because human pattern recognition capabilities are very powerful. Once the location and arrangement of the tiles is learned, operators no longer have to read the individual tiles to comprehend the overall status. Contrast this with a computer-based control room having a message list system that is not organized by functions and systems. There are no identifiable patterns to recognize at a glance because of the lack of spatial dedication (except, perhaps, the severity of the condition based on the number of incoming alarms). With such an alarm system, determining that there is a problem requires reading individual alarm messages, a much more effortful task than glancing at tile displays. Interface management tasks can be automated to the extent that the interface is predictable.

Another human performance consideration associated with the lack of predictability of the HSI stems from its flexibility. That is, in a spatially dedicated control room, operators know what information is located on the various panels. In a virtual workspace, when operators view a VDU, they do not necessarily know what is displayed because the display context can change. If the displays on a specific VDU are frequently changed or tailored, then operators must examine each display screen to see what is included; this requires controlled information processing capability. If operators fail to perform this recognition task, they may misidentify the display. Thus, situation assessment can be hampered by such errors.

In general, highly predictable HSIs do not have to be thought about a great deal, and can be largely addressed by the operator's automatic information processing resources. This discussion is not intended to suggest that flexibility is a negative feature and should be avoided. The positive aspects of flexibility were noted above. What is important is that there are tradeoffs between the workload associated with flexibility and its beneficial characteristics, and a balance between the two is needed; however, guidance is lacking on how to achieve this balance.

Therefore, the flexible user-interface features provided should be the result of careful analyses of user requirements. A flexible user interface feature should address the need to optimize operator performance under specific conditions. Designers should not include them as a way of avoiding analyses of user requirements. That is, designers should not avoid the work of analyzing operator requirements by setting up a design that can be used in many different ways. Flexibility without proper analysis can expose the operator to configurations that may impair performance, thereby increasing the likelihood of errors or delays.

### **A.7.6 Mental Models and Display Organization**

Well-developed mental models are needed for accurate situation assessment and good performance. These mental models improve performance by enabling the HSI to be predictable and enabling operator performance to become less effortful and guided more by expectations. A key in the ability of operators to perform interface management tasks effectively is their mental model of the organization and behavior of the HSI. While organizing controls and displays around plant systems may have been adequate for conventional control rooms, it may pose difficulties in computer-based control rooms. For example, a system-based organization may be rather easy to understand, but may require excessive work for display retrieval when the system-based organization of displays does not match operator task requirements (e.g., tasks require interactions with displays and controls from multiple systems). Alternative models have

been proposed but their level of acceptability is not known. Research must address the issue of providing a display organization that leads to an acceptable interface management load, so that operators can easily retrieve the information they need for acceptable primary task performance.

### **A.7.7 Effects of Information Access Costs on Routine Monitoring**

Additional research is needed to determine the degree to which information access costs may negatively affect the frequency and accuracy with which operators routinely monitor the status of plant systems. One root cause for the negative effects of secondary tasks upon primary tasks is that they demand the same cognitive resources at the same time. Thus, if the same cognitive resources are required for both manipulating the HSI and controlling the plant, then during periods of high demand, one task may suffer as resources are directed to the other. However, if different cognitive resources are required for these two tasks, then it is less likely that one task will interfere with the other, and, consequently, a higher overall level of performance may be maintained. Additional research is needed to explore approaches for performing interface management tasks and to assess their acceptability and potential benefits for using them in a control room.

Operators are less likely to perform an interface-management activity if they do not expect the benefits to outweigh the associated costs (e.g., time and effort). Just as the design of displays (e.g., the keyhole effect) can increase information access cost and reduce the likelihood of monitoring, the design of interface management controls may also increase such costs. As a result, operators may be less likely to perform routine monitoring if the controls are difficult or awkward to operate (e.g., poorly placed relative to the operator or associated displays, awkward means of operation, or not reliable in operation). For example, a display device with touch interface located outside of the operator's immediate reach may be monitored less often than one within easy reach. Also, if actuation using an input device is not highly reliable (i.e., an operator may have to press a button multiple times to select a desired display), the display may not be monitored as frequently as displays that are easier to operate. It is necessary therefore, to consider the extent to which monitoring frequency may decrease as a result of control device characteristics, and the acceptable limits for these characteristics.

### **A.7.8 Role of Conventional and Computer-based Interfaces**

It has been observed that operators may prefer conventional HSIs under high workloads. Consequently, there is often a migration toward including more conventional equipment into control rooms that start out being based completely on advanced technologies. This has been true of several advanced NPP control rooms (such as ABWR and EDF N4). Heslinga and Herbert (1995) likewise noted:

It was a general finding that introducing a new HMI (human-machine interface) in an existing situation where both old and new systems are available leads to a situation where the old systems continues to be used. This occurs particularly in disturbance situations where operators tend to return to well-known information sources.

The desire for the conventional HSIs may reflect a preference for the types of display and control designs (such as gauges and J-handles) in analog HSIs. More likely, the characteristics

of spatially dedicated, parallel presentations of controls and displays may be more appropriate to control tasks than those of non-spatially dedicated, flexible, virtual controls and displays. The relative role of conventional and computer-based HSIs and the design characteristics that are important to these preferences need to be better understood.

### **A.7.9 The Effects of Interface Design Features on Interface Management Task Performance**

The detailed design of HSIs affects the performance of interface management tasks. Below are issues associated with different aspects of HSI design. NUREG-0700 gives guidance on many aspects of these HSIs. However, the issues below are focused more on interface management aspects, as well as the relationships between multiple HSI components in a control room. Further, the overall focus of these issues would be to reduce interface-management workload, while maintaining high HSI situation awareness.

#### **A.7.9.1 Relative Comparisons of Human-system Interfaces**

What are the relative advantages of different HSI design features for supporting interface management tasks?

#### **A.7.9.2 Command Language Interfaces**

Command dialogues have some advantages compared to other dialogues, such as menus. For example, it may be possible to retrieve a display in a single step by entering an identification code rather than through a set of steps in a series of hierarchically arranged menu screens. Commands also have drawbacks, such as increased demands on the user's memory for recall and susceptibility to input error; e.g., incorrect or transposed letters or digits. There are design trends away from command language dialogues and toward direct manipulation and menu-based systems. However, many studies found information retrieval is better using command language dialogues. Thus, guidance is needed on their appropriate use that should consider the skill level of trained operators and the fact that multiple interaction methods may be available at the same time. Much of the current literature addresses only novice users. Research has shown that command names should be evaluated as a set, rather than individually. Many factors, such as name set effects (relationships between individual commands, size of set), task conditions, and user population characteristics can affect the ability of users to recall commands. Additional guidance is needed for determining the acceptability of command name sets. The use of command dialogues also may be affected by such features as on-line help and undo commands. In addition, some command dialog systems allow users to abbreviate or customize commands. The acceptability of these features remains to be determined. Owing to the effects of contextual factors such as name set, task conditions, and user population characteristics, system developers relied heavily on tests and evaluations to ensure that command dialogues can be used effectively. Many protocols for evaluating command dialogues were developed for text-processing tasks that may not be relevant to NPP operations. In addition, simplistic approaches to measuring task times and errors may overlook the range of consequences of different types of errors or delays associated with command usage. Thus, development of tests and evaluations of command dialogues for NPP HSIs is an issue.

### **A.7.9.3 Menus**

A menu is a type of dialogue in which a user selects one item out of a list of displayed alternatives by actions such as pointing and clicking, entering an associated option code, or activating an adjacent function key. Menu interfaces have gained widespread use in many computer-based systems. By presenting the user with a set of options, menus can reduce cognitive demands (e.g., the need to recognize rather than recall options). Many menu systems reduce the set of options to those relevant to the current situation. However, menus can pose potential problems for users. For example, studies have shown that as menus increase in size, the time required to access items may increase greatly. Users may be unable to determine the location of, or successfully retrieve, desired items. Research and operating experience identified several factors that affect user performance with menus, including techniques for depicting the display network and the user's current location, techniques for highlighting relevant options, and "look ahead" features that indicate options that can be accessed from a current one. The appropriate use of these features in NPP interfaces is an issue.

### **A.7.9.4 Direct Manipulation Interfaces**

Direct manipulation interfaces, especially those that are object-oriented, are being adopted into a broad range of human-computer interfaces in many domains. They are potentially beneficial in reducing mental demands associated with interpreting display information and executing actions. Potential applications in NPP HSIs may include display icons (e.g., icons in mimic displays), displays for organizing information based on metaphors (e.g., the desktop metaphor), and interfaces for managing display windows. Direct manipulation interfaces rely heavily on the use of metaphors and analogies. Because users and designers may have different mental models, users may interpret the interface in ways that are different from the designer's intentions. In addition, metaphors may have limited applicability. Usually, there are situations in which the metaphor is not consistent with the task domain (e.g., the metaphor suggests actions that are not supported by the HSI or are inconsistent with the operation of the plant). This may lead to problems in learning or using the interface. In addition, these interfaces may be prone to errors that differ from those of more conventional display interfaces (e.g., an input action may be legal with respect to the user interface, but undesirable for the task domain). A better understanding is needed of how the characteristics of direct-manipulation formats contribute to their effectiveness.

### **A.7.9.5 Function Keys, Programmable Keys, and Macros**

The use of these HSI design features may support increased automation of interface management tasks. Their advantages and disadvantages need to be defined, and their potential to increase the probability of errors assessed.

### **A.7.9.6 Query Language, Natural Language, and Question and Answer Dialogues**

Query language, and question and answer dialogues have a long history as user interfaces in computer systems, especially for interrogating databases. Natural-language interfaces have a more recent history. All three methods use conversation metaphors for interacting with the computer and inputs are usually entered as text strings via a keyboard. Question and answer dialogues are slow; users must wait for the system to ask questions before expressing their

needs. Query-language interfaces have developed special terms and grammars that must be used when generating requests. High mental demands are associated with determining the type of processing (information sorting) that is desired and then translating the request into query language. In addition, execution errors are associated with keyboard entry of queries. Natural-language interfaces were developed to reduce the cognitive demands of formulating inputs. Compared to query-language systems, inputs to natural-language systems more closely resemble the types of phrases used in normal communication. However, owing to the complexity and ambiguity of natural languages, these interfaces still require special, restricted terms and grammar. Users still encounter difficulty in determining the type of processing (information sorting) that is desired, and then translating the request into an expression that will be understood by the computer system. In addition, requests expressed in natural language may be lengthy, which may increase operator response time and impose high demands on keyboard entry skills. If such technologies are used in NPP HSIs, it must be determined that burdens associated with query language, natural language, and question and answer dialogues do not detract the operator from tasks that are more directly involved in assessing and controlling the plant.

#### **A.7.9.7 Speech**

One of the problems associated with computer-based HSI interface management is that it shares the same cognitive resources as supervisory control tasks. Speech offers an alternative cognitive resource that may lessen competition with primary tasks that are performed using the HSI. However, the possible conflicts need to be assessed between speech as an HSI input mode, and speech during operator communication tasks.

#### **A.7.9.8 Navigation of Display Networks**

The issue of “Mental Models and Display Organization” above, addresses appropriate organizational approaches for NPP displays. Related to that issue is what navigation features support the use of the displays. Navigation methods that are based on spatial principles can require operators to access multiple displays before reaching the desired one. Multiple navigation methods (e.g., menus, commands, direct manipulation methods) within a single display system require users to conceptualize paths to the target display. It also introduces opportunities for navigation errors that can affect the operators’ ability to monitor plant condition or to respond promptly to changes. A goal of display system design is to support the user in developing an accurate understanding of how data is organized, which navigation paths are available, and how the system will respond to user inputs. This is called the user’s conceptual model. Conceptual models for display navigation support users in understanding the relationships between display pages, planning paths to needed data, and developing appropriate courses of action in novel situations. A variety of design approaches can support the user in developing conceptual models for display navigation, such as metaphors (e.g., desktop metaphors), overview displays that depict the organization of the display network, display landmarks, and display-page designation schemes that indicate relationships between them. The user’s conceptual model of the display system may differ from that of the designer, leading to the development of features that do not support an appropriate conceptual model of the display system. The appropriate use of these design approaches for supporting operator understanding and use of the display system needs to be defined, especially with regard to understanding the structure of the display network and planning and executing navigation paths.

#### **A.7.9.9 Navigation of Large Display Pages**

Large display pages present large amounts of related data together, which reduces the need for operators to access many individual pages. In NPPs, large displays with graphical data may include overviews of the display network, mimic displays (e.g., plant system representations), flowcharts (e.g., representations of procedure steps), and maps (e.g., a representation of the physical arrangement of equipment in the containment building). Large displays with non-graphical data may include text displays, such as tables of plant data with long columns and many rows. In some cases, display pages are too large to be viewed at once from a single display screen with a level of resolution that is sufficient for user tasks. For example, if the page were reduced to fit the available space of the display device, the text and other details would be too small to read. Navigation techniques for finding and retrieving items from large display pages include non-distortion-oriented techniques (e.g., scrolling, paging, zooming and panning, hierarchical paging) and distortion-oriented techniques (e.g., fisheye views that show both detail and context). While these techniques contain features for enhancing user orientation and retrieval, they also impose new demands. Human factors guidance is needed to address these techniques, including their appropriate use, potential benefits, and characteristics for reducing orientation and retrieval errors.

#### **A.7.9.10 Hypertext and Hypermedia**

Hypertext-based systems consist of information nodes connected by organizational and relational links. Nodes may vary in size, content, and format. While hypertext systems can provide rapid access to information, studies have shown that they are associated with disorientation (difficulty determining current location), and difficulty in identifying paths to desired information. In addition to difficulties with navigating between nodes, problems have been associated with managing windows that contain retrieved nodes and finding information within large nodes. Guidance is needed on the appropriate use of hypertext and specific characteristics, such as network structure, orientation aids (e.g., overview displays, landmarks), retrieval features (e.g., bookmarks, histories, “previous node” buttons, and features that support users in determining whether a node should be accessed), window management, and retrieval of information. In addition, guidance is needed about the appropriate use of hypermedia capabilities that can show information in a variety of media, including text, graphics (still and animated), video, audio, and executable programs.

#### **A.7.9.11 Use of Windows and View Arrangement Features**

Operators adjust the way that items are presented in the display system to make them easier to view. Two of these tasks include de-cluttering displays and display windows. The ability to do this allows a high volume of data to be presented when needed and removed when it is not needed. This is especially useful when personnel must handle a large volume of data and the available display space is limited. Potential applications in NPP HSIs are mimic displays of plant processes and overviews of display networks. De-cluttering capabilities may affect operator awareness of changes in plant status. Because information is removed from immediate view, the operator may not observe important indications for assessing changes in plant status or evaluating possible control actions. A second potential concern is the ability of the operator to recover from the de-cluttered mode. Display windows are de-cluttered through

window-management features. While window-based display systems can provide flexibility for information access and use, window management (e.g., opening, closing, moving, and resizing windows) is a secondary task that can detract from the primary task. Studies suggest that the need to manually adjust display windows can interfere with operator performance in monitoring and decision-making. Automated display management systems, which perform window-management operations automatically based on their interpretations of operator intentions or changes in plant or display system status, may impose new cognitive demands. These may include determining whether a display has been changed, determining why the window-management system operated as it did, anticipating what the system will do next, tracking the system's assessments and actions, and coordinating them with one's goals. If such automated systems are not based on adequate models of operator functions and the task environment, they may increase rather than decrease, the mental workload for operators and detract from overall performance. Guidance is needed on the appropriate use of display de-cluttering features and manual and automated window management systems.

#### **A.7.9.12 Features for Moving between Multiple Display Devices**

In some systems, an operator may use the same input device (e.g., mouse) to interact with different display devices. For example, the operator may switch control of one display device to another via a selection command. Also, two adjacent displays may be coordinated to act as a single display device (e.g., each presenting portions of a larger display). The HSI should provide features that support the operators in maintaining awareness of the currently active display device and preventing input errors (e.g., providing the right input to the wrong display). The consequences of errors may range from accidentally operating the wrong plant component, to selecting the wrong display, to delays in responding to an event. Research is needed to more thoroughly review interface management tasks and develop review guidance on the coordinated use of multiple displays.

#### **A.7.9.13 Input Devices**

Issues associated with providing many different interface management input devices were identified, as were issues associated with having all computer input (interface management and process control inputs) entered through one device. These problems need to be explored further.

#### **A.7.9.14 User Guidance Features**

User guidance features, such as online help, support users in learning and using the interfaces of HSI components. A broad range of systems exists, ranging from manually operated systems with static information, to automatic systems with intelligent guidance generation. Often, the use of these features represents yet another interface management task. Little is understood about how these systems can be systematically designed to support human-computer interaction in complex systems. Some studies showed that online help systems may increase, rather than decrease, the amount of time for users to solve a problem. Some systems do not provide the appropriate type of information to support user tasks. Also, information presented in an inappropriate format can generate additional interface management tasks, such as window management and searches for information. Guidance is needed regarding such topics as

information content, presentation style, interaction methods, and integration into the HSI design process.

#### **A.7.9.15 Global Human-system Interface Considerations**

An NPP HSI will likely contain many display devices, often with multiple methods of interaction. Global HSI considerations encompass the effect that the HSI, as a whole, has on crew performance. There are three major topics. The first topic, layout and distribution of information and controls, addresses the fact that controls and displays can be accessed from multiple locations through multiple paths in the HSI. New opportunities for operator error may be created by HSI features that provide flexibility in presenting controls and displays. For example, they may be shown in ways that violate stimulus-response or population stereotypes. Controls and displays that are functionally unrelated may appear functionally dependent, leading to errors in interpreting the information or in executing control actions. The second topic, interface management consistency and compatibility, covers the variety of presentation and interaction methods that may be obtained from the many components of the HSI. Studies have shown that users can encounter difficulties when switching between different interaction methods (e.g., operators providing inputs in a manner that is consistent with another HSI component but inconsistent with the components being used). Conflicts can arise when similar interaction methods are not compatible. These inconsistencies can arise from upgrades that use different technologies that are not well integrated with the rest of the HSI. Also, features that provide flexibility in the ways that information is given (e.g., operator-configured displays) can result in the use of symbols and coding schemes inconsistent with the rest of the HSI and may lead to operator errors. The third topic, coordinating HSI usage between crew members, refers to the fact that the HSI acts as a communication medium through which members monitor each other's activities and coordinate their actions. HSI features, such as shared display devices, operator-configured displays, and computer-based "soft" controls create new requirements for such coordination. Crew performance can be disrupted when these devices are not used in a coordinated fashion (e.g., operators lose awareness of the state of the HSI or the plant). Guidance is needed to ensure that the individual components of the HSI are properly integrated to support crew performance.

### **A.8 Maintenance**

The issues in this section were identified in Stubler, Higgins, & Kramer (2000).

Two issues were identified in reviewing human performance considerations associated with maintaining digital systems. The first area was policies, procedures, and practices for ensuring maintainability. Industry experience indicated that procedure-related problems were a leading cause of events involving the maintenance of digital systems in NPPs. A systematic approach is needed to ensure that human factors considerations in maintenance are adequately addressed. Such a systematic approach should cover both the process by which maintainability features are designed into digital equipment, and the process by which the equipment is maintained. It should include the development of maintenance interfaces for digital equipment, test equipment and tools, maintenance training, and maintenance procedures.

The second area is emerging digital technologies. Digital technology evolves rapidly and in the

future there are likely to be human factors considerations related to these technologies that are not explicitly addressed by the current knowledge of digital technology.

Two strategies are proposed to address these issues:

- establish process-oriented guidance for reviewing maintenance policies, procedures, and practices, including developing (a) maintainability features during design, and (b) maintenance programs for ensuring that digital systems operate properly after installations
- develop supplemental human factors guidance to address specific design topics in digital technology

These strategies are described below.

### **A.8.1 Process-oriented Guidance**

This strategy would result in the development of guidance for reviewing practices, policies, and procedures related to maintaining digital systems. The guidance would have a format similar to that of NUREG-0711, Human Factors Engineering Program Review Model (O'Hara et al., 2004). Good HFE design principles dictate that maintainability considerations be addressed systematically during design. NUREG-0711 describes a top-down HSI design review process with 10 review elements. Guidance should be established for each of them to specifically address the maintainability of digital systems. Some specific topics are addressed in the following sections.

#### **A.8.1.1 Human Factors Engineering Program Development**

It is difficult to incorporate useful maintainability features at the end of the equipment design process. Careful planning must ensure that maintainability is addressed systematically throughout the design process. This guidance will be directed at the goals and scope of programs that cover HFE and maintainability in the development of digital systems.

#### **A.8.1.2 Human-system Interface Design**

Design requirements for maintainability features and test equipment should be developed from systematic analyses based on the needs of the personnel performing the maintenance. This guidance will address HFE considerations in developing maintainability features and test equipment for digital systems.

#### **A.8.1.3 Training Maintenance Personnel**

While many maintenance skills are transferable to different types of equipment, troubleshooting skills tend to be more specific to particular equipment and, consequently, less transferable. In addition, certain types of traditional training are rather ineffective for acquiring certain maintenance skills. While classroom lectures are an ineffectual way of acquiring troubleshooting skills, training simulators can be productive (Maddox, 1996). However, many dimensions of simulator fidelity influence their efficiency. Guidance is needed for developing

maintenance training programs, including such topics as training methods, simulator fidelity, and assessing the program's effectiveness.

#### **A.8.1.4 Design of Maintenance Procedures and Technical Information for Digital Systems**

Plant events, such as safety system actuations. Many such maintenance errors have caused events stemmed from unanticipated interactions between the state of the plant or plant system, the type of maintenance task performed, and the types of information, aids, and tools used. Maintenance procedures are one means of controlling the combinations of these factors to reduce the likelihood and consequences of errors. In addition, correct, complete technical information is needed to support maintenance. Guidance is needed on establishing maintenance procedures, including the management of technical information, to reduce the likelihood and consequences of mistakes and slips during maintenance work.

#### **A.8.1.5 Automated Test Equipment and Maintenance Aids**

Automated test equipment has become an important tool for testing digital systems. These are usually programmable devices that execute a set of tests in rapid succession, and may have advanced capabilities for diagnosing failures. These capabilities are likely to increase in complexity and sophistication as more digital system upgrades are introduced in NPPs. Computer-based maintenance aids may be used for such functions as tracking adherence to technical specifications when removing equipment from service, tracking regulatory requirements, storing and analyzing system performance and maintenance data, scheduling maintenance, and tracking replacement parts. Errors in using maintenance aids may range from employing incorrect technical data, to scheduling problems, such as failing to carry out a surveillance test. Guidance is needed for reviewing the processes by which automated test equipment and maintenance aids are implemented and maintained in NPPs.

#### **A.8.1.6 Verification and Validation of Maintenance**

Plant safety may be affected by incidents that occur during maintenance, especially when undertaken while the plant is at power. Maintenance practices that pose threats to plant safety should be evaluated through verification and validation tests. This guidance would provide criteria for determining when maintenance activities should be verified and validated, and criteria for assessing the acceptability of these evaluations.

### **A.8.2 Supplemental Guidance for Digital System Features and Capabilities of Digital Systems**

Digital systems have features and capabilities that pose unique challenges for maintenance activities that are likely to grow in importance as the nuclear industry replaces existing equipment with digital technologies to upgrade plant performance. Specific issues are identified in the following sections.

### **A.8.2.1 On-line Maintenance Features**

Considerations include the design of HSI features that affect personnel's awareness of the status of equipment, or reduce the likelihood of input errors. Alarms and displays may include features showing the availability and operating modes (e.g., test, manual control, automatic control) of plant systems. Controls may include features that reduce the likelihood of incorrect control actions, such as entering the wrong value, operating the wrong control, or causing a bump when switching control between processors.

### **A.8.2.2 Advanced Features of Test and Diagnosis Equipment**

This includes features for reducing sources of detection and interpretation errors, such as long, unreadable failure codes and look-up tables that can be misread.

### **A.8.2.3 Circuit Cards**

Industry experience indicates that because digital equipment, especially printed circuit cards, often contains similar looking components in close proximity, the likelihood of maintenance errors involving the wrong component may be increased. These errors probably will rise as NPPs install more digital systems. As maintenance personnel are required to service more digital components, more opportunities may be created for servicing the wrong component. In addition, the complexity of digital systems may make the detection of errors more difficult. Before more definitive review guidance is established, a better understanding is needed of the types of errors that occur when the wrong component on a circuit card is serviced, and the factors contributing to these errors. Further review and research is required.

### **A.8.2.4 Data-bus Technologies**

Within digital systems, there is a trend toward transmitting signals via communication buses, rather than individual wires; where connections are made via computer addresses, rather than physical wire connections. This may introduce new opportunity for personnel error. For example, by inadvertently assigning the wrong addresses, signals may be sent to the wrong processors. Accordingly, higher cognitive burdens may be imposed on maintenance personnel to understand which signals are being transmitted and the failures that may result from improper connections. Guidance is needed to review features intended to reduce these types of errors.

## **A.8.3 Software Configuration Management**

Configuration control of digital systems was among the issues identified in the hybrid project report that were not specifically addressed in subsequent guidance development.

For many digital control systems, software maintenance, upgrades, and logic configuration is performed via an engineering workstation. The introduction of workstations for the configuration of the control system poses many questions regarding the types of safeguards needed to maintain the integrity of the control system. Computer-based aids for modifying control logic allows changes to be made rapidly. Errors are possible due to a lack of mode awareness of the configuration workstation (e.g., configure versus test), and can lead to undesirable changes that

may be made without personnel realization. Also, safeguards to control access to the configuration workstation need to be considered.

Another related issue is that changes may be made by different elements of the organization, e.g., I&C, IT, and operations. Provisions need to be designed to allow access to various user groups, and to ensure administrative control over changes and modifications.

## A.9 References

- Baker, S., Gertman, D., Hollnagel, E., Holmstrom, C., Marshall, E., & Owre, F. (1985). *An Experimental Comparison of Three Computer-based Alarm Systems: Results and Conclusions* (HWR-142). Halden, Norway: Halden Reactor Project.
- Blackman, H. & Nelson, W. (1988). Unexpected Effects of Computer Presented Procedures. In *1988 Fourth Conference on Human Factors and Power Plants*. New York: Institute of Electrical and Electronics Engineers.
- Brown, W.S., O'Hara, J.M., & Higgins, J.C. (2000). *Advanced Alarm Systems: Revision of Guidance and its Technical Basis* (NUREG/CR-6684). Washington, DC: U.S. Nuclear Regulatory Commission.
- Chignell, M. & Zuberec, S. (1993). *Computerization of Operating Procedures*. Toronto: University of Toronto.
- Christoffersen, K., Hunter, C., & Vicente, K. (1995). Ecological Interface Design and Fault Management Performance: Long-term Effects. In *Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.
- DoD (1996). *Department of Defense Technical Architecture Framework for Information Management, Volume 8: DoD Human-computer Interface Style Guide* (Version 3.0). Washington, D.C.: Defense Information Systems Agency.
- Hansen, J. (1995). An Experimental Investigation of Configural, Digital, and Temporal Information on Process Display. *Human Factors*, 37, 539-552.
- Heslinga, G. & Herbert, M. (1995). Experiences with Advanced Systems for Human-machine Interaction. In *Proceedings of the 6th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design and Evaluation of Man-Machine Systems*. Cambridge, MA: Massachusetts Institute of Technology.
- Hoecker, D., Corker, K., Roth, E., Lipner, M., & Bunzo, M. (1994). Man-machine Design and Analysis System (MIDAS) Applied to a Computer-based Procedure-aiding System. In *Proceedings of the Human Factors and Ergonomics Society 38th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.
- Hoecker, D. & Roth, E. (1996). Using Models of Operator Performance to Support MMIS Design: An Example in the Use of Procedural Aids. In *Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*. La Grange Park, IL: American

Nuclear Society.

- Hutchins, E. (1990). The Technology of Team Navigation. In J. Galegher, R. Kraut, and C. Egido (Eds.), *Intellectual Teamwork: Social and Technological Foundations of Cooperative Work*. Hillsdale, NJ: Erlbaum.
- IAEA (1994). *Development and Implementation of Computerized Operator Support Systems in Nuclear Installations* (Technical Reports Series No. 372). Vienna: International Atomic Energy Agency.
- Jeffroy, F. & Charron, S. (1997). Safety Assessment to Research in the Domain of Human Factors: The Case of Operation with Computerized Procedures. In *Proceedings of the 1997 IEEE Sixth Conference on Human Factors and Power Plants*. Washington DC: IEEE.
- Maddox, M. (1996). Critique of "A Longitudinal Study of the Effects of Ecological Interface Design on Skill Acquisition." *Human Factors*, 38, 542-545.
- Mitchell, C. & Miller, R. (1983). Design Strategies for Computer-based Information Displays in Real Time Control Systems. *Human Factors*, 25, 353-369.
- Norman, D. (1988). *The Psychology of Everyday Things*. New York, NY: Basic Books.
- Norman, D. & Bobrow, D. (1975). On Data-limited and Resource-limited Processes. *Cognitive Psychology*, 7, 44-64.
- 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., Hallbert, B., Skråning, G., Wachtel, J., & Persensky, J. (2000). *The Effects of Alarm Display, Processing, and Availability on Crew Performance* (NUREG/CR-6691). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- O'Hara, J., Brown, W., Higgins, J., & Stubler, W. (1994). *Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems* (NUREG/CR-6105). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- O'Hara, J., Brown, W., Lewis, P. & Persensky, J. (2002). *Human-System Interface Design Review Guideline* (NUREG-0700, Rev 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- 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., Higgins, J., Stubler, W., & Kramer, J. (2000). *Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6634). 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. (Chapter 7, pp 139-159).
- O'Hara, J., Stubler, W., & Higgins, J. (1996). *Hybrid Human-system Interfaces: Human Factors Considerations* (BNL Technical Report J6012-T1-4/96). Upton, New York: Brookhaven National Laboratory.
- Oser, R., McCallum, G., Salas, E., & Morgan, A. (1989). *Toward a Definition of Team Work: An Analysis of Critical Team Behaviors* (Tech. Report 89-004). Orlando, FL: Naval Training Systems Center, Human Factors Division.
- Reason, J. (1987). The Psychology of Mistakes: A Brief View of Planning Failures. In J. Rasmussen, K. Duncan, & J. Leplat, eds, *New Technology and Human Error*. John Wiley: New York, N.Y. Pgs 45-52.
- Reason, J. (1988). Modeling the Basic Error Tendencies of Human Operators. *Reliability Engineering and System Safety*, 22, 137-153.
- Reason, J. (1990). *Human Error*. New York, NY: Cambridge University Press.
- 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.
- Salas, E., Dickinson, T., Converse, S., & Tannenbaum, S. (1992). Toward an Understanding of Team Performance and Training. In R.W. Swezey and E. Salas (Eds.), *Teams: Their Training and Performance*. Norwood, NJ: Ablex.
- Segal, L. & Wickens, C. (1990). TASKILLAN II: Pilot Strategies for Workload Management. In *Proceedings of the Human Factors and Ergonomics Society - 34th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.
- Sheridan, T. (1997). Supervisory Control. In G. Salvendy (ed.), *Handbook of Human Factors*. New York: John Wiley.
- Sperandio, J. (1978). The Regulation of Working Methods as a Function of Work-load among Air Traffic Controllers. *Ergonomics*, 21, 195-202.
- Spurgin, A., Orvis, D., Spurgin, J. & Luna, C. (1990). *The BWR Emergency Operating Procedures Tracking System (EOPTS): Evaluation by Control-room Operating Crews* (EPRI NP-6846). Palo Alto, CA: Electric Power Research Institute.

- Stubler, W., Higgins, J., & Kramer, J. (2000). *Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6636). Washington, D.C: U.S. Nuclear Regulatory Commission.
- Stubler, W., Higgins, J., & O'Hara, J. (1996). *Evaluation of the Potential Safety Significance of Hybrid Human-system Interface Topics* (BNL Report J6012-T2-6/96). Upton, New York: Brookhaven National Laboratory.
- Stubler, W. & O'Hara, J., (1996). *Human-System Interface Design Process and Review Criteria* (BNL TR E2090-T4-1-9/96). Upton, New York: Brookhaven National Laboratory.
- Watts, J. (1994). Navigation in the Computer Medium: A Cognitive Analysis. In *Proceedings of the Human Factors and Ergonomics Society - 38th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.
- Wickens, C. (1992). *Computational Models of Human Performance* (Report ARL 92-4). Champaign, IL: University of Illinois.
- Wickens, C. & Carswell C. (1995). The Proximity Compatibility Principle: Its Psychological Foundation and its Relevance to Display Design. *Human Factors*, 37, 473-494.
- Wickens, C. & Carswell, C. (1997). Information Processing. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (Second Edition). New York, NY: Wiley-Interscience.
- Woods, D. (1993). The Price of Flexibility. In *Proceedings of the 1993 International Workshop on Intelligent User Interfaces*. New York, NY: Association for Computing Machinery.
- Woods, D., Roth, E., Stubler, W., & Mumaw, R. (1990). Navigating through Large Display Networks in Dynamic Control Applications. In *Proceedings of the Human Factors Society - 34th Annual Meeting*. Santa Monica, CA: Human Factors and Ergonomics Society.