



**BNL-91087-2010**

***Review of the IEEE Standard for Computerized  
Operating Procedure Systems***

**John O'Hara and James Higgins**

February 2010

**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..



# **Review of the IEEE Standard for Computerized Operating Procedure Systems**

*Prepared for*

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

*Prepared by*

John O'Hara and James Higgins  
Brookhaven National Laboratory  
Energy Sciences and Technology Department  
Upton, NY 11973-5000

February 26, 2010

## **ABSTRACT**

Increasingly nuclear power plant procedures, such as emergency operating procedures, are being presented in computer form with functionality to support operator use and management of the procedures. The U.S. Nuclear Regulatory Commission (NRC) currently has guidance for the review of computer-based procedures (CBPs); however, there remain CBP functions and human performance issues for which up-to-date guidance is lacking. The Institute of Electrical and Electronics Engineers (IEEE) has initiated a standard development effort to address the human factors engineering (HFE) aspects of CBP systems. When completed, it may provide guidance to supplement the NRC staff's review criteria. The purpose of our study was to evaluate the suitability of the IEEE Standard for use in the NRC's HFE safety reviews of CBP systems and to ensure that the guidance meets the NRC's standard for scientific and engineering rigor used in its own guidance development efforts. We established the following criteria with which to evaluate the Standard: (1) it should meet an existing need of NRC reviewers, (2) it should be based in sound HFE principles, (3) it should be thoroughly peer-reviewed, and (4) it should address CBP-related human performance issues identified in the literature. This report describes the methodology we used to evaluate each criterion. Our evaluation concluded that the Standard generally does meet these criteria, however several areas were identified for which additional clarifications are needed. Thus consideration of the Standard's use by the NRC is supported. The standard evaluation methodology developed in this study can be generally applied to the review of other HFE standards being considered for possible use or endorsement by the NRC.

# Contents

<b>ABSTRACT .....</b>	<b>ii</b>
<b>ABBREVIATIONS .....</b>	<b>v</b>
<b>1 Introduction .....</b>	<b>1</b>
1.1 Background .....	1
1.2 Summary of the NRC HFE Guidance Development Process .....	2
1.3 Purpose of this Review.....	2
<b>2 Existing Need Evaluation .....</b>	<b>4</b>
2.1 Objective .....	4
2.2 Methodology.....	4
2.3 Results .....	4
2.4 Conclusion.....	5
<b>3 IEEE Guidance Evaluation .....</b>	<b>6</b>
3.1 Objective .....	6
3.2 Methodology.....	6
3.3 Results .....	7
3.3.1 General Comments .....	7
3.3.2 General Principles .....	10
3.3.3 Design Guidelines .....	12
3.3.3.1 Guidelines Applicable to Type 1, 2 & 3 Systems .....	12
3.3.3.2 Guidelines Applicable to Type 2 and Type 3 Systems .....	14
3.3.3.3 Guidelines Unique to Type 3 Systems .....	16
3.3.3.4 COPS Backup .....	22
3.3.3.5 Quality Assurance .....	23
3.3.3.6 Maintenance and Configuration Management .....	25
3.4 Conclusion.....	27
<b>4 Guidance Peer Review Evaluation .....</b>	<b>29</b>
4.1 Objective .....	29
4.2 Methodology.....	29
4.3 Results .....	29
4.3.1 Peer-Review Process.....	29
4.3.2 Subject Matter Participants .....	30
4.3.3 Treatment of SME Comments.....	31
4.4 Conclusion.....	31
<b>5 Human Performance Issue Evaluation .....</b>	<b>32</b>
5.1 Objective .....	32
5.2 Methodology.....	32
5.3 Results .....	32
5.4 Conclusion.....	33
<b>6 Recommendations.....</b>	<b>34</b>
6.1 Overall Summary.....	34
6.2 Recommended Follow-up to This Evaluation.....	35
6.3 Recommendation for Standard Endorsement.....	35

<b>7</b>	<b>References .....</b>	<b>36</b>
----------	-------------------------	-----------

<b>Appendix - HFE Research Issues Pertaining to Computer-based Procedure Systems .....</b>		<b>38</b>
A.1	Lack of Data on the Effects of CBPs on Crew Performance .....	38
A.2	Acceptance Criteria for CBP Performance Effects .....	39
A.3	Role of Plant Personnel in Procedure Management: Trust and Appropriate Use .....	39
A.4	Level of Automation of Procedure Functions .....	39
A.5	Teamwork and Team Performance .....	40
A.6	Situation Awareness, Response Planning, and Operator Error .....	40
A.7	Keyhole Effects and Use of Multiple Computer-based Procedures .....	41
A.8	CBP Complexity and Opacity .....	41
A.9	Specific Computer-Based Procedure Design Features .....	42
A.10	Hybrid Procedure Systems .....	42
A.11	CBP Degradation, Failure Modes, and Backup Systems .....	42
A.12	Transitioning to CBP Systems from a PBP Operational Environment .....	43
A.13	Training in CBP Usage .....	43

## Tables

Table 2-1	Contents of the IEEE CBP Standard .....	5
Table 3-1	Summary of IEEE Guideline Evaluations .....	28
Table 5-1	CBP HFE Research Issues Addressed by the IEEE Standard .....	33

## ABBREVIATIONS

AI	additional information
AOP	abnormal operating procedure
ARP	alarm response procedure
CBP	computer-based procedure
COPS	computerized operating procedure system
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
HFE	human factors engineering
HPR	Halden Project report
HSI	human-system interface
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
ISG	interim staff guidance
NA	not applicable
NOP	normal operating procedure
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
PBP	paper-based procedure
QA	quality assurance
SC	subcommittee
SME	subject matter expert
SP	surveillance procedure
VDU	video display unit
V&V	verification and validation

# 1 Introduction

## 1.1 Background

Increasingly in new and modernized plants, procedures such as emergency operating procedures are being presented in computer form with functionality to support operator use and management of the procedures. Computer-based procedure (CBP) systems typically reside in plant computer systems and obtain data and execute controls through the instrumentation and control (I&C) subsystems. The NRC's HFE review guidance for CBPs currently exists in the *Human-System Interface Design Review Guidelines* (NUREG-0700) (O'Hara et al., 2002) and the Interim Staff Guidance (ISG) for *Highly-Integrated Control Rooms - Human Factors Issues* (NRC, 2008). NUREG-0700, Rev. 2, contains the guidance for the review of CBP systems in Section 8, CBP Systems, and Appendix B.3, Review Guidelines for the CBP System Design Process. NUREG-0700's CBP guidance was developed as part of a research project that was conducted a decade ago (O'Hara et al., 2000). At the time, CBPs were a new technology with limited functionality. CBP systems were implemented in very few plants, thus little operational experience was available. More recently, the NRC has developed additional review guidance for CBP systems. The guidance updates some of the guidance in NUREG-0700 and addresses some aspects of CBP systems not included in NUREG-0700, such as procedure automation and the use of soft controls. This new guidance is contained in the ISG, Section 1, CBPs. Together NUREG-0700 and the ISG provide comprehensive guidance for the review of CBP systems.

The Institute of Electrical and Electronics Engineers (IEEE) has initiated a standard development activity, entitled *Human Factors Guide for Applications of Computerized Operating Procedure Systems (COPS)*<sup>1</sup> at Nuclear Power Generating Stations and other Nuclear Facilities, IEEE Std 1786, (IEEE, 2009a) is to:

... provide application guidance, based on current industry experience, for the design and use of COPS at nuclear power generating stations and other nuclear facilities. The Guide will identify acceptable practices and important considerations for applying COPS to facility operations. The guide is intended to support developers, users, and reviewers of COPS.

IEEE Std 1786, hereafter referred to as the "Standard," is in the draft stage. When completed, it may provide guidance to supplement the NRC staff's review criteria for CBP systems by addressing functionality that was not addressed when the NRC's guidance was being developed. Additionally the Standard may provide updated guidance for those aspects of CBP systems that are addressed in the staff's design review guidance.

Thus the NRC will review the Standard to evaluate its suitability, in whole or in part, for use in the staff's review of CBP systems and to ensure that the guidance meets the NRC's standard for scientific and engineering rigor used for its own HFE guidance development efforts. The NRC's HFE design review guidance development process is briefly summarized below.

---

<sup>1</sup> For the purposes of this report, CBP and COPS are used synonymously.



## 1.2 Summary of the NRC HFE Guidance Development Process

NRC human factors engineering (HFE) design reviewers evaluate systems proposed for use in existing and new plants. Any system, such as a CBP system, has characteristics and functions that plant operators interact with in order to accomplish their tasks. NRC reviewers evaluate these characteristics and functions to ensure that they are designed in accordance with HFE principles and that crew performance is appropriately supported. The NRC's Office of Nuclear Regulatory Research develops the criteria used by NRC reviewers to conduct the HFE evaluations. The methodology used to develop HFE review guidance is shown in Figure 1. Aspects of the methodology are briefly summarized here. A more complete description is contained in Appendix B of NUREG- (O'Hara et al., 2008a).

Following the analysis of user needs and lessons learned, a technical basis upon which to develop review guidance is developed. The first step in the technical basis development for any aspect of the human-system interface (HSI) is to develop a characterization. In this case, the characterization describes the characteristics and functions of current and near-term CBP systems. The characterizations have to be sufficiently robust to accommodate the review of a diversity of CBP systems that applicants may propose. The characterizations are explicitly described in NUREG-0700. Once the characterization is completed, research and operating experience is analyzed to identify human performance issues associated with CBPs and best practices for minimizing issues and supporting performance. This technical basis of information is then used to develop draft design review guidance. The draft guidelines are submitted for peer review and the guidance is modified accordingly. The resulting guidance is typically integrated into NUREG-0711 (O'Hara et al., 2004) and NUREG-0700.

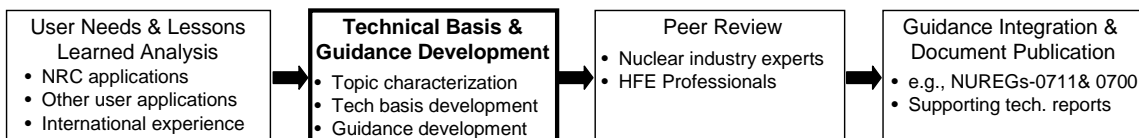


Figure 1 Major steps in NRC HFE guidance development

The NRC's HFE guidance development methodology places a high priority on establishing the validity of the guidelines. Validity is defined along two dimensions: internal and external validity. *Internal validity* is the degree to which the individual guidelines are linked to a clear, well founded, and traceable technical basis. *External validity* is the degree to which the guidelines are supported by independent peer review. Peer review is a good method of screening guidelines for conformance to generally accepted HFE practices and to industry-specific considerations, i.e., for ensuring that the guidelines are appropriate based on practical operational experience in actual systems.

## 1.3 Purpose of this Review

The purpose of this review is to evaluate the IEEE Standard on Computerized Procedures for its suitability for use in the staff's HFE safety reviews of CBP systems and to ensure that the guidance meets the NRC's standard for scientific and engineering rigor used for its own guidance development efforts. To be used in the staff's safety review of applicants' CBP systems, the Standard should meet the following criteria.

1. The Standard meets an existing need of NRC reviewers, i.e., the Standard should provide guidance that addresses characteristics of CBP systems not currently addressed in existing NRC guidance.
2. The Standard is based in sound human factors engineering principles. (This is referred to as “internal validity” in the NRC HFE guidance development process.)
3. The Standard is a thorough peer-reviewed. (This is referred to as “external validity” in the NRC HFE guidance development process.)
4. An additional consideration is whether the Standard addresses CBP-related human performance issues. While it is not necessary for the Standard to address specific human performance issues identified by the NRC and industry, it is a significant benefit if it does.

If the Standard meets some but not all of these criteria, it may still be useful for the NRC in a more limited fashion depending on the specifics identified during the review.

## 2 Existing Need Evaluation

### 2.1 Objective

With respect to Section 1.3, Criterion 1, our first evaluation was performed to determine whether the Standard provides guidance that addresses an existing need, i.e., it addresses characteristics of CBP systems not currently addressed in existing NRC guidance.

### 2.2 Methodology

We reviewed recent literature and system descriptions to update the characterization of CBP systems in NUREG-0700; e.g., to update the NRC characterization for CBP features and functions that were not available in systems in use when the characterization was developed. We also conducted observations of CBP systems, such as the Westinghouse's CBP for the AP1000. The updated characterization will point out aspects of CBP characteristics and functions that are not addressed in the NRC's existing review guidance. These constitute gaps in our guidance.

We compared the updated CBP characterization to the scope of the IEEE guidance to assess whether it (1) addressed aspects of CBP systems not addressed in NRC guidance or (2) provided an update or expansion to the NRC's guidance.

### 2.3 Results

The high-level contents of the Standard are shown in Table 2-1. The Standard addresses several CBP topics that are not currently addressed by NRC guidance. In addition, the Standard provides expanded guidance for several topics that are addressed in the NRC's guidance. Some examples are identified below.

*Procedure automation of plant control functions* - Type 3 procedures provide the capability to automate controls. NUREG-0700 does not address plant control. The ISG addresses procedure control, but it is only performed upon operator command (ISG Guideline 11).<sup>2</sup>

*Multiple users of CBPs* – Standard Guideline 5.2-5 states "the capability should be provided for a read-only view of the ongoing procedure activities within the main control room." CBP use by multiple users is an important topic that is not addressed in the current NRC guidance.<sup>3</sup>

*Quality assurance* – The NRC CBP guidance provides very limited treatment of quality assurance (QA). The Standard provides an expanded treatment of QA as applied specifically to CBPs.

---

<sup>2</sup> Note that in addressing the topic of automation, the Standard has also raised an issue pertaining to the automation of EOPs (see evaluation of Guideline 5.3-3).

<sup>3</sup> The guidance provided for use of procedures by multiple operators was being formulated at the time this review was performed; thus it likely will change in future revisions.

*Configuration management* – The NRC CBP guidance provides very limited treatment of configuration management. The Standard provides an expanded treatment of this topic as applied specifically to CBPs.

Table 2-1 Contents of the IEEE CBP Standard

1 Overview
1.1 Scope
1.2 Purpose
2 Normative References
3 Definitions
4 Conceptual Framework
4.1 General Principles
4.2 Types of COPS
4.3 Types of Operating Procedures
5 Design Guidelines
5.1 Guidelines Applicable to All Types of COPS
5.2 Additional Guidelines Applicable to Type 2 & Type 3 Systems
5.3 Guidelines Unique to Type 3 Systems
5.4 COPS Backup
5.5 Quality Assurance and Operator Real-Time Verifications
5.6 Maintenance and Configuration Management
Annex A Bibliography
Annex B (informative) COPS Functionality and Concept of Operations
Annex C (informative) Additional Design Guidance

Note: Based on the September 30, 2009 version of the Standard.

## 2.4 Conclusion

The conclusion of our evaluation is that the Standard does address aspects of CBPs that are not addressed in existing NRC guidance. It also provides additional guidance for some topics that are addressed.

## **3 IEEE Guidance Evaluation**

### **3.1 Objective**

With respect to Section 1.3, Criterion 2, we evaluated whether the guidance in the Standard is based in sound HFE principles.

### **3.2 Methodology**

The NRC uses its own design review guidelines to determine whether a design document (such as a specification or style guide) and actual HSI design implementations are based on sound HFE principles. The same approach was used to evaluate each individual guideline in the Standard. We considered the following factors when performing this review:

- In areas where there is technical overlap in the guidance, we evaluated the Standard using the NRC review guidance.
- Where we identified a discrepancy between the Standard and the NRC guidance, we evaluated the discrepancy to determine if it can be justified in terms of recent research and/or knowledge gained through operating experience.
- For aspects of the Standard that are beyond the scope of existing NRC guidance, we evaluated the Standard to determine if the guidance is a reasonable extrapolation of current research and operating experience, i.e., does the Standard have sound internal validity. Standards do not typically document the technical basis upon which their guidance is based. We identified the individual guidelines for which validity could not be established. We can ask the Standard's development group to identify the basis of those individual guidelines.

We considered a guideline sound when it was found to be

- consistent with an existing HFE guideline on the same aspect of CBPs
- a CBP application of an existing higher-level HFE guideline
- a reasonable extrapolation of sound HFE principles and practices

The following documents were used to evaluate the Standard's technical basis:

- Highly-Integrated Control Rooms - Human Factors Issues: Interim Staff Guidance (NRC, 2008), hereafter referred to as the "ISG"
  - Section 1 – Computer-based Procedures
- Human-system Interface Design Review Guidelines (NUREG-0700, Rev 2) (O'Hara et al., 2002), hereafter referred to as the "NUREG-0700"
  - Section 1 – Information Display
  - Section 7 – Soft Control System
  - Section 8 – Computer-Based Procedure System

- Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis (BNL Technical Report 91017-2010) (O'Hara & Higgins, 2010), hereafter referred to as the "Automation Report"
- The Effects of Degraded Digital Instrumentation and Control Systems on Human-system Interfaces and Operator Performance: HFE Review Guidance and Technical Basis (O'Hara, Gunther, & Martinez-Guridi, 2010), hereafter referred to as the "Degraded Conditions Report"

### **3.3 Results**

Following the presentation of general comments, the remainder of this section is organized according to the Standard's structure. Each guideline is presented first, followed by its evaluation.

#### **3.3.1 General Comments**

In reviewing the guidance provided in the Standard, we identified a number of recommendations for the Standard's developers for consideration in future revisions. The topics included are

- Supporting utility decisions about types of COPS to select
- Types and classes of procedures
- Type 2 procedure guidance
- Procedure-based automation
- Soft control vs. automatic control
- Embedded soft controls
- Multiple controls
- Guidance on configuration management, quality control, and procedure maintenance

#### Supporting Utility Decisions about Types of COPS to Select

The Standard distinguishes between three types of COPS distinguished by functional capabilities. As COPS are a relatively new technology for most utilities, especially in the U.S., one might expect to find some guidance (or Annex-type material) that would guide a utility in making the decision as to what level of CBP functionality is appropriate for their application. No such guidance is presented. At the very least, providing the trade-offs between them might be helpful.

#### Types and Classes of Procedures

The Standard's guidance is organized by procedure types which are distinguished by increasing levels of capability:

- A Type 1 COPS represents procedure text documents for operational use in electronic form.
- A Type 2 COPS may utilize dynamic process data for embedded display, to evaluate conditions or procedure logic, or to monitor plant conditions during

procedure-defined intervals of applicability. A Type 2 COPS cannot issue control commands, but it may provide access to soft control capabilities that exist outside of the COPS.

- A Type 3 COPS may issue control commands to plant equipment. The capability to issue a control command from a COPS application, either individually or sequentially, is referred to as embedded soft control.

However, the Standard's guidance is applicable to a range of classes of procedures, include: Normal Operating Procedures (NOPs), Surveillance Procedures (SPs), Alarm Response Procedures (ARPs), Abnormal Operating Procedures (AOPs), and Emergency Operating Procedures (EOPs).

It is not clear that all of the guidance presented can be applied without regard to the class of procedures. Thus, the COPS capabilities of embedded soft controls may be applied differently depending on whether it is an ARP, NOP, or EOP.

### Type 2 Procedure Guidance

In Table 4-1, Type 2 procedures are distinguished from Type 1 by the following capabilities:

- Display process data in the body of procedure steps
- Evaluate procedure step logic and display results
- Provide access links to process displays and soft controls that reside on a separate system

However, almost no guidance is provided in Section 5.2, Guidelines Applicable to Type 2 and 3 Systems, for these capabilities. We think guidance is warranted and can be developed to address these features. The only guidance is related to step-logic analysis and Guideline 5.2-3 simply states that "Data evaluated by COPS to reach a result should be available to the operator." This is probably inadequate if the step logic is not also available.

Another example is the use of soft controls related to the third bullet. Guidance is needed as to how these controls are accessed and how they should be used in the context of the procedure. For example, outside the COPS, soft controls may be used in the context of mimic-type process display and appear as pop-up windows. Their design may assume the mimic display provides related information that helps assure proper use by operators. If the soft control is accessed through the COPS, what specifically is accessed – the control pop-up window, the entire mimic display, or some hybrid display? This topic is addressed in Annex C, but something should be stated in the guidance, as the Annex is informative only.

### Procedure-based Automation

The Standard defines *procedure-based automation* as "The evaluation and execution of a predefined sequence of procedure steps by a computerized operating procedure system." This seems to limit the consideration of automation to evaluation of step logic (such as

determining that a valve is closed) and performance of step defined actions (such as proceeding to the next step if the valve is closed or closing the valve if open). Yet, CPBs can provide other automated functions, such as monitoring of continuously applicable steps, procedure entry conditions, cautions, and critical safety functions. Some of these are addressed and others are not.

An example of where this comes into play is the distinction between Type 2 and Type 3 procedures. Type 3 procedures are the same as Type 2, except they also have the following unique capabilities:

- Issue control commands to equipment from embedded soft controls
- On operator command, evaluate a sequence of steps that is predefined by the procedure

These two capabilities represent different functionality and it is conceivable that a licensee might want to implement one and not the other. For example, a utility might want to enable the COPS to “on operator command, evaluate a sequence of steps that is predefined by the procedure,” but not want the procedure to execute plant control actions as is provided by the first bullet. In such a COPS, the procedure might run through a series of steps that check conditions at each one, but it stops when an action has to be taken. It may make more sense to consider each procedure function and how increasing levels of automation can be applied, rather than forming two general “types” of procedures that package automation capabilities.

#### Soft Control vs. Automatic Control

The Standard defines a *soft control* as “A computer-generated device that is operationally equivalent to a physical device (e.g., a pushbutton, selector switch, potentiometer, component controller, etc.) that is used to operate plant equipment.” This definition does not distinguish who the controller is – personnel or an automatic system. In NUREG-0700, the ISG, Electric Power Research Institute (EPRI) guidance documents, the term soft control is used for controls initiated by operators. Guidance for controls may be different when one is addressing a control presented to operators for their use vs. automatic control functions. The Standard refers to the latter as an “embedded soft control,” but that term is not in the definitions section (Section 3) of the Standard. The first time this term appears is in the definition of a Type 3 COPS which states that “A Type 3 COPS may issue control commands to plant equipment. The capability to issue a control command from a COPS application, either individually or sequentially, is referred to as embedded soft control.” We recommend using a different term to clearly distinguish who the controller is, e.g., use soft control for operator initiated controls and automatic control to indicate that the procedure is automatically taking action. There is guidance for embedded soft controls, but not for soft controls provided to operators.

#### Embedded Soft Controls

Type 3 COPS provide the capability for control to be automatically taken by the procedure. This appears to be in conflict with ISG Guideline 11 which states that “The computer-based procedure system should not automatically initiate control actions without first receiving a command from the operator to do so.”



This may be an issue where the class of procedures may come into play. While embedded soft controls are probably acceptable for NOPs they may not be for EOPs.

### Multiple Controls

Whether control from the COPS is in the form of an operator initiated soft control (Type 2) or an embedded soft control (Type 3), plant control can take place at multiple locations such as at the COPS workstation and another non-COPS workstation. The guidance should address lockout of controls so simultaneous efforts to control the same systems do not occur.

### Guidance on Configuration Management, Quality Control, and Procedure Maintenance

Guidance is presented in two section of the Standard to address the topics of configuration management, quality control, and procedure maintenance. It is a good idea to address these topics in the context of COPS. The guidance does seem to address aspects of produces that go beyond COPS, for example, ensuring the technical content of the procedures. Rigorous standards already exist for procedure modification, QA, and configuration management that do not have to be addressed here or perhaps can simply be referenced. There are unique aspects, such as updating the technical procedure content of COPS without requiring COPS software changes that are appropriately addressed.

There also seems to be quite a bit of internal redundancy in these two sections that can probably be eliminated.

### **3.3.2 General Principles**

Section 4.1 of the Standard provides four general principles.

- 4.1.1 Human operators are responsible for the proper application of operating procedures. Thus, COPS should be designed and implemented such that human operators remain in command of the processes being operated.

### Evaluation

This guideline is consistent with ISG Guideline 11 which states that “The computer-based procedure system should not automatically initiate control actions without first receiving a command from the operator to do so.” That operators should be in control of plant processes is also consistent with NRC guidance in the Automation Report.

It is also consistent with Automation Guideline 8.2-1, Locus of Authority, which states that “Except in cases where automation is mandatory based on performance requirements, operators should be in charge of the automation, be able to redirect it, stop it, and assume control if necessary.”

We conclude that this guideline is based on sound HFE principles.

- 4.1.2 COPS with sufficient capability may *evaluate* one or more procedure steps, if the results in each case are fully determined by the step logic and the available process

data. Steps with undetermined elements will require a *decision* to be made by the operator. COPS shall not make such decisions.

#### Evaluation

This guideline is consistent with NRC NUREG-0700, Section 8.2.2, Procedure Monitoring and Assessment, particularly Guideline 8.2.2-5.

Note the meaning of “undetermined elements” should be defined. If it pertains to information needed from operators to resolve step logic, then it is consistent, in part, with NUREG-0700 Guideline 8.2.2-11:

##### 8.2.2-11 Identification of User Input Requirements

The CBP should provide users with clear, timely indications when they need to input any information not available to it.

*Additional Information:* CBPs may rely on users to process parameter values, equipment status (such as whether a valve is open or closed), analyses of logic steps where users' judgment is involved, or to assess any conditions not within the capability of the CBP.

We conclude that this guideline is based on sound HFE principles.

- 4.1.3 Results evaluated by COPS shall be the same as those expected from operator evaluations of the same steps.

#### Evaluation

Does this guideline mean that the “Results obtained from the COPS should be ...”?

Is the evaluation of step logic by operators the appropriate criterion for acceptability? One might expect the use of the COPS to improve human performance by helping to minimize error in procedure use, such as those associated with difficult logic steps. Where possible, the step logic results should be independently verified for correctness by analysis.

How would a designer show compliance to this guideline as stated?

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 4.1.4 Loss of the COPS should not affect the operator's ability to safely operate the plant.

#### Evaluation

In general, this guideline is consistent with the need for a backup system upon COPS failure and the need to support a smooth transfer to the backup system as identified in the ISG and NUREG-0700.

We conclude that this guideline is based on sound HFE principles.

### 3.3.3 Design Guidelines

IEEE Standard Section 5 provides guidance for COPS design. Additional explanation for the guidelines is contained in Annex C of the Standard.

#### 3.3.3.1 Guidelines Applicable to Type 1, 2 & 3 Systems

- 5.1-1 Presentation of information by COPS should meet accepted human factors engineering (HFE) principles and practices.

##### Evaluation

As stated, the guideline does not provide sufficient information, e.g., how does the designer show compliance with this guideline? The guideline should identify what constitutes "Accepted HFE principles and practices." Annex C contains a general discussion as to additional considerations that might be made. But it references NRC and EPRI documents that contain more detailed guidelines for COPS. The Annex does not mention following practices and principles in IEEE Standards 1023 (IEEE, 2004) or 1289 (IEEE, 1998). However, in the introduction to these guidelines, the Standard states that "COPS are assumed to be a significant human interface as defined in IEEE Std 1023. As such, HFE principles and methods should be considered as applicable to COPS designs. See IEEE Stds 1023 and 1289 for additional information on the basic considerations of HFE and their systematic application in design."

This guideline might be better placed in the general principles and its scope extended to the entire COPS HSI and not just information presentation.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.1-2 The currently active procedure(s) should display a unique identification.

##### Evaluation

This is a high-level version of NUREG-0700, Guideline 8.1.1-1, Procedure Title and Identification Information. The NRC guideline identifies title, procedure number, revision number, date, and organizational approval as well. Annex C identifies this information as well.

We conclude that this guideline is based on sound HFE principles.

- 5.1-3 COPS should not determine what procedure will be used by the operating crew. The crew should decide what procedure would be used in any given situation.

##### Evaluation

This guideline is consistent with ISG Guideline 2 indicating the CBP user should always remain in control of the procedure system and NUREG-0700 Guideline 8.2.1-1 that users are in control the procedure path.

We conclude that this guideline is based on sound HFE principles.

- 5.1-3.1 COPS may recommend or prompt the operator to use a particular procedure, but the operator should be able to override this.

#### Evaluation

This guideline is consistent with the NUREG-0700 Guideline 8.2.2-1 indicating CBPs should only alert users when procedure entry conditions are satisfied.

We conclude that this guideline is based on sound HFE principles.

- 5.1-4 Backup procedures (PBPs <paper-based procedures> or alternate COPS) should be provided in case of COPS failure.

#### Evaluation

This guideline is consistent with ISG Guidelines 25 and NUREG-0700 Guideline 8.5.-1 that backup procedures be available in the event of CPS failure.

We conclude that this guideline is based on sound HFE principles.

- 5.1-4-1 The structure and format of information in COPS should be compatible with the backup procedures.

#### Evaluation

This guideline is consistent with ISG Guideline 29 and NUREG-0700 Guideline 8.5.-2 regarding compatibility of various procedure presentations.

We conclude that this guideline is based on sound HFE principles.

- 5.1-5 Access to relevant displays and supporting information should be provided. Type 1 COPS will assure required displays and supporting information are available at the work location (e.g. Main Control Room). Type 2 and 3 COPS may provide information as part of COPS displays.

#### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.1.3.-5 on the availability of supplemental information.

We conclude that this guideline is based on sound HFE principles.

- 5.1-6 The COPS should provide the capability to look-ahead and look-back within the procedure.

### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.3.2.-1, Flexible Navigation.

We conclude that this guideline is based on sound HFE principles.

- 5.1-7 The COPS should provide a placekeeping function.

### Evaluation

This guideline is consistent with NUREG-0700 Guidelines in Section 8.3.1, Path Monitoring.

We conclude that this guideline is based on sound HFE principles.

### **3.3.3.2 Guidelines Applicable to Type 2 and Type 3 Systems**

- 5.2-1 COPS should provide the capability to verify that prerequisites or initial conditions have been met before procedure execution will continue.

### Evaluation

This guideline is a specific instance of NUREG-0700 Guideline 8.2.1-4, User's Verification of CBP Information. The functional capability to assess initial conditions is addressed in NUREG-0700 Guideline 8.2.2-1, Automatic Identification of Procedures.

We conclude that this guideline is based on sound HFE principles.

- 5.2-2 The COPS should indicate the active step(s).

### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.3.1-3, Coding of Current Location.

We conclude that this guideline is based on sound HFE principles.

- 5.2-3 Data evaluated by COPS to reach a result should be available to the operator.

### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.2.1-4, User's Verification of CBP Information.

Recommend that the guideline be expanded to make the logic/rules available as well as data.

We conclude that this guideline is based on sound HFE principles.

- 5.2-4 For procedures available in COPS, document control information (e.g. document and revision number, Level-of-Use category, plant name, procedure type) should be either continuously displayed or accessible on demand.

#### Evaluation

This guideline is consistent with NUREG-0700, Guideline 8.1.1-1, Procedure Title and Identification Information. The NRC guideline identifies title, procedure number, revision number, date, and organizational approval. The IEEE guide indicates “Level-of-Use category, plant name, procedure type”. These are good additions.

Why is this guideline not applicable to Type 1 procedures? If it is, it can be located following Guideline 5.1-2 above.

We conclude that this guideline is based on sound HFE principles.

- 5.2-5 The capability should be provided for a read-only view of the ongoing procedure activities within the main control room. While viewing any step is permissible in this mode, the currently active step will be controlled and advanced by the designated controller of the procedure.<sup>4</sup>

#### Evaluation

This capability is not addressed in the NRC CBP review guidance. In general, making procedures available to more than one operator is a good practice to support procedure verification, peer checks, and teamwork. However, this guideline raises some interesting questions.

- Can procedures other than the ones open at the primary procedure user be opened as active by other operations or once an operator is in COPS, his workstation is the only one which can display active procedures?
- What happens when an operator wants to get the support of another operator to handle a portion of a procedure?
- Should this guideline be applied to all classes of procedures, EOPs, NOPs, ARPs, etc?

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.2-5-1 Multiple views of the ongoing procedure in the Main Control room allow the shift supervisor and other operators to be aware of ongoing plant operations to support as necessary.

---

<sup>4</sup> See footnote number 3.

### Evaluation

This is a rationale for 5.2-5, not a design guideline. Since the information is already in Annex C, this guideline could be deleted.

### **3.3.3.3 Guidelines Unique to Type 3 Systems**

- 5.3-1 The characteristics and behavior of embedded soft controls should be compatible between the COPS and the plant control system.

### Evaluation

It is not clear exactly what this guideline means. Does the guideline imply that the COPS may incorporate plant control logic that is different from the control logic used elsewhere in the plant control system? Otherwise, how could an incompatibility exist? If a COPS uses an embedded soft control, I would think it should simply access the controller in the plant control system rather than having its own unique control software.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.3-2 Information needed to support effective use of embedded soft controls, such as the plant and equipment status, should be available at the point of use.

### Evaluation

While used in a slightly different context, the IEEE guideline is consistent with ISG Guideline 16 which states that "Soft controls should provide needed feedback to the user regarding the state of the control." This is one aspect of the information needed for effective use. NUREG-0700 does not explicitly address soft controls in CBPs. However, as noted in Annex C of the standard, NUREG-0700, provides review guidance for soft controls that are applicable to soft controls wherever they are implemented in the HSI. The IEEE guideline is consistent with many of the guidelines provided in NUREG-0700, Section 7, Soft Control System, that address feedback on control actions, e.g., Guidelines 7.2.3-3, Coordination of Soft Controls with Process Display.

We conclude that this guideline is based on sound HFE principles.

- 5.3-3 Procedure-based automation may be used to execute sequences of fully determined steps between predefined hold points in a procedure.

### Evaluation

The definition of "fully determined" should be provided.

We are not convinced this practice is acceptable for all categories of procedures. While sequence automation may make sense for normal operational procedures such as plant start-up, it may not be for emergency operations which are less often used and where the main function of the procedures is ensuring that plant safety

functions are maintained and restored if compromised. In this situation, operator awareness of the status of the plant's safety is supported by procedure execution. When sequences are automated, the possibility of loss of situation awareness increases (O'Hara & Higgins, 2010). Some evidence for this concern in EOP use stems from tests conducted early in the N4 design. Electricité de France implemented automation of EOP steps, and the results were not favorable. They subsequently abandoned the practice. Is there more recent information from research or operational experience to support this guidance for all types of procedures?

Further, when the automated sequence involves taking a control action, this guideline may be contrary to the guidance provided in the ISG. Review guideline 11 states that:

The computer-based procedure system should not automatically initiate control actions without first receiving a command from the operator to do so...

Thus procedure initiated control without operator authorization is not consistent with this guidance.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

*If the COPS provides the capability for procedure-based automation, then the following additional guidance applies.*

- 5.3-4 Automatic execution of sequences shall be initiated manually and utilized at operator discretion.

Evaluation

This guideline is consistent with ISG Guidelines 8 and 10.

We conclude that this guideline is based on sound HFE principles.

- 5.3-5 The use of automatic sequences by the COPS shall not be necessary to successfully perform the procedure.

Evaluation

This guideline is consistent with ISG Guideline 8. Is this guideline necessary given Guideline 5.3-4?

We conclude that this guideline is based on sound HFE principles.

- 5.3-6 The specification of automated sequences and hold points should be part of the formally controlled contents of such operating procedures.



### Evaluation

This is not explicitly addressed in NRC guidance. However, it is a logical extension of ISG Guideline 12 on criteria for determining hold points. Annex C provides a good list of examples of hold points that is consistent with the list in the ISG. The list should be made into a guideline, such as “hold point should be implemented when the following conditions exist...”

We conclude that this guideline is based on sound HFE principles.

- 5.3-7 Automated sequences shall begin and end within a single procedure.

### Evaluation

This is not explicitly addressed in NRC guidance; however, it is implied by NRC guidance that *procedures* should be manually initiated by operators, not automation, e.g., ISG Guideline 10.

We conclude that this guideline is based on sound HFE principles.

- 5.3-8 The COPS shall display the current system mode or state of system execution (e.g., manual, automatic, ready, running, holding, interrupted, completed, etc.).

### Evaluation

Not addressed in NRC CBP guidance, but is addressed in the Automation Report. Guideline 8.3-1 states that the current mode should be displayed and Guideline 1.1.3-2, Current Progress, states that the HSI should provide information on the progress of its current processes.

We conclude that this guideline is based on sound HFE principles.

- 5.3-9 The COPS should alert the operator if an unexpected mode or state change (e.g., an interrupt) occurs automatically.

### Evaluation

Not addressed in NRC CBP guidance, but is addressed in the Automation Report. Guideline 8.3-5 indicates that operators should be notified of mode changes.

How is this guideline different from 5.3-15 below?

We conclude that this guideline is based on sound HFE principles.

- 5.3-10 The COPS should provide the time history of step execution for automated sequences.

### Evaluation

Not addressed in NRC CBP guidance, but is addressed in the Automation Report. Guideline 8.4.2-1, Provide Information on Task Status, indicates that the HSI should provide the information on the status of all tasks performed by automation, e.g., all tasks accomplished thus far and the tasks yet to be performed.

We conclude that this guideline is based on sound HFE principles.

- 5.3-11 The COPS should provide information on initial conditions that must be met before an automated sequence may begin.

### Evaluation

Not addressed in NRC CBP guidance, but is addressed in the Automation Report. Guideline 8.4.2-2, Provide Information Needed to Authorize Task Continuation, indicates that the HSI should provide the information needed for operators to easily evaluate the current task status and determine if all conditions are met for authorizing automation to continue the task. Consistent with this more general guidance, should the COPS provide information on the status of the sequence just completed?

Additional information is needed to determine whether this guideline is based on sound HFE principles.

<Note: in the Standard, the next two guidelines duplicate the numbering of guidelines -10 and -11.>

- 5.3-10 Hold points define the end of each sequence, where procedure-based automation stops and waits for the operator to continue. Hold points should be established to engage the operator to:
- monitor and confirm the automation's progress
  - maintain awareness of the status of the affected plant systems and operations
  - evaluate decisions required by the procedure

### Evaluation

This guideline is consistent with ISG Guideline 12 which states that hold points should be established.

The first sentence is a definition, not a design guideline.

We conclude that this guideline is based on sound HFE principles.

- 5.3-11 The location of hold points should be conspicuously displayed on the COPS.

### Evaluation

This aspect of CBPs is not explicitly addressed in NRC CBP guidance, but is an application of ISG Guideline 8 indicating that procedure steps should be predictable. The guideline is also addressed at a higher-level in the Automation Report.

Guideline 8.1.3-4 states the HSI should support the prediction of future status. Conspicuously identifying hold points will enhance the operator's awareness of how the automation will function and, therefore, the predictability of the procedure.

We conclude that this guideline is based on sound HFE principles.

- 5.3-12 At any <missing word from the Standard> before the start of an automatic sequence, the COPS should permit the operator to temporarily add hold points between the steps of the sequence. That is, the operator should be able to subdivide a sequence as needed to better manage the controlled process.

#### Evaluation

Is the word "time" missing from the guideline?

This is not explicitly addressed in the NRC guidance, but is a logical extension of the NRC guidance on need for operators to be in control of the procedures.

We conclude that this guideline is based on sound HFE principles. However, guidance should be provided to address the management of temporary hold points once the procedure is completed.

- 5.3-13 Both predefined and temporary hold points should be selected such that the controlled process is left in a stable condition.

#### Evaluation

This is not explicitly addressed in the NRC guidance. While predefined hold points can be evaluated during procedure development to ensure that they occur in places where stable conditions are assured, how can stability be assured for temporary hold points?

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.3-14 The operator may manually interrupt execution at any point in a sequence. Control commands issued prior to the interrupt may continue in effect or to completion on the controlled system.

#### Evaluation

This guideline is consistent with ISG Guideline 8. We suggest that the Standard clarify how a manual interrupt differs from a temporary hold point.

We conclude that this guideline is based on sound HFE principles.

- 5.3-15 The COPS should automatically interrupt the sequence if (1) conditions are not satisfied to complete the current step, or (2) selected faults or trips occur in the controlled plant systems.

### Evaluation

This guideline is generally consistent with ISG Guideline 11. Shouldn't it state that the COPS should automatically interrupt if the automatic sequence cannot complete its activity? The meaning of "selected" should be clarified, especially since it may be different for different classes of procedures.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.3-16 Automatic interrupts should include an alerting function and identify the source of the interrupt and where the sequence has stopped.

### Evaluation

This guideline is consistent with several NRC guidelines:

- NUREG-0700 Guideline CBP 8.2.2-11, Identification of User Input Requirements
- Automation Report Guideline 8.1.3-5, Notification of Significant Changes
- Automation Report Guideline 8.3-5, Notification of Automatic Mode Change

Stopping an automatic sequence based on an identified condition is referred to as "automation by exception" in the draft automation guidance. Automatic interruptions as defined in the Standard are examples of exceptions. Automation Report Guideline 8.4.3-1, Provide Information on Reason for Exception, states that "The HSI should identify the exception automation has encountered and the information needed by the operator to evaluate the exception condition. Additional Information for this guidelines states that "Automation may pause for a number of reasons and the operator's decision as to how to proceed may differ depending on the exception encountered."

We conclude that this guideline is based on sound HFE principles.

- 5.3-17 After manually interrupting a sequence, the operator should be able to resume automatic execution if desired.

### Evaluation

This capability is not addressed in NRC guidance. However, a means to reengage the automation is necessary. Guidance for assessment of preconditions for engaging automation should apply at this point and operators should be given the information needed to assess or verify preconditions.

We conclude that this guideline is based on sound HFE principles.

### 5.3-18 Direction for multiple procedure step processing.

#### Evaluation

This guideline does not provide design guidance.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

### **3.3.3.4 COPS Backup**

The guidance in this section applies to all types of COPS unless otherwise noted.

- 5.4-1 Backup procedures should be readily accessible to the users of COPS, such that users can make the transition from COPS to backup procedures in a timely manner under all conditions.

#### Evaluation

This guideline is consistent with NUREG-0700, Guideline 8.5-1, ISG Guideline 25, and ISG Guideline 26.

We conclude that this guideline is based on sound HFE principles.

- 5.4-2 Backup procedures should be presented in a manner that is compatible with the presentation of the same procedure on the COP system; to facilitate training of the operators on both presentations and to reduce the potential for confusion or errors when making the transition from one to the other.

#### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.5-2 and ISG Guidelines 29 and 30 addressing compatibility of CBPs and their backup systems.

While I agree that compatibility between procedure systems will “facilitate training of the operators on both presentations and reduce the potential for confusion or errors when making the transition from one to the other,” it seems out of place as a specific design guideline. It’s a rationale for the guideline and perhaps should be moved to Annex C.

We conclude that this guideline is based on sound HFE principles.

- 5.4-3 Identifiable failure modes and degraded conditions of the COPS should be identified, and COPS users should be trained to recognize when such conditions exist so that transition to the backup procedures can be performed in a timely manner.

#### Evaluation

This guideline is consistent with Degraded Conditions Report Guideline 1 and 2 in Section 7, Design Process Review Guidelines. It is also consistent with Automation

Report Guidelines 8.6-1, 8.6-2, and 8.6-3 addressing the communication of degraded and failed conditions to operators.

While we agree that “COPS users should be trained to recognize when such conditions exist so that transition to the backup procedures can be performed in a timely manner,” it seems out of place as a specific design guideline. Perhaps it should be moved to Annex C.

We conclude that this guideline is based on sound HFE principles.

- 5.4-4 For Type 2 or Type 3 COPS, when a system failure or degradation occurs that requires transition to a backup procedure, the operator should be able to determine: (1) what procedures were being executed at the time of failure, (2) which step in each procedure was being processed at the time of failure, and (3) what conditions or steps, if any, were being continuously monitored by the COP system at the time of failure.

#### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.5-3 and ISG Guideline 28.

We conclude that this guideline is based on sound HFE principles.

- 5.4-5 The time required for the operator to effectively transition from the COP to the backup procedure should not be so long that the primary goals of the procedure cannot be met or plant safety is jeopardized due to the delay necessitated by the transition.

#### Evaluation

This guideline is consistent with ISG Guideline 28.

We conclude that this guideline is based on sound HFE principles.

- 5.4-6 After transitioning to a backup procedure from a failed or degraded Type 3 COPS, the operator should be able to stop the processing of the computerized procedure.

#### Evaluation

This topic is not addressed in NRC guidance. In general, this is consistent with the guidance on operator control of procedures.

We conclude that this guideline is based on sound HFE principles.

### **3.3.3.5 Quality Assurance**

- 5.5.1-1 When procedures are implemented on a platform (hardware and software) that is not safety-related, appropriate IEEE standards for isolation between systems should be consulted.

### Evaluation

This area is not addressed in the NRC CBP guidance. This area is addressed by I&C guidance and standards, but it is good to point to those standards.

We conclude that this guideline is based on sound engineering principles.

- 5.5.1-2 For Type 1, the computer system should be subject to administrative controls suitable for systems that manage data important to safety.

### Evaluation

This area is not addressed in the NRC CBP guidance. Perhaps the guidance should also recommend that designers apply nuclear power plant-specific QA and administrative controls that are applicable to both procedure development and control room/HSI design.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.5.1-3 For Type 2, a graded approach can be taken in determining the level of rigor of the QA/V&V <verification and validation> activities undertaken to demonstrate adequate quality of the hardware and software of the CBP system.

### Evaluation

See comment for Guideline 5.5.1-2.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

*The following three guidelines apply to Type 2 and Type 3 COPS.*

- 5.5.2-1 COPS should use validated data for display of process information, step processing, and automation.

### Evaluation

Good in general. This guidance is consistent with the guidance in Section 1.4 of NUREG-0700 and ISG 7.

We conclude that this guideline is based on sound HFE principles.

- 5.5.2-2 When quality status information is available for data displayed by COPS and the quality of a displayed data item is bad or suspect, the quality information should also be displayed.

### Evaluation

This is consistent with NUREG-0700 Guidelines 1.4-9 and 1.4-10 and ISG Guideline 7.

We conclude that this guideline is based on sound HFE principles.

- 5.5.2-3 COPS should inform the operator when a data quality problem is detected with data that is used in step logic processing potentially affecting the results of the processing. For Type 3, the automated sequence should stop (i.e., an automatic interrupt should occur with an audible and visual alarm to alert the operator) and wait for the operator to determine an appropriate course of action.

#### Evaluation

In general, this guidance is generally consistent with NRC guidance for addressing degraded conditions. Alerting operators to degraded data quality and to early termination of an automatic sequence is appropriate. However, does the guideline mean that poor data can be used for logic processing as long as operators are alerted? If data is of sufficiently poor quality, it seems no logic assessment should be made at all. Operators should be made aware of the issue and use alternative means to assess the step logic.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

### **3.3.3.6 Maintenance and Configuration Management**

The Standard provides guidelines related to maintaining COPS and configuration management associated with COPS. The guidance applies to all three types of computerized procedures except where otherwise noted.

- 5.6.1-1 Means should be provided to control changes made to the procedures over the life of the plant, ensuring that quality and correctness of the procedures and any associated automation are maintained during the lifetime of their use in the plant. The system should be able to be updated without impacting plant operations.

#### Evaluation

With respect to changes to procedures, the guidance is consistent with NUREG-0700 Guidelines in Section B3.8.4, Maintenance of Procedures, Section B3.8.10, Verification and Validation. Utilities make procedure changes and improvements over the lifetime of the plant and these changes need to be reflected in the COPS. The technical content of the procedures should be capable of being updated in a controlled fashion as is standard practice in utilities today. The modified procedures should be able to be "loaded" into the COPS without having to modify the COPS software.

As for the automation, clarification (and possibly guidance) is needed regarding the aspects of automation being maintained, e.g., resolution of step logic, transition through procedure steps, monitoring (e.g., of continuously applicable steps, procedure entry conditions, cautions, critical safety functions), and embedded soft controls.

The last sentence should be a separate guideline.



Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.6.1-2 The configuration control and procedure management processes should ensure that: (1) the procedure contents are fully verified and validated prior to being issued for use and (2) the COPS always presents the most recent approved and issued version of each procedure.

#### Evaluation

For the first part of this guideline, see comments for Guideline 5.5.1-2 and 6.6.1-1 (regarding updating of procedure technical content). The second part of this guideline is consistent with ISG Guideline 3.

We conclude that this guideline is based on sound HFE principles.

- 5.6.1-2.1 COPS should support station administrative processes for identifying procedure errors and necessary revisions.

#### Evaluation

It is not clear what type of support this guideline is referring to.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

- 5.6.1-2.2 The COPS should provide the operator the capability to flag errors discovered in its content.

#### Evaluation

This guideline is consistent with NUREG-0700 Guideline 8.3.3-3, Note Taking.

We conclude that this guideline is based on sound HFE principles.

- 5.6.1-3 To facilitate ease of procedure maintenance and system configuration management, the software architecture and data structures of the COPS should be designed such that procedure changes can be made without changing the application software.

#### Evaluation

As noted in the discussion of Guideline 5.6.1-1, this guidance is needed to ensure utilities can maintain updated procedures in a timely manner (not require COPS designers to modify software every time a procedure change is made). This also avoids the potential introduction of software programming errors into the COPS software every time that a procedure is updated.

We conclude that this guideline is based on sound HFE principles.

5.6.1-4 Means should be provided to ensure adequate V&V of changes made to Type 2 and Type 3 COPS.

#### Evaluation

This guideline needs to be clarified to make it clear what is being addressed that is not already addressed in the earlier guidance presented above, e.g., Guideline 5.6.1-2 which also requires V&V.

Additional information is needed to determine whether this guideline is based on sound HFE principles.

5.6.1-5 The configuration management program should ensure that consistency is maintained between COPS and any backup procedures expected to be used upon failure of the COPS.

#### Evaluation

This guideline addresses the same overall concern as ISG Guidelines 27 through 30 and 0700 Guideline 8.5-2.

We conclude that this guideline is based on sound HFE principles.

### **3.4 Conclusion**

Although the IEEE Standard is still in development, it is sufficiently mature for us to conclude that the IEEE Standard generally meets Criterion 2; that the guidance is based in sound HFE principles. Table 3-1 summarized the number of guidelines (GIs) in each section of the Standard and the distribution of the evaluations into acceptable vs. need additional information (AI) to evaluate fully.

Of the 57 guidelines in the Standard, we found 44 to be acceptable, i.e. based on sound HFE principles. For some of these guidelines, we provided suggestions to help clarify or expand the guidelines application, but these comments did not impact the evaluation of the guidance itself.

We identified 14 guidelines for which additional information is needed before a determination of acceptability can be made. These guidelines are identified in the last column of Table 3-1.

We identified one potential exception concerning automation of procedure sequences when applied to EOPs:

5.3-3 Procedure-based automation may be used to execute sequences of fully determined steps between predefined hold points in a procedure.

This guidance would allow the automation of EOP steps, including procedure-initiated control actions. We concluded this guidance was not justified based on current information and is discrepant with guidance in the ISG (see the evaluation section for Guideline 5.3-3 for a full discussion of our concerns). If the IEEE standard developers cannot provide

additional information in support of the acceptability of this guidance, we recommend the NRC staff take exception to this guideline.

Table 3-1 Summary of IEEE Guideline Evaluations

Section	No of GIs	Acceptable	AI Needed	GIs Needing AI
General Principles	4	3	1	4.1.3
<i>Design Guidelines</i>				
Guidelines Applicable to Type 1, 2 & 3 Systems	9	8	1	5.5-1
Guidelines Applicable to Type 2 and Type 3 Systems	5	5	1	5.2-5
Guidelines Unique to Type 3 Systems	20	15	5	5.3-1 5.3-3 5.3-13 5.3-15 5.3-18
COPS Backup	6	6	0	
Quality Assurance	6	3	3	5.5.1-2 5.5.1-3 5.5.2-3
Maintenance and Configuration Management	7	4	3	5.6.1-1 5.6.1-2.1 5.6.1-4
<b>Total</b>	<b>57</b>	<b>44</b>	<b>14</b>	

## 4 Guidance Peer Review Evaluation

### 4.1 Objective

With respect to Section 1.3, Criterion 3, we evaluated whether the guidance is subject to a thorough peer-review process.

### 4.2 Methodology

We evaluated the peer-review process to identify whether (1) a documented process is used, (2) the process involves appropriate subject matter experts (SMEs), and (3) SME comments are reasonably resolved.

### 4.3 Results

#### 4.3.1 Peer-Review Process

As a consensus standard, the IEEE document has a formal process for obtaining and resolving comments. Peer review occurs at multiple stages in the standard development process. During development, the standard development committee accepts comments per the *Boggi Procedure*<sup>5</sup> (Boggi, 1998). Section 4 of the procedure describes the comment process:

- 4.1 Complete Attachment C, "Review and Comment." (This is a formal comment form).
- 4.2 Submit completed form to the Standard Champion.
- 4.3 The Standard Champion shall perform an initial screening for completeness, validity and to ascertain if the request is a change of intent or an editorial change.
- 4.4 If necessary, the Champion will contact the reviewer to clarify the comment.
- 4.5 The Champion will disposition each comment in writing.
- 4.6 Comment dispositions will be sent to each reviewer.
- 4.7 The reviewers will signify they accept the Champions' disposition by either signing the Comment Form or by other written means. Irreconcilable differences will be passed to the Working Group Chair for judgment.

Once the Standard is complete from the perspective of the SC-5 development activities, it is sent for ballot approval. IEEE standard balloting is a formal process used for all IEEE standards. It is governed by rules provide in the *Standards Board Operations Manual* (IEEE, 2009b).

---

<sup>5</sup> IEEE Subcommittee (SC) – 7 has been combined with SC-5. All activities are now under SC-5.

Section 5.4 of the manual addresses the ballot process. Some key aspects of the methodology are summarized below. See Section 5.4 of the manual for complete details.

A key aspect of the process is the need for diverse representation of SMEs:

The balloting group shall provide for the development of consensus by all interests significantly affected by the scope of the standard. This is achieved through a balance of such interests in the balloting group membership. Balance is defined as the avoidance of dominance by any single interest category. (p. 21).

Balloters identify their type of affiliation, e.g., corporation, government agency, and academic, and the pool of balloters cannot exceed 50% of any one category. If needed, the SC can recommend outside experts to participate in order to obtain the necessary technical SMEs to provide a thorough review.

Balloters vote on a standard as “approve,” “do not approve (negative vote),” or “abstain.” When casting a negative vote, the balloter provides comments that need to be addressed to make the standard acceptable.

Each ballot comment has to be addressed and documented. Per the methodology for addressing comments:

Changes may be made in the document to resolve negative votes that are accompanied by comments or for other reasons. All substantive changes made since the last balloted draft shall be identified and recirculated to the Sponsor balloting group. All unresolved negative votes with comments shall be recirculated to the Sponsor balloting group. The verbatim text of each comment, the name of the negative voter, and a rebuttal by the members conducting the resolution of comments shall be included in the recirculation ballot package. Responses to comments should include sufficient detail for ballot group members to understand the rationale for rejection of the comment or revision of the change proposed by the commenter. (p. 25)

For a ballot process to be successful, 75% of the balloter must vote. For a standard to be approved 75% approval is required.

The Standard is not yet at this stage. The ballot process provides review from a broader group of SME. A balloter can accept or reject the standard. They can provide technical issues that should be addressed. When a standard is rejected, the balloter provides technical justification for the rejection and identifies what needs to be addressed to make the standard acceptable. Thus the IEEE process to ballot standards provides yet another opportunity to obtain peer review.

Taken together, the IEEE procedure to obtain comment during standard development and balloting as part of standard approval provides a comprehensive and auditable means of obtaining peer review.

#### **4.3.2 Subject Matter Participants**

The comments currently made on the Standard are from members of IEEE Subcommittee 5. As discussed above, the IEEE ballot process requires a diverse group of SMEs. Thus, the IEEE Standard should be reviewed by appropriate SMEs.

### **4.3.3 Treatment of SME Comments**

At the present time, the Standard's development committee has received approximately 300 comments, under the Boggi Procedure, that are in the process of being resolved. As noted above, the formal balloting process for Standard approval has yet to take place.

As the comments received are currently being addressed by the Standard's developers, and resolutions are not finalized, we examined a small sample of them to determine whether they are, in our judgment, being fairly considered.

### **4.4 Conclusion**

Although the Standard has not completed its peer review process, based on the information reviewed at this time, plus the current plan in place to obtain comments during the balloting process, we conclude that the Standard meets Criterion 3 for a thorough peer-review process that uses (1) a documented process, (2) appropriate subject matter experts (SMEs), and (3) a reasonable approach to resolving SME comments.

## 5 Human Performance Issue Evaluation

### 5.1 Objective

With respect to Section 1.3, Criterion 4, we evaluated whether the Standard addresses identified CBP human performance issues. The existence of a CBP issue means that the NRC does not have sufficient guidance to address that aspect of human performance. If the Standard addresses any of these issues, it helps to fill gaps in the NRC guidance.

### 5.2 Methodology

CBP issues are identified in the following reports:

- BNL Technical Report 79947-2008 (O'Hara et al., 2008b), which includes those identified in NUREG/CR-6634 (O'Hara et al., 2000)
- HPR-355 (O'Hara et al., 2003)
- Recent CBP literature

In addition, we considered HFE issues identified in the reports on automation (O'Hara & Higgins, 2010) and degraded I&C conditions (O'Hara, Gunther, & Martinez-Guridi, 2010). These reports contained many HFE issues that can be interpreted within the context of CBPs.

The lists of issues contained in the above documents overlap to a great extent. Therefore, we consolidated the issues into one list. The Appendix to this report described the issues identified. Recent literature pertaining to CBP issues is cited in the Appendix.<sup>6</sup> We then evaluated the Standard to determine if the guidance addressed any of the issues identified.

### 5.3 Results

The HFE research issues pertaining to computer-based procedure systems are listed in the first column of Table 5-1 (see the Appendix for a description of the issues). Where the Standard does provide guidance addressing an identified issue, the section is identified in the second column of the table, and a brief description of the information address to the issue is given. If the Standard does not address the issue, the column entry is not applicable (NA).

Where we noted the Standard addresses an issue, it does not mean the issue is completely resolved by the guidance provided. In all cases where the Standard provides information and contributes to issue resolution, additional research is still needed.

---

<sup>6</sup> We reviewed studies published after 2000. While there were many CBP publications, most were system descriptions. Very few discuss issues beyond those already identified by the NRC. Those few pertinent studies are identified in the Appendix. This is not surprising in light of the fact that the NRC recently updated the issues list in 2008.

Table 5-1 CBP HFE Research Issues Addressed by the IEEE Standard

HFE Research Issue	Standard Section
Lack of Data on the Effects of CBPs on Crew Performance	NA
Acceptance Criteria for CBP Performance Effects	NA
Role of Plant Personnel in Procedure Management: Trust and Appropriate Use	NA
Level of Automation of Procedure Functions	5.3, Guidelines Unique to Type 3 Systems – This section addresses automation of control functions, sequence automation, and hold points
Teamwork and Team Performance	5.2 Additional Guidelines Applicable to Type 2 & Type 3 Systems, specifically Guideline 5.2-5 addressing multiple users of CBPs (see footnote 3)
Situation Awareness, Response Planning, and Operator Error	NA
Keyhole Effects and Use of Multiple Computer-based Procedures	NA
CBP Complexity and Opacity	NA
Specific Computer-Based Procedure Design Features	NA
Hybrid Procedure Systems	NA
CBP Degradation, Failure Modes, and Backup Systems	Section 5.4, COPS Backup – specifically Guidelines 5-4-4 through 5.4-6 that identify the need to evaluate degraded conditions and timely transition to backup procedures
Transitioning to CBP Systems from a PBP Operational Environment	NA
Training in CBP Usage	NA

## 5.4 Conclusion

We conclude that the Standard meets Criterion 4 by addressing human performance issues identified by the NRC and others in the nuclear industry. Specifically, the Standard contributes to resolving issues related to:

- Level of Automation of Procedure Functions
- Teamwork and Team Performance
- CBP Degradation, Failure Modes, and Backup Systems



## 6 Recommendations

### 6.1 Overall Summary

The purpose of this review is to evaluate the IEEE Standard on Computerized Procedures for its suitability for use in the staff's HFE safety reviews of CBP systems and to ensure that the guidance meets the NRC's standard for scientific and engineering rigor used for its own guidance development efforts. To be used in the staff's safety review of applicants' CBP systems, the Standard should meet the following criteria:

1. The Standard meets an existing need of NRC reviewers, i.e., the Standard should provide guidance that address characteristics of CBP systems not currently addressed in existing NRC guidance.
2. The Standard is based in sound human factors engineering principles. (This is referred to as "internal validity" in the NRC HFE guidance development process.)
3. The Standard is a thorough peer-reviewed. (This is referred to as "external validity" in the NRC HFE guidance development process.)
4. An additional consideration is whether the Standard addresses CBP-related human performance issues. While it is not necessary for the Standard to address specific human performance issues identified by the NRC and industry, it is a significant benefit if it does.

The conclusion of our evaluation is that the Standard meets Criteria 1 and addresses aspects of CBPs that are not addressed in existing NRC guidance. It also provides additional guidance for some topics that are addressed.

Although the Standard is still in development, it is sufficiently mature for us to conclude that it generally meets Criterion 2; the guidance is based in sound HFE principles. Table 3-1 summarized the number of guidelines in each section of the Standard and the distribution of the evaluations into "acceptable" vs. "need additional information to evaluate fully." We found that most of the guidelines are acceptable. For some of these guidelines, we provided suggestions to help clarify or expand the guidelines application, but these comments did not impact the evaluation of the guidance itself.

We identified 14 guidelines for which additional information is needed before a determination of acceptability can be made. One of these may warrant an exception. It addresses automation of procedure sequences when applied to EOPs:

5.3-3 Procedure-based automation may be used to execute sequences of fully determined steps between predefined hold points in a procedure.

This guidance would allow the automation of EOP steps, including procedure-initiated control actions. We did not think this guidance is justified based on current information and is discrepant with guidance in the ISG (see the evaluation section for Guideline 5.3-3 for a full discussion of our concerns). If the IEEE Standard developers cannot provide additional information in support of the acceptability of this guidance, we recommend the NRC staff take exception to this guideline.

Although the Standard has not completed its peer review process, based on the information reviewed at this time, plus the current plan in place to obtain comments during the balloting process, we conclude that the Standard meets Criterion 3 for a thorough peer-review process that uses (1) a documented process, (2) appropriate subject matter experts (SMEs), and (3) a reasonable approach to resolving SME comments.

Finally, we conclude that the Standard meets Criterion 4 by addressing human performance issues identified by the NRC and others in the nuclear industry.

## **6.2 Recommended Follow-up to This Evaluation**

As noted above, this review should be updated to address (1) clarifications that may be provided by the Standard developers for the guidelines listed in the last column in Table 3-1, (2) changes that are made to the guidance subsequent to the September 30, 2009 version of the Standard, and (3) changes made in subsequent revisions of the standard and to follow-up on the resolution of peer review comments.

Once the balloting process is complete, a verification of the proper completion of the peer review process should be made.

## **6.3 Recommendation for Standard Endorsement**

We recommend that the NRC provisionally endorse the Standard<sup>7</sup> with possible exceptions. The guidance found acceptable can be included in the endorsement. However, the endorsement is provisional pending completion and verification of the final guidance. Possible exceptions are the guidelines for which additional information is needed. If the IEEE can provide the additional information addressing the concerns raised, some or all of the guidelines may be reevaluated as “acceptable” and the exceptions eliminated.

---

<sup>7</sup> Note that for NRC to endorse the Standard, it has to be approved by the IEEE ballot process. That process should take place early in 2010.

## 7 References

- Boggi, M. (1998). *SC-7 Boggi Procedure: SC-7 Internal Procedure to Request, Review and comment on Standards*. Piscataway, NJ: IEEE.
- Huang, F. & Hwang, S. (2009). Experimental studies of computerized procedures and team size in nuclear power plant operations. *Nuclear Engineering and Design*, 239 (2), 373-380.
- IEEE (2009a). *Human Factors Guide for Applications of Computerized Operating Procedure Systems at Nuclear Power Generating Stations and other Nuclear Facilities* (Draft Guideline 1786, 9/30/09 version). New York, NY: Institute of Electrical and Electronics Engineers.
- IEEE (2009b). *IEEE-SA Standards Board Operations Manual*. New York, NY: Institute of Electrical and Electronics Engineers.
- IEEE (2004). *IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations* (IEEE Std. 1023-2004). New York: Institute of Electrical and Electronics Engineers. New York, NY: Institute of Electrical and Electronics Engineers.
- IEEE (1998). *IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations* (IEEE Std. 1289-1998). New York, NY: Institute of Electrical and Electronics Engineers.
- Mackay, W. (1999). Is Paper Safer? The Role of Paper Flight Strips in Air Traffic Control. *ACM Transactions on Computer-Human Interaction*, 6 (4), 311-340.
- Nomura, S., Hutchins, E., & Holder, B. (2009). The Uses of Paper in Commercial Airline Flight Operations. *CSCW'06*, Alberta, Canada: ACM.
- NRC (2008). *Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF): Interim Staff Guidance* (DI&C-ISG-05, ML082740440). Washington, D.C.: U.S. Nuclear Regulatory Commission.
- 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., Gunther, W., & Martinez-Guridi, G. (2010). *The Effects of Degraded Digital Instrumentation and Control Systems on Operator Performance: HFE Review Guidance and Technical Basis* (Draft BNL Technical Report 91047-2010). Upton, NY: Brookhaven National Laboratory.

- O'Hara, J. & Higgins, J. (2010) *Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis* (BNL Technical Report B91017-2010). Upton, NY: Brookhaven National Laboratory.
- O'Hara, J., Higgins, J., Brown, W., Fink, R., Persensky, J., Lewis, P. & Kramer, J. (2008a). *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants* (NUREG/CR-6947). Washington, D.C.: U. S. Nuclear Regulatory Commission.
- O'Hara, J., Higgins, J., Brown, W. & Fink, R. (2008b). *Human Factors Considerations with Respect to Emerging Technology in Nuclear Power Plants: Detailed Analyses* (BNL Technical Report No: 79947-2008). Upton, NY: Brookhaven National Laboratory.
- O'Hara, J., Higgins, J., 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., Pirus, D., Nilsen, S., Bisio, R., Hulsund, J-E, and Zhang, W. (2003). *Computerization of Procedures: Lessons Learned and Future Perspectives* (HPR-355). Halden, Norway: Institute for Energiteknikk – OECD Halden Reactor Project.
- 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.
- 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.
- Throneburg, E. & Jones, J. (2006). Situation Awareness and Trust in Computer-Based Procedures in Nuclear Power Plant Operations. In *Proceeding of the American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2006)*. La Grange Park, Illinois: American Nuclear Society, Inc.
- Woods, D., Roth, E., Stubler, W., and Mumaw, R. (1990). Navigating through large display networks in dynamic control applications. In *Proceedings of the Human Factors Society 25th Annual Meeting*. Santa Monica, CA: Human Factors Society.
- Xu, S., Song, F., Li, Z., Zhao, Q., Luo, W., He, X., & Salvendy, G. (2008). An ergonomics study of computerized emergency operating procedures: Presentation style, task complexity, and training level. *Reliability Engineering & System Safety*, 93 (10), 1500-1511.

## **Appendix - HFE Research Issues Pertaining to Computer-based Procedure Systems**

This appendix presents a list of human performance issues related to CBP systems. The issues are mainly derived from various reports including (O'Hara et al., 2000; O'Hara et al., 2003; O'Hara et al., 2008b). The lists of issues contained in these documents overlap to a great extent. Therefore, we consolidated the issues into one list presented below. These main sources are not individually cited below.

In addition, we considered HFE issues identified in recent reports on automation (O'Hara & Higgins, 2010) and degraded I&C conditions (O'Hara, Gunther, & Martinez-Guridi, 2010). These reports contained many HFE issues that can be interpreted within the context of CBPs.

Finally, we also examined recent literature directly pertaining to CBP issues. Where appropriate, these studies are cited below.

The results led to the identification of the following issues:

- Lack of Data on the Effects of CBPs on Crew Performance
- Acceptance Criteria for CBP Performance Effects
- Role of Plant Personnel in Procedure Management: Trust and Appropriate Use
- Level of Automation of Procedure Functions
- Teamwork and Team Performance
- Situation Awareness, Response Planning, and Operator Error
- Keyhole Effects and Use of Multiple Computer-based Procedures
- CBP Complexity and Opacity
- Specific Computer-Based Procedure Design Features
- Hybrid Procedure Systems
- CBP Degradation, Failure Modes, and Backup Systems
- Transitioning to CBP Systems from a PBP Operational Environment
- Training in CBP Usage

### **A.1 Lack of Data on the Effects of CBPs on Crew Performance**

Definitive conclusions about the value of CBP systems are hampered by the lack of data on their effects on crew performance and plant safety. While CBPs are beginning to be used in nuclear power plants (NPPs), there is little operational experience to use in evaluating their effects.

There have been experimental evaluations of CBPs, but these have been quite limited as well. Generally, the studies were not well-controlled comprehensive evaluations and have not examined CBP usage in broad operational contexts. 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 (e.g., O'Hara et al., 2000) 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).

Methodologically sound and comprehensive evaluations of CBPs and their effects on crew performance have yet to be performed.

## **A.2 Acceptance Criteria for CBP Performance Effects**

The issue of acceptance criteria for CBP acceptance needs to be addressed from both research and regulatory review perspective. Should CBP systems improve performance in comparison to paper procedures, or is it sufficient that such systems do not degrade performance? This is a very important distinction. If the criteria is to improve performance, criteria on what constitutes improvements needs to be established. In either case, we need to identify the performance measures and criteria to be used.

## **A.3 Role of Plant Personnel in Procedure Management: Trust and Appropriate Use**

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.

These issues are common to all applications of automation (O'Hara & Higgins, 2010). CBPs automate certain aspects of procedure use. As with any automation, the issue of trust and appropriate use need to be addressed to avoid issues related to complacency and automation bias. The applicability of these general automation issues to CBPs has recently been recognized in the literature (Huang & Hwang, 2009; Throneburg & Jones, 2006).

Thus, an issue that needs to be addressed is how to design CBP systems that foster appropriate levels of trust and enable the operators to maintain an independent perspective so they can monitor and evaluate the procedure's contribution to achieving higher-level safety goals; while at the same time managing operator workload. The knowledge required to manage a CBP system will be different from that required to handle conventional procedures. For example, the CBP system may use different analyses to resolve logic steps than those employed by operators.

## **A.4 Level of Automation of Procedure Functions**

CBPs can perform many functions and can employ different levels of automation for each (O'Hara & Higgins, 2010). The decision as to the appropriate level of automation will impact operator performance, situation awareness, workload, and errors. A better understanding is needed of the tradeoffs between procedure function automation and overall management of the events and activities the procedures are being used for.

One area of procedure automation that is especially noteworthy 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 Teamwork and 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 situation awareness (SA), error detection and recovery. Thus, technologies that impact teamwork may impact defense-in-depth and plant safety. For example, there is 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. Research is needed to better understand the effect of CBP automation on teamwork, including coordinating team members and communications, and team performance.

## **A.6 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, 2002). 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. The situation awareness of other operators is affected as well.

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. 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.

## **A.7 Keyhole Effects and Use of Multiple Computer-based Procedures**

The keyhole<sup>8</sup> effect has been identified as a root cause of many of the known human performance challenges in computer-based control rooms (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. 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.8 CBP Complexity and Opacity**

One of the recurrent themes that cut across many of the issues identified associated with computer-based control rooms and automated systems is that of complexity. 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.

---

<sup>8</sup> The characteristic of viewing information through the limited area provided by video display units (VDUs) has been referred to as the "keyhole effect" (Woods et al., 1990). In the analogy, one views only a small portion of a room when peering through the keyhole in a closed door. Similarly, VDUs are like keyholes in that they provide operators a view of only a small amount of the available information at any one time. The consequence of the keyhole effect is that, at any given time, most of the information is hidden from view.



This issue applies as much to CBP systems as it does to other HSI resources. For example, Xu et al. (2008) found that complexity of CBP affected error rates. 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.

A related issue is the level of detail the CBP presents. 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 operator's situation awareness.

## **A.9 Specific Computer-Based Procedure Design Features**

The relative effects of specific CBP design features on performance have received little attention in the literature. Most studies have focused on overall system comparisons, e.g., CBP vs. paper-based procedure (PBP), and not systematic evaluations of individual characteristics.

As an example of this issue, the use of traditional procedure formats, such as column formatted text and flowcharts, may not be the best method of representing of procedure information in CBP systems. The effects of HSI techniques, such as outline views, navigational aids, and coding and highlighting on text and flowchart formats, needs to be determined.

## **A.10 Hybrid Procedure Systems**

In some plants, CBP systems may be available for all plant procedures, while others may limit CBP systems to certain procedures, such as EOPs, leaving the other in paper form. This essentially creates a hybrid procedure system. The issue arises as to whether operators can effectively use CBPs when they are only used in emergencies. 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.11 CBP Degradation, Failure Modes, and Backup Systems**

Most of the studies that have considered loss of CBP systems focus on complete failure. HFE guidance addressing CBP failure has followed the same approach, limiting the consideration to loss of CBPs and transitions to alternative backup systems, such as PBPs. However, recent research has shown that HSIs are impacted by a wide range of degraded I&C conditions (O'Hara, Gunther, & Martinez-Guridi, 2010). Many of these degraded conditions can be more significant than complete failure in that the degradation may not be recognized by operators. With complete failure, the loss of the CBP is obvious as is the need to transition to backups. This is not the case with degraded conditions. Further, some degraded conditions can lead to displays that are misleading and confusing.

This topic needs additional research to identify the types of degraded conditions of concern and to develop methods to identify them. Backup systems need to be considered from this

broader perspective by matching backup alternatives to the significant type of degraded conditions that can arise.

Another consideration is the context of the degraded condition or failure. The 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.12 Transitioning to CBP Systems from a PBP Operational Environment**

When CBP systems are included in new plant designs, the concept of operations will incorporate the use of procedure automation, and operating crews will be trained in their use from the start. When CBP systems are introduced into a plant whose operations center on paper procedures and manual procedure management, the CBPs significantly alter the concept of operations (Roth & O'Hara, 2002). Research is needed to identify appropriate ways to manage the transition from paper/manual operations to CBP/automated operations and ensure the safety is not negatively impacted. For example, in an air traffic control system undergoing automation upgrades, Mackay (1999) noted the preserving a role for paper interfaces enabled controllers to build upon their existing "safe work practices" and let controllers gradually adapt to the new work practices offered by the new systems. An analogous approach in NPP operations may be to gradually introduce the automated features over time. Research on automation further suggests that automating lower-level cognitive activities, such as information acquisition, may be a good first step. Research is needed to better understand how such changes in concept of operations can be effectively managed without compromising safety. Similar research has been suggested in the aviation domain (Nomura, Hutchins, & Holder, 2009).

## **A.13 Training in CBP Usage**

Compared to the use of paper procedures, training for operators to use CBPs poses additional challenges to ensure that operators acquire adequate understanding of CBP operations. Training with CPSs requires training that goes beyond traditional procedure use. It should include

- Appropriate use of the CPS
- Crew supervisory roles and responsibilities
- Teamwork and communication
- HSI features and function and their usage
- CPS failure modes and how to recognize them
- Transitions to backup systems

With respect to recognition of failure modes and degraded conditions, research in automation and degraded conditions has emphasized the importance of simulator training. Exposure to specific degraded conditions improves the ability of operators to recognize such conditions when they actually occur in the operational environment. Research is needed to identify training methods needed to support operators in recognition and management of degraded conditions.