Computerized Procedures

Design and Implementation Guidance for Procedures, Associated Automation and Soft Controls

EPRI 1015313

Draft Report, December 2007

EPRI Project Manager
Joseph Naser

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

CDF Services, Inc.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

CITATIONS

[Later]

PRODUCT DESCRIPTION

[Later]

ABSTRACT

[Later]

ACKNOWLEDGMENTS

[This page will acknowledge the members of the NEI Task Force and other contributors to the preparation of this report.]

LIST OF ACRONYMS

AOP	Abnormal operating procedure
ARP	Alarm response procedure
BWR	Boiling water reactor
CBP	Computer-based procedure
CP	Computerized procedure (includes EP, CBP, and CBP with PBA)
EB	Emergency blowdown
EOP	Emergency operating procedure
EP	Electronic procedure
EPG	Emergency procedure guideline
HFE	Human factors engineering
HSI	Human-system interface
I&C	Instrumentation and control
IC	Isolation condenser
OP	Operating procedure
PBA	Procedure-based automation
PBP	Paper-based procedure
PRA	Probabilistic risk assessment
RPV	Reactor pressure vessel
SRV	Safety relief valve

STP	Surveillance test procedure
VDU	Video display unit

CONTENTS

LIST OF TABLES

1
INTRODUCTION

This industry guidance report provides guidance on the design and implementation of computerized procedures – procedures that are presented via computer as opposed to hard copy or paper-based procedures. Computerized procedures are an important part of the overall human-system interface in advanced control rooms being designed for new nuclear power plants. They also are being introduced into some operating plants as those plants modernize their control rooms. The guidance in this report can be applied for both new designs and modernizations.

1.1 Scope of the Guidance

The focus of the guidance is on design and implementation of computerized procedures used by the control room operating crew. These may include normal operating procedures (OPs), abnormal operating procedures (AOPs), alarm response procedures (ARPs), surveillance test procedures (STPs) and/or emergency operating procedures (EOPs). Operating crew members may use computerized procedures either inside or outside of the main control room (e.g., at the remote shutdown station). Although the focus is on operations, the guidance in this report may also be useful for design and implementation of computerized procedures used for plant maintenance activities.

In addition to computerized procedures, this guidance also addresses automation and soft controls that may be associated with computerized procedures. It does not address automation or soft controls that are not associated with computerized procedures.

The procedure development and maintenance program for a nuclear power plant should incorporate human factors engineering (HFE) principles and criteria, along with other design requirements, to develop and maintain procedures that are technically accurate, comprehensive, explicit, easy to use, and validated. The guidance in this document addresses only the computerized aspect of the procedures – it does not address the scope of procedures to be provided, the content and quality of the procedures themselves, or procedure generation. Those are addressed in existing regulatory guidance documents (e.g., Chapter 13 of NUREG-0800 [16], Regulatory Guide 1.33 [23], NUREG-0899 [17], Regulatory Guide 1.206 [22]). Also, the guidance given here addresses updating, configuration management and maintaining the validity of procedures, but only those aspects that are related to a computerized implementation. The existing regulatory guidance documents address the overall subject of procedure updating and maintenance.

The guidance in this document addresses design and implementation of computerized procedures. It does not address licensing submittals, when they may be required or what they should contain.

1.2 Computerized Procedure Installations

Computerized procedure (CP) systems have been accepted by various regulatory authorities and are in use at several nuclear power plants around the world. Additional CP systems are planned for future installations. Examples include the following:

- COMPRO system installed in the Beznau nuclear power plant in Switzerland and the Temelin nuclear power plant in the Czech Republic (see Portmann [21], NUREG/CR-6634 [12], and NUREG/CR-6749 [13])
- N4 Computerized Procedure System, Electricité de France, installed at the Chooz and Civaux nuclear plants in France (see DaCruz 2006 [1], NUREG/CR-6634 [12])
- Plant safety monitoring and assessment system (PLASMA) installed in Paks VVER-440 units in Hungary (see Eiler 2006 [3])
- Computerized Procedure System planned for the APR 1400 plants, Korea Hydro & Nuclear Power Company, in Korea (see Chung 2002 [24])
- On-Line Procedures System (OLPS) planned for the Advanced Boiling Water Reactor (ABWR) at Lungmen Power Station, Taiwan Power Company, in Taiwan (see Gutierrez 2005 [10], NUREG/CR-6634 [12])

It is expected that additional CP systems will be implemented as operating plants upgrade their instrumentation and control (I&C) systems and modernize their control rooms. CP systems also will be part of the control room designs for new nuclear plants (e.g., see Lipner 2006 [11]).

1.3 Benefits of Computerized Procedure Systems

Varying levels of functionality have been incorporated into different CP systems, addressing to varying degrees some of the limitations found with paper-based procedures (PBPs). Limitations of PBPs include:

- Information presented is static and does not reflect actual plant conditions. Operators must obtain real-time process information needed to execute the procedures by going to various instruments or displays, sometimes at multiple locations.
- Procedure steps are presented in a fixed sequence, which sometimes requires numerous iterations through the procedures.
- Cautions or warnings in PBPs can be confusing if they are not applicable for all system states in which the procedures may be used.

Experience with operating CP systems and the results of research studies show that CP systems can provide a number of performance benefits (NUREG/CR-6634 [12], NUREG/CR-6749 [13], Portmann 2002 [21], O'Hara 2003 [20]).

Some of the positive impacts of CPs on operator performance include the following:

- Tasks can be performed more quickly
- Overall workload can be reduced
- Cognitive workload can be minimized
- Fewer errors may be made in transitioning through or between procedures

In addition, most operators accept CPs readily and find them easy to use. Some of the reasons cited by operators for the positive impact of CPs on performance include:

- CPs ease the burden of selecting appropriate procedures, navigating through the procedures, performing place-keeping, and receiving information at an appropriate level of detail
- CPs aid in performing timekeeping functions (e.g., monitoring parameter-dependent steps for their applicability, and then notifying the operator when actions should be performed).
- CPs can monitor operator actions, helping identify deviations from the expected
- CPs can perform many of the low-level cognitive tasks associated with analyzing and following procedures, e.g., resolving step logic, keeping track of steps of continuous applicability, and assessing cautions and critical safety functions; this allows the operator to focus on higher-level monitoring tasks

1.4 Challenges Associated with Computerized Procedures

In addition to the benefits cited above, various challenges also have been identified with CP systems. These should be addressed in the design and implementation of CPs where they are applicable. Some of the challenges include:

- Transitioning to backup procedures (e.g., PBPs) in the event of CP system malfunction; the potential for human errors in navigation and timekeeping can be increased because operators have become accustomed to the support provided by CPs
- Narrower "field of view" provided by CP systems than with PBPs, reducing the number of steps viewable in parallel, thus making "looking ahead" more difficult
- Failure to recognize problems with the CP system or to take appropriate action due to inattention, which may be caused by other activities requiring attention, or by complacency (because the automated CP system has been in use for a long time and it has always functioned properly)
- Potential negative impact on crew communication and coordination – with some CP systems one person can handle the procedure with little assistance, whereas with PBPs several crewmembers may be involved in executing the procedure; this can reduce crew

communications and crewmember awareness of the status and progress through the procedure

The guidance provided in this report is intended to aid in the design and implementation of computerized procedure systems so as to provide the intended benefits of CPs, while at the same time adequately addressing and mitigating the potential challenges associated with CP implementation.

1.5 Types of Computerized Procedures

Computerized procedures can provide different levels of functionality, including varying levels of automation. Because the guidelines and criteria that are applicable to design and implementation of CPs depend on the types of functionality provided, it is helpful to define categories of CPs based on their functionality.

First, the following terms are used to distinguish between hard copy or paper-based procedures and computerized procedures:

Paper-Based Procedures (PBPs) – procedures provided on conventional hard copy media

Computerized Procedures (CPs) – procedures presented on a computer-driven video display unit (VDU), potentially including additional functionality beyond simply replicating them on a VDU (see below).

Within CPs, three different categories are defined according to the functionality provided. Note that these categories are defined only for the purpose of structuring the guidance in this report and clarifying its applicability – these terms may be used differently in other contexts:

Electronic Procedures (EPs) – CPs that are presented on a computer-driven VDU in text or graphical form that are essentially replicas of PBPs. EP systems may include the ability to call up a relevant procedure from a link on another display, or links between related procedures, but in each case the procedure that is presented is the same as or similar to an equivalent PBP. EP systems may also include links from a procedure to another display page where relevant indications and/or controls are located.

Computer-Based Procedures (CBPs) – CPs that incorporate additional functionality not found in PBPs or EPs, such as:

- Automatic retrieval and display of the specific information needed to perform a procedure step
- Display of relevant indications either directly in the procedure itself or on another display page or section of the display
- Automatic processing of step logic and display of the results

- Automatic checking of prerequisites or preconditions (but leaving the decision up to the operator)
- Tracking of preconditions over multiple steps
- Automatic retrieval and display of a soft control needed to carry out the action(s) called for by a procedure step
- Context-sensitive aids for making branching decisions, and/or
- Cautions or warnings based on current plant conditions.

Note that, as differentiated from EPs, CBPs automate the gathering and display of information relevant to a procedure step. They may also automate the processing of procedure step logic and display results including pass/fail indications. CBPs may suggest and prompt the operator to take actions or execute branches in a procedure. However, they do not by themselves make the decision to act – operators must make those decisions with CBPs.

CBPs with Procedure-Based Automation (PBA) – CBPs that include the ability for the system or machine to automatically carry out multiple procedure steps when directed to by the operator. Once a sequence of automated steps has been authorized/commanded by the operator, the PBA system can make decisions as to whether and when to carry out each succeeding step within the sequence based on plant conditions that are changing in real time. CBPs with PBA can take control actions as part of executing the procedure steps, until a point is reached at which operator input or authorization is required – this is referred to as a "hold point" or "break point." The automated sequence also may be halted prior to reaching a hold point if an error is detected by the PBA system, or at any time the operator decides it is necessary or desirable to interrupt the automated sequence.

It is important to distinguish between PBA and other types of automation. For example, there are sequences of actions in plants today that are initiated and carried out automatically – protective actions such as shutdown of a major pump or other piece of equipment, for example, which occur automatically when preset conditions are sensed by the equipment protective features. Reactor and turbine-generator trips and engineered safeguards actuations are other examples. In contrast, PBA refers to automatic sequences of actions that are started on command by the operator, and for which there are procedures and training that would allow the operator to perform the steps manually if necessary or desired.

Table 1-1 provides examples of the different levels of functionality that may be provided by the different categories of procedures as they are defined here.

Table 1-1
Examples of Functionality Provided by Different Categories of Computerized Procedures

Functionality	PBPs	CPs		
		EPs	CBPs	CBPs with PBA
Medium for presentation of procedure	Paper	Computer-driven displays		
Ability to select and display procedure on computer screen		Yes	Yes	Yes
Navigation links to aid in moving between procedures		Possibly	Yes	Yes
Automatic display of process information relevant to a procedure step			Yes	Yes
Automatic processing of procedure step logic and display of results			Possibly	Yes
Integrated soft controls providing capability to send control commands to equipment			Possibly	Yes
Ability for machine to carry out multiple steps on command from operator				Yes

Table 1-2 illustrates how operator activities in carrying out procedures can be impacted by the different levels of functionality provided with CPs. This is illustrated using the example of a particular emergency operating procedure for a boiling water reactor (BWR). This is a contingency procedure for use of steam cooling as a last resort for situations in which reactor vessel level cannot be maintained. It is important to note that in this type of situation, this would be only one of several procedures being executed simultaneously by the operating crew. The purpose of this example is to illustrate how different levels of CP functionality can impact how an operator carries out the activities prescribed in the procedure, and what assistance is provided by the CP system.

Table 1-2
Example of Changes in Operator Activities with Different Levels of CPs – BWR EPG Contingency #3 Steam Cooling

EOP Step	Actions Taken with PBPs	Actions Taken with CPs		
		EP	CBP	CBP with PBA
Continuously re-check conditions that, if they occur, require entry into alternate procedures, overriding the present procedure (Ex: Level indication is no longer available)	Operator has to continually check/recheck these conditions for possible entry to other procedures	Same as PBP, but possibly with navigation links to move more easily to the alternate procedure when necessary	CBP could continuously monitor and display a prompt when conditions are met indicating the need to follow an alternate procedure	Same as CBP
Determine whether Isolation Condenser (IC) has initiated; if not, manually initiate the IC	Operator must check displays for indication of IC initiation; operator must take manual actions to initiate IC if required	Same as PBP	CBP can automatically display status of the IC system If not initiated, CBP can prompt for initiation Operator action still required to initiate IC, following a sub-tier IC system procedure	Same as CBP, but operator can take a single action to command IC initiation PBA then carries out the steps needed to initiate IC, performing multiple valve operations automatically per the sub-tier procedure

EOP Step	Actions Taken with PBPs	Actions Taken with CPs		
		EP	CBP	CBP with PBA
Stabilize reactor pressure vessel (RPV) pressure using one or more of several systems including: • Isolation Condenser • Safety relief valves (SRVs) but only if suppression pool level is above the SRV discharge • Other systems specified in procedure	Operator required to identify available systems and select one; operator takes manual action to control RPV pressure within prescribed limits	Same as PBP	CBP can automatically determine and display which systems are available based on system and plant status (e.g. it would conclude that SRVs are not available for this purpose if suppression pool level is below SRV discharge) CBP can prompt the operator to select an available system Operator continually monitors pressure and uses the chosen system to maintain it within limits	Same as CBP, but on command from the operator, PBA may automatically monitor and control pressure, e.g., by cycling SRVs as required to keep RPV pressure within limits, relieving operator from having to monitor pressure and cycle valves manually
When RPV water level falls below the "Minimum Zero Injection RPV Water Level," enter the Emergency Blowdown (EB) contingency procedure	Operator monitors RPV water level, and enters EB contingency when level falls below the specified value	Same as PBP, but navigation link may be provided to facilitate transition to EB procedure	CBP can automatically monitor RPV water level and display a prompt for the operator to exit this procedure and enter the EB contingency procedure when the specified level is reached	Same as CBP.

1.6 CP Functionality and Concept of Operations

The level of functionality provided by CPs, and the way that this functionality is employed in the design and by the operating crew, can have an impact on the roles, responsibilities, and interactions of the crewmembers. Of course, the design of the overall control room, arrangement of the operators' workstations, and design of the associated HSIs also play an important role here. However, the focus of this discussion is on implementation of different levels of CPs and their interaction with the crew organization, roles and responsibilities, and overall concept of operations.

Consider the example of emergency operations carried out in accordance with the plant's EOPs. Using PBPs in a conventional control room, a supervisor typically reads the procedure and evaluates the prescribed steps, asking board operators to obtain plant data and to perform specified control actions. Much of the crew is involved in carrying out the procedure. Use of EPs rather than PBPs may not change this situation greatly, because EPs allow only limited additional functionality. The EPs may aid in navigating to procedures or make them available at more locations, but crewmember roles, responsibilities, and communications may be unchanged.

With CBPs, additional changes are likely depending on the level of functionality that the CBPs provide. If the CBPs display the needed process data, the supervisor may not have to ask operators for values, and may be able to perform the procedure independently until a control action is required. The supervisor may inform the rest of the crew of progress through the procedure and when important points have been reached.

When CBPs incorporate soft control capability, individual operators may be able to execute procedures more independently, obtaining data and taking control actions as required, and communicating with other crewmembers only at critical points in the procedure or as needed to exchange information. The supervisor provides oversight of actions taken by operators; assesses progress, strategy, and overall plant state; and/or coordinates the execution of multiple procedures.

With PBA, other role changes may occur. Automatic execution of sequences of procedure steps can free operators to perform other tasks. The automation may perform evaluations and make recommendations to the crew, acting to some degree like an additional crewmember. Operating and training practices should address these changes in order to maintain adequate crew communication and coordination, and to maintain cognizance of plant status by all members of the crew.

The concepts of CP usage described here are only examples. There is no single concept of operations applicable to all plants or plant designs, and reasonable latitude is permitted in this area by current regulatory requirements. Therefore, vendors and utilities should define operating concepts that best suit the goals and strategies of specific plants and plant designs, taking advantage of the capabilities of the CP system to improve overall plant performance. Ultimately, the roles and responsibilities of plant operators for procedure execution should be consistent with the results of the overall HFE program. Regulatory requirements for minimum staffing per

10 CFR 50.44, and regulatory guidance in NUREGs 1122 and 1123 for operator knowledge and abilities [18, 19] should be factored into the HFE process.

1.7 Definitions of Terms

In addition to the terms defined in Section 1.5 related to the different types of computerized procedures, it is important to note the following additional terms and their meanings as used in this report:

- *"Manual" versus automatic* – when this report discusses "manual actions" or performing tasks or actions "manually" this simply means that the human takes the action, not the computer system or machine. As used in this report, an action or decision is performed automatically if the machine does it, and manually if the human does it. A manual action does not have to be accomplished through physical means (e.g., manually turning the handwheel to open a valve) – it can be done from a hard switch or a soft control, "manually" issuing a command through the HSI. Finally, the term "manual" does not specify or refer to the location at which the action is taken (e.g., main control room or out in the plant). It simply means the human does it, regardless of where it is done.

- *"Operator" as the user* – when this report refers generically to the "operator," this can be any member of the operating crew (operator, senior operator, supervisor, or other crewmember) who is using the computerized procedure.

- *"Operator verification"* – this relates to the need, at selected points in a computerized procedure, for the operator to verify information or results that are processed by the CP system, ensuring that the information/results are accurate and appropriate. These operator verifications are performed in real time during execution of the procedure, and thus are separate and distinct from the verifications performed as part of procedure generation to ensure accuracy of the procedure content.

- *"CP system"* – this term is used to refer to the hardware and software system or systems that implement the computerized procedures. Note that this may include data communications and networking associated with gathering and processing data and control commands, as applicable. Also, note that a CP system can host more than one type of computerized procedure (e.g., a CBP for one set of procedures, and CBP with PBA for another). CP system refers to the digital system (hardware and software), not the functionality.

- *"Soft control"* – as used in this report, soft controls refer to controls that are mediated by software rather than hardware (e.g., controls actuated through a computer screen versus a hard control such as a hard switch) and which manipulate plant equipment. An example is a soft control appearing on a computer display that provides the user the capability to open or close a valve, or start or stop a pump.

1.8 Technical Basis for the Guidance

The guidance provided in this report is based on the following sources of information:

- Guidance contained in EPRI 1010042 [4] on computerized procedures and automation – the guidance contained in that report was developed under the direction of an industry working group made up of representatives from plant owners/operators, suppliers, and consultants. The document was peer-reviewed by a cross-section of working group members and other industry experts.
- Guidance contained in EPRI 1011851 [7] on automation for nuclear power plants, and the technical basis for the guidance as described in the report. That report also was peer-reviewed by industry experts.
- An updated literature search and evaluation of previous studies on computerized procedures and automation, conducted as part of developing this report.

The guidance has undergone extensive review by members of an industry task force comprised of representatives from utilities, suppliers, new plant consortia, and consultants.

1.9 Contents of this Report

Section 2 provides general design implementation guidelines for computerized procedures, addressing topics such as HFE design, quality assurance, verification and validation, configuration management, and transitioning to backup procedures.

Section 3 gives additional guidelines for the design of procedure-based automation, and interaction between the operator and the automation.

Section 4 provides guidelines for the design of soft controls, which may be integrated with CPs.

Section 5 provides references cited in this report.

2
GENERAL DESIGN AND IMPLEMENTATION GUIDELINES

This section provides general guidance for the design and implementation of computerized procedures. It addresses human factors engineering (HFE) of CPs, including overall HFE design, operating monitoring and verifications, and transitioning to backup procedures. It also addresses CP system design including quality assurance, verification and validation, procedure maintenance and configuration management.

In this section and those that follow, guidance is provided in the form of numbered guidance statements, shown in a distinctive font, followed where appropriate by additional explanatory information that can help in interpreting and applying the guidance.

2.1 HFE Design

The guidance in this section applies to all three types of computerized procedures (EPs, CBPs, and PBA).

2.1-1 For a new plant, computerized procedures should be designed as an integral part of the overall control room, following accepted human factors engineering (HFE) methods and principles. The level of automation and specific roles and responsibilities assigned to automation and to personnel should be consistent with the plant's overall concept of operations.

NUREG-0711 [15] provides guidance on an acceptable HFE design and evaluation process that is applicable to new plant designs. NUREG-0700 [14] provides HFE review guidelines for CPs, and EPRI 1010042 [4] provides design guidance for CPs. Those documents contain guidelines that are specific to CPs, but they also contain related guidelines that may be applicable to various aspects of CPs such as display design, user interaction and interface management, alarms, automation and soft controls. Section 3 of this document provides additional guidelines on procedure-based automation, and Section 4 provides additional guidelines on soft controls that are integrated with CPs.

2.1-2 When procedures are computerized for an operating plant, the CPs should again be designed using accepted human factors engineering methods and principles. This should include consideration of plant-specific standards and conventions that need to be followed.

The impact of any new automation provided on the roles and responsibilities of the crew should be assessed and addressed in evaluation and training on the CPs.

Operating plants typically have existing engineering procedures and processes that address the HFE activities needed to support modifications impacting the control room. In addition, NUREG-0711 [15] can be used as guidance for determining an appropriate set of HFE design and evaluation activities to support design and implementation of CPs. In addition to new plants, NUREG-0711 also provides guidance for HFE activities related to operating plant modifications.

Operating plants typically have existing HFE design criteria they use to ensure HFE considerations are incorporated into the design of modifications impacting HSIs. In addition, NUREG-0700 [14] provides HFE review guidelines for CPs, and EPRI 1010042 [4] provides design guidance for CPs and other related HSI design guidelines. Section 3 of this document provides additional guidelines for procedure-based automation, and Section 4 provides additional guidelines on soft controls that are integrated with CPs.

2.1-3 A graded approach can be applied to determine the appropriate levels and types of HFE design and evaluation activities that should be performed for CPs, depending on the importance to safety or operations, and/or the uniqueness or degree of change associated with the particular design as compared to previous designs.

Guidance for application of a graded approach to HFE for both new plants and modifications to operating plants is provided in EPRI 1015312 [9].

2.1-4 Computerized procedure systems should continuously indicate the title and version number of the currently displayed procedure(s). Other information on the procedure (e.g., author, plant name, unit, procedure type) should be available on demand.

In order to verify that the correct procedures are being used, the operator must have easy access to this information.

2.1-5 Computerized procedure systems should present procedure information in a structure and format such that the information is readable and usable on the chosen display device(s). If the procedure text cannot all be displayed at once, then continuous up/down scrolling should be implemented. The CP system should avoid left/right scrolling for text. If left/right scrolling is unavoidable, the presence of information to the left or right of the viewable window should be obvious to the user.

2.2 Quality Assurance and Operator Real-Time Verifications

As discussed in Section 1, computerized procedures have the potential to reduce the likelihood of operator errors in carrying out their assigned tasks. However, it is also important to address the

potential for errors that may occur due to failures in the digital system that implements the CPs or in other supporting systems.

CPs are typically implemented using non-safety hardware and software, often using commercial off-the-shelf equipment, and are either part of or are interfaced with the control and information systems the operators use to monitor and control the plant. The guidance provided in this section applies to implementation of CPs on non-safety hardware/software platforms. Note that because these systems are non-safety and thus cannot be credited in the safety analysis, backup procedures are required for accident mitigation and safe shutdown – the need for backup procedures is addressed in Section 2.2.2.

2.2.1 Potential Sources of Errors or Problems in Executing CPs

This section discusses three primary sources of errors or problems that can occur in execution of computerized procedures. These include:

- Problems with quality or integrity of the data or information used in processing the procedure
- Problems with completeness of the data or information used in processing the procedure
- Problems in the processing of the step logic and procedural instructions.

All of these sources of errors are present with PBPs as well as CPs. Therefore, it is important to consider what is unique or different with a CP implementation that may require different or additional measures to protect against errors when using CPs. Because EPs essentially replicate paper-based procedures and present them on a computer screen with little additional functionality, there is little difference in how the types of errors discussed here are addressed with EPs versus PBPs. Therefore, the discussion focuses on the differences in how they are addressed with CBPs (including CBPs with PBA) as opposed to PBPs or EPs.

Table 2-1 summarizes the measures that are typically taken to address each of the three sources of errors when using PBPs (or EPs), and lists measures that can be taken to address them when CBPs (including CBPs with PBA) are used. It is important to note that operator training plays an important role in helping to prevent or detect and correct operator errors, whether using paper-based or computerized procedures. Because it applies to many of the items listed, training is not specifically included in the measures noted in the table.

The last column of the table provides pointers to sections of this report that are relevant to each set of measures.

> Note: The NEI Human Factors Task Force is monitoring the progress and results of an EPRI/NEI effort to collect and evaluate digital system failure experience data. Any lessons learned that are applicable to computerized procedure systems will be reflected in this discussion and the related guidance.

Table 2-1
Measures for Addressing Potential Errors in Executing PBPs and CPs

Sources of Errors/Problems	Measures to Address These with PBPs and EPs	Measures to Address These with CBPs or CBPs with PBA	Reference to Guidance Section
Bad source data (e.g., failed sensor)	Automatic data validation for selected variables	Same situation if the validated data are used by the CP system	Section 2.2.4
	Indication of bad or suspect data quality in displays	Same for information display with a CP system if quality information is available to the CP system	
		Data processing and step processing logic implemented in a CBP should detect data quality problems and act accordingly.	
	Procedure steps may direct the operator to verify or cross-check unvalidated data against other available indications/variables.	Where procedure steps are provided for cross-checking, the situation is the same as for PBP. However, the CBP may provide aids to the operator in doing the cross-checks, for example, by automatically performing and displaying the results of cross-checking.	
Error in selecting or reading the information needed to process step logic (e.g., inadvertently reading the level in SG A rather than SG B)	Supervision and peer checks performed when called for by procedure, or based on normal crew operating practices	These types of operator errors can be virtually eliminated by CP systems that automatically collect the data and process the step logic. CP system error probability is limited through a combination of QA/V&V and operator monitoring and verification; the level of assurance needed depends on the risk significance of the procedure.	Section 2.2.2

Sources of Errors/Problems	Measures to Address These with PBPs and EPs	Measures to Address These with CBPs or CBPs with PBA	Reference to Guidance Section
Drawing the wrong conclusion or making an inappropriate decision in executing a procedure due to *incomplete information or unawareness of mitigating conditions* or circumstances not specifically called out in the procedure	The operator performing the procedure, other crew members or a supervisor may make use of additional information not specifically called out in the procedures, or may be aware of conditions that affect how or whether a procedure step should be carried out. Procedure writers attempt to capture in the procedure the need to check for information that may be important to execution of the procedure; however, not every eventuality can be foreseen and built into the procedure.	CBPs can provide continuous monitoring of applicable conditions, thereby enhancing operators' awareness of conditions not included in the immediate step. In addition, contextual information (e.g., relevant system or equipment information within or in proximity to the procedure display) assists the operator in considering conditions that may be relevant to the current procedure. When PBA is used, hold points can be provided so that the operator will be aware of what step is being executed, can monitor for any conditions that may impact procedure execution, and can interrupt the procedure at any time. In general, freeing the operator from the routine tasks associated with procedure execution can improve the operator's ability to retain the "big picture" and more effectively monitor the plant as the procedure progresses.	Section 2.2.5 Section 3.2
Drawing the wrong conclusion or making an inappropriate decision due to an *error in processing the information or the procedure step logic*	Supervision and peer checks performed when called for by procedure, or based on normal crew operating practices	Human error probability in processing can be significantly reduced by a CP system that automatically gathers the data, processes the step logic and presents the conclusions to the operator. CP system error probability is limited through a combination of QA/V&V and operator monitoring and verification; the level of assurance needed depends on the risk significance of the procedure. For PBA, keeping the operator in the loop, monitoring progress and checking the conclusions of step processing, helps ensure that system errors would be detected. To ensure that the operator maintains adequate cognizance of process status with PBA, hold points should be applied at critical procedure steps.	Section 2.2.5 Section 3.2

Sources of Errors/Problems	Measures to Address These with PBPs and EPs	Measures to Address These with CBPs or CBPs with PBA	Reference to Guidance Section
Selecting the wrong control or taking the wrong action	Supervision and peer checks performed based on normal crew operating practices Crew observes if system responds as expected to the control action	A CBP can automatically check operator actions and provide alerts to deviations from the procedure. A CBP also may support navigation or automatic access to the correct control, or may issue the control signal to the component directly (with operator direction in CBPs, or as a matter of sequence execution in PBA.) Each of these techniques reduces the potential for operator selection errors. CP system error probability is limited through a combination of QA/V&V and operator monitoring and verification; the level of assurance needed depends on the risk significance of the procedure. For PBA, keeping the operator in the loop, monitoring progress and checking the conclusions of step processing, helps ensure that system errors would be detected. Hold points should be applied at critical procedure steps.	Section 2.2.2 Section 3.2

As shown in Table 2-1, two important measures that can be taken to protect against errors in the computerized procedure system causing problems in operation include:

- Quality assurance and V&V activities[1], which help ensure a low probability of errors in the hardware and software of the computerized procedure system
- Operator monitoring and verifications performed in real time during procedure execution, which help detect and mitigate any errors or problems that do occur; for CBPs, this may include cross-checking of information displayed by the CBP and used in step logic processing, as well as verification of the results of any automatic step logic processing; for PBA, operator verifications include the same items as for CBPs plus verification of the correctness of decision-making and automatic actions taken by the PBA system.

In order to provide adequate assurance that operational errors will not occur due to problems in the computerized procedure system, both of these measures are employed in the design, implementation and use of computerized procedure systems.

2.2.2 Safety Classification and Quality Assurance

This section applies to risk-significant procedures, i.e., EOPs and other procedures needed for accident mitigation, safe shutdown, emergency response, severe accident management, or to perform other risk-significant manual actions identified in the PRA.

Note that this section applies different criteria depending on the category (or level of functionality) of the computerized procedure. For EPs, only administrative controls are required because the computer system simply presents a replica of a paper-based procedure, without any live process data, logic processing, or automation. For CBPs, additional criteria apply due to the additional functionality provided and the potential for errors in the system leading to errors in procedure execution. Finally, for PBA, additional criteria apply related to automation and inclusion of hold points in automated sequences.

2.2.2-1 When risk-significant procedures are implemented on a platform (hardware and software) that is not safety-related, and thus cannot be credited under accident conditions, a minimum set of backup procedures should be provided for accomplishing these functions. The backup procedures can be provided as PBPs or as CPs implemented on a safety-related platform.

Criteria for determining the minimum set of backup procedures and the associated design requirements are defined in EPRI 1015089 [8], which addresses the Minimum Inventory of HSIs that should be provided in the main control room. Guidance related to making the transition between CPs and backup procedures is provided in Section 2.4 of this report.

[1] For information on methods for ensuring quality of digital systems used in nuclear plant applications, refer to NUREG-0800 Chapter 7 [16], EPRI TR-102348 Rev. 1 (NEI 01-01) [5], and EPRI TR-106439 [6]. Although these documents focus on safety-related digital systems, the information provided can help guide QA and V&V efforts for non-safety systems such as those discussed here for implementation of computerized procedures.

Note that this guideline is not intended to preclude the option of providing backup procedures on a separate nonsafety platform. However, for risk-significant procedures as define here, there will still be a need for a minimum set of backup procedures to be provided in paper form or on a safety-related platform.

2.2.2-2 For EPs, the computer system should be subject to administrative controls suitable for systems that manage data important to safety.

2.2.2-3 For CBPs, a graded approach can be taken in determining the level of rigor of the QA/V&V activities undertaken to demonstrate adequate quality of the hardware and software of the CBP system. The quality assurance activities should consider all hardware, software and systems involved in processing and presenting the procedures and associated information, including data sources, data communications, and computer systems that process and present the procedures. The level of QA/V&V activities in each case should be determined based on: (1) risk significance of the procedures and potential risk impact of failures in the CBP system, (2) complexity of the hardware-software system, and (3) the operator verifications, cross-checks and confirmations that will be performed during procedure execution that help detect and mitigate effects of CBP system errors or failures.

Note that the complexity and risk associated with failures in a CBP system, which are important factors in determining the level of QA/V&V and operator verifications that may be required, depend in part on the functionality provided by the system, including the level of automation and whether the procedure system provides capability to control plant equipment.

2.2.2-4 For CBPs incorporating PBA, in addition to the guidelines above for CBPs, the guidance given in Section 3 for automation should be applied, including guidelines for incorporating hold points in automated sequences.

2.2.3 Other Digital System Design Requirements

The guidance given in this section applies to CBPs including CBPs with PBA. It does not apply to EPs.

2.2.3-1 If a CP system involves interdivisional data communications (i.e., communications among different safety divisions or between a safety division and a non-safety entity), the applicable guidance on interdivisional communications should be applied.

At the time of this writing, the most recent NRC-issued guidance related to interdivisional communications was contained in Interim Staff Guidance document DI&C-ISG-04 [2].

2.2.3-2 If CBPs have the capability to issue control commands to safety-related equipment, then the hardware-software platform used to implement the procedures should meet the applicable guidance for multi-divisional control and display stations.

At the time of this writing, the most recent NRC-issued guidance related to multi-divisional control and display stations was contained in Interim Staff Guidance document DI&C-ISG-04 [2]

2.2.4 Data Integrity

The guidance given in this section applies to CBPs including CBPs with PBA. It does not apply to EPs.

2.2.4-1 CP systems should use validated data wherever possible for display of process information, step processing, and automation (PBA).

2.2.4-2 When quality status information is available for data displayed by a CP and the quality of a displayed data item is bad or suspect, the quality information should also be displayed.

2.2.4-3 A CBP system 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 PBA, 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.

2.2.4-4 Procedure steps in PBPs that call for operator cross-checking or verification of unvalidated data should be carried over to CPs. If the CP system has access to data the operator needs for cross-checking, consider providing automatic cross-checks. These cross-checks or verifications should at a minimum duplicate what the operator would be expected to do, and the system should make available to the operator (automatically or on demand) the data/readings used in the verification.

2.2.5 Monitoring and Verification by Operating Crew

The guidance given in this section applies to CBPs including CBPs with PBA. It does not apply to EPs.

As discussed in Section 2.2.1, operator monitoring and verification of information used by CPs, results obtained by any automatic processing of information, and any decisions made or suggested by CP systems, is an important part of protecting against errors. This section provides guidance on building appropriate checks and verifications into CPs, and supporting and training the operating crew in monitoring and verifying CP results and actions.

2.2.5-1 The CP system should not determine what procedure will be used by the operating crew. The crew should decide what procedure will be used in any given situation. The CP system may recommend or prompt the operator to use a particular procedure, but the operator should be able to override this.

The operating crew may be aware of mitigating conditions or circumstances that the CP system logic is not aware of. The crew should always be able to decide for themselves what procedure should be used.

2.2.5-2 The HSI should continuously indicate the state of the CP system and the status of the active procedure(s).

In order to monitor progress through the procedures, the operator must have easy access to this information. The HSI that displays the information may be part of, or separate from, the CP system itself.

Also see the guideline in Section 2.1 that calls for continuous indication of the procedure title and version number.

2.2.5-3 The content of a CP should capture the relevant information needed to support procedure step processing and decision-making. This may include information that was not explicit or well-defined in equivalent PBPs. When preparing procedure contents for use in CPs, procedure writers should identify any implicit information that the operators use as part of their normal practice and determine how to incorporate it into the CPs explicitly (for example, as a note, as a manual step, or as a computer-evaluated step). This will depend on the level of automatic processing that is performed in the CP. Operations and training staff should be encouraged to continue refining CP contents (conditions, logic, criteria, notes, cautions, etc.) as the procedures are used in service to help ensure that relevant conditions are explicitly called out in the procedures.

It is more important with CPs than with PBPs that the procedure content captures the relevant information that may be needed to properly execute the procedures, because the computer will only process the information it has been programmed to utilize and operators may tend to rely on the CP and be less likely to check for other relevant information when using the CP.

2.2.5-4 When PBPs are converted to CPs in an operating plant, or when content is generated for CPs in a new plant, peer checks that are built into PBPs should be carried over to the CPs, to the extent appropriate for the new roles and responsibilities of crewmembers. Operator training should emphasize the need for the crew to continue performing appropriate supervision and peer checking of operator actions when using the CPs.

Although CPs can reduce the incidence of certain types of operator errors, operating crews should not become complacent when using CPs. They should continue to perform appropriate

peer checks and supervision of operator actions, consistent with their roles and responsibilities while using CPs, to help guard against operator errors.

2.2.5-5 Procedure step logic that is processed by a CP should be as precise and objective as practical so that the CP can correctly evaluate the logic according to the intent of the procedure. When subjectivity is involved in correctly evaluating the logic, operator verification may be needed.

Subjective or qualitative evaluations may be encountered in procedure steps that are difficult to implement as computerized logic. For example, when implementing a step that begins with "If pressure is decreasing…" it may not be sufficient to simply check the sign of the change in pressure at a single instant of time. The intent of the procedure step may be to ensure that pressure is consistently trending lower by an amount that is operationally significant before proceeding. A simplistic implementation might result in the CP interpreting a small, momentary fluctuation as satisfying the criterion, potentially misleading the operator, particularly if the operator does not independently confirm the CP result. To the extent practical, ambiguity and subjectivity should be eliminated in the CP implementation of the logic. If significant subjectivity remains for a particular step, that step may be a good candidate either for manual evaluation or to prompt the operator to verify the CP result.

2.2.5-6 Operator training on use of CPs should emphasize the importance of employing a questioning attitude, and should reinforce the need to monitor the processing performed by CPs and to override the CP system if required.

For various reasons, including the inherent reliability of high-quality CP systems, operators may be less inclined to take issue with CP guidance than with PBP guidance. It is important that training reinforce the need for operators to monitor, question, and verify or override CP results and actions.

2.2.5-7 The CP system should assist the operator in understanding the logical processing that it performs and in verifying the results (e.g., by making available information on the details of the processing and any intermediate as well as final results).

To the extent that CP processing of information and step logic relieves the operator of having to process the details, the operator may miss potentially meaningful details and thus may be less cognizant of a developing situation. Additional guidelines on design of procedure-based automation and operator interaction with the automation are provided in Section 3 of this report.

2.2.5-8 A CP system may automatically process procedure step logic, evaluate prerequisites and permissives, process decision logic at branch points, and provide recommendations to the operator regarding how to proceed. However, the operator should have the ability to decline to follow the automation's recommendation. The automated system may provide cautions or warnings when an operator deviates from a procedure, as an aid to help detect

and recover from a potential error. However, the operator is always the final authority. Deviations from procedures should be logged for historical purposes.

Automation should assist the operator in safely and effectively completing a procedure, but should not take away the operator's decision-making authority. Logging of deviations can provide information to help identify potential improvements to procedures or training. See Section 3 for additional guidelines on design of procedure-based automation and operator interaction with the automation.

2.2.5-9 Training should address the potentially different roles for individual crewmembers when using CPs versus PBPs, including the role of the supervisor, and also should address the potential impact on crew communication and coordination.

Implementation of CPs may impact the roles of individual crewmembers and the communications among the crew, thus affecting the ability of other crewmembers and the supervisor to remain aware of procedure progress and status. Transition to backup paper-based procedures may also have implications for crewmember roles. This should be addressed in crew training.

2.3 Computerized Procedure Maintenance and Configuration Management

This section provides guidelines related to maintaining computerized procedures and configuration management associated with CPs. It is not intended to address details related to maintenance of the procedure contents, which are already covered by current regulatory guidance. The guidance provided here is focused primarily on the computerized aspect of the procedures, including automation.

The guidance in this section applies to all three types of computerized procedures (EPs, CBPs, and PBA) except where otherwise noted.

2.3-1 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.

2.3-2 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 CP system always presents the most recent approved and issued version of each procedure.

2.3-3 To facilitate ease of procedure maintenance and system configuration management, the software architecture and data structures of the CP system should be designed such that separation is maintained between: (1) data that represent procedure contents (step

logic, text of procedure steps, cautions and warnings, etc.), and (2) the CP application software.

This is relatively straightforward for EPs, which display replicas of paper-based procedures on the computer screen with little additional functionality. It becomes more challenging for CBPs and PBA, where live process data may be integrated into the procedure display along with automatic processing of procedure step logic. Maintaining separation between the procedure content and the application software allows the configuration control processes to distinguish between changes to procedural instructions and aids, which can be managed in a manner similar to how PBPs are managed, and changes that represent design modifications and thus should be controlled by the plant's engineering change control process.

2.3-4 Means should be provided to ensure adequate verification and validation of changes made to CBPs and PBA. The CP system may provide tools that assist with verification and validation.

For example, manual changes to CBPs might be limited to plant ID tags for instruments and components. Engineering tools could automatically link these tags to computer tags for displays and controls within the software. This type of engineering automation can minimize the manual V&V activities needed for changes to CBPs.

2.3-5 The configuration management program should ensure that consistency is maintained between CPs and any backup procedures expected to be used upon failure of the CP system.

The CP system may provide tools for maintaining consistency between CPs and associated backup procedures – for example, a tool that automatically generates new PBPs as backup procedures whenever the CPs are modified or a tool that automatically generates CPs whenever the PBPs are modified. Similarly, a tool might be provided to automatically generate procedure content for a backup procedure implemented on an alternative platform whenever the content is changed in the normally-used CP system, or vice versa.

2.4 Transitioning Between CPs and Backup Procedures

The guidance in this section applies to all three types of computerized procedures (EPs, CBPs, and PBA) except where otherwise noted.

2.4-1 Backup procedures should be readily accessible to the users of the CP system, such that users can make the transition from CPs to backup procedures in a timely manner.

2.4-2 Backup procedures should be presented in a manner that is compatible with the presentation of the same procedure on the CP 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.

Backup procedures may be implemented in paper form, or on an alternative platform that does not have the same range of capabilities as the CP system normally used. It may not be practical or desirable to have identical presentations on both media, given the significant difference in functionality between the normally-used CP system and the backup implementation that is either on paper, which has essentially no functionality, or on an alternative computer implementation, which may have reduced functionality. However, it is important that the two presentations be sufficiently compatible that operators do not become confused when switching to or from the backup upon failure or restoration of the normally-used CP.

2.4-3 Potential failure modes and degraded conditions of the CP system should be identified, and CP users should be trained to recognize when such conditions exist so that transition to the backup procedures can be performed in a timely manner.

2.4-4 For CBPs or PBA, 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 whether that step was fully or only partially completed, and (3) what conditions or steps, if any, were being continuously monitored by the CP system at the time of failure.

This information is required for the operator to be able to make an orderly transition from the failed CP to the backup procedure. For example, the CP system might automatically store a status summary or snapshot on a regular basis in a form that would remain available after CP system failure, so that if the system fails the operator can retrieve the latest status information and use it to support making a safe and effective transition to the backup.

2.4-5 Upon transition to a backup procedure from a CBP or PBA, the operator should be able to continue the procedure at a point that is as close as possible to where the CP was at the time of failure. This will avoid having to re-evaluate or repeat previously-executed steps unnecessarily, and avoid risk associated with moving back to an earlier point in the procedure, which could create an undesirable or unsafe situation.

Ideally, the operator would continue the procedure at precisely the point at which the CP system failed. However, the safest and most effective resumption point may be different depending on the operations underway at that time. Starting over at the beginning may appear to be the simplest approach, but it may not be the most productive one. It also may not be a safe approach, as it risks performing steps in an order not intended by the procedure designers (the state of the plant or the configuration of equipment may be different after partial completion of the procedure, and as a result performing an early step again could cause undesired results). In addition, starting over may cause significant delay in completing safety actions and thus potential

for deteriorating and possibly unsafe plant conditions. The operating crew may need to determine at the time of failure the best point at which to resume the procedure.

2.4-6 The time required for the operator to effectively transition from the CP 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.

2.4-7 After transitioning to a backup procedure from a failed or degraded CBP or PBA, the operator should be able to stop the processing of the computerized procedure or mute its outputs in order to avoid spurious alarms or prompts that could be distractions.

3
ADDITIONAL GUIDELINES FOR PROCEDURE-BASED AUTOMATION

Section 2 provides guidance that is applicable to any computerized procedure system. This section provides additional guidelines specifically for procedure-based automation (PBA).

First, general guidelines are provided here based on basic principles that are applicable to the design of any automated system or process and which should be applied to PBA. Then guidelines specific to PBA are provided.

The guidance in this section refers to human-system interfaces (HSIs) used for personnel interaction with procedure-based automation. These may be the HSIs that are part of the CP system itself, or other control room HSIs that personnel use while working with the CP system.

Guidance is provided in the following areas:

- General automated system design guidelines applicable to procedure-based automation
- Guidelines to support operator monitoring and interaction with procedure-based automation specifically
- Operator training for interactions with procedure-based automation

3.1 General Design Guidelines

This section contains general guidelines for the design of integrated human-automation systems. They reflect basic principles of automation that should guide the design. Subsequent sections provide more detailed guidance for applying these principles to the design and implementation of procedure-based automation.

3.1-1 Personnel should be in command of automatic systems.

Personnel are ultimately responsible for the safe operation of the plant and thus they should be in command of automated processes and systems. Accordingly, automation and its HSIs should be designed to permit personnel involvement with the automation.

Note that being in command does not necessarily mean that personnel will be able to intervene and override all automatic processes. One of the reasons to automate some processes is that the task requirements exceed human capabilities. For example, there are situations, e.g., reactor scram, in which a response to a signal must occur so quickly that the time required for an

operator to take the necessary action would be too long. In such cases, where direct human intervention in the automatic process is not feasible, personnel should be able to monitor the performance of the automation as part of their supervisory role. On the other hand, for procedure-based automation, where pre-defined sequences of procedure steps are carried out on command by the operator, the operator should be able to intervene and take over from the automation when necessary.

3.1-2 Automated processes should be well understood by personnel who monitor and interact with the automation.

The automation, the interaction between automation and personnel, and associated procedures and training should be designed such that communications between automation and personnel, and the automation itself, are well understood by personnel.

3.1-3 Interfaces to automation should be designed to minimize the effort required to interact with the automation.

The secondary task interactions through which personnel monitor and direct the automation should be as simple as possible and not unnecessarily burdensome, such that they can be carried out along with ongoing primary (i.e., operational) tasks for which personnel are responsible.

3.1-4 Personnel interaction with automation should be supported by associated procedures and training.

In the case of procedure-based automation, the automation and personnel are both working to the same procedure. Backup procedures may be provided for situations in which the computerized procedure fails. For other forms of automation, separate procedures may be needed to support personnel interaction including taking over upon failure of the automation. In any case, training should address interaction with automation and dealing with situations in which the automation is failed or degraded.

3.2 Guidelines to Support Operator Monitoring and Interaction with Procedure-Based Automation

3.2-1 The HSI should support operator awareness of the goal or purpose of the procedure-based automation.

It is important that personnel be aware of the goal or objective that the automation is intended to accomplish. This understanding will support personnel in deciding whether to authorize or direct the automation to begin, and support their assessment of the effectiveness of the automation once it has begun. If the purpose of the automation is to execute a pre-defined block of procedure steps, the goal may simply be to complete the actions according to the acceptance criteria for each step. The system should make clear what specific steps will be performed and at what point

the automated sequence will be completed. However, the automation may have important higher-level goals, such as starting a system and verifying its correct operation, or warming a system to a certain temperature. It is important for the automation to make the operator aware of these goals to support the operator's decision on whether and when to begin the automation, and to support monitoring its effectiveness once the automation has begun.

3.2-2 The CP system should provide information on initial conditions that must be met before an automated sequence should begin.

The CP system may evaluate the prerequisites or initial conditions that must be met before proceeding with a block of steps/actions, and provide a prompt to the operator asking for acknowledgment and authorization that the automation can proceed. The system also should make available, either automatically or on demand, the specific prerequisites and initial conditions that were evaluated so that they can be independently verified by the operator if desired. If the system does not have access to data needed to evaluate a prerequisite or initial condition, the system should prompt the operator to evaluate this information.

3.2-3 The operator should be able to choose whether to execute a block of steps automatically or manually.

The operator should always be in command, and thus should be able to decide whether to use the automation or to execute the procedure steps manually.

3.2-4 The HSI should provide information to enable personnel to determine the current status of automated processes and to evaluate progress toward achieving the goal of the automation. For an automated sequence of actions, the HSI should indicate the specific sequence of steps that the automation will follow and the current status of steps (within an active or immediately pending block of steps), including the point at which a hold point will be reached or the sequence will be completed.

Information on the current state of the processes or actions that are automated will enable personnel to determine if the automation is performing as designed or manual intervention is required. The way in which the displays present information should support the timely assessment of automation's progress. For example, if the automation is changing a measured value over time, then displaying progress using a trend graph that shows both the current trend and the goal state or objective will facilitate personnel assessment of progress toward reaching the goal. If the automation is executing a sequence of actions, displaying the sequence and the current status will facilitate operator awareness of progress through the sequence. If the goal of the current block of automated steps is to start or line up a plant system, the display might show system status so that personnel can easily monitor progress toward the goal and know when the goal has been reached.

3.2-5 For EOPs with procedure-based automation, the HSI should indicate when multiple steps are being performed concurrently and their status. Continuously applicable steps or

preconditions being monitored across multiple steps should also be indicated. When parallel paths are being followed concurrently (e.g., two legs of an EOP flowchart) the HSI should display the progress and current status for each concurrent path. Similarly, when multiple procedures are being executed simultaneously, the HSI should display the progress and status of each procedure.

This information is needed in order for the operator to be able to monitor and supervise the automation when the system is performing multiple tasks simultaneously.

3.2-6 Pre-defined "break points" or "hold points" should be provided where procedure-based automation stops and waits for the operator to authorize continued progress through the procedure. Hold points should be established as necessary to allow operators to effectively monitor the automation's progress, to maintain adequate awareness of the status of the procedure and affected plant systems, and to confirm or evaluate decisions at critical points in the procedure.

For example, hold points should be provided where:

- Upcoming decisions or actions could involve a risk to plant safety, personnel safety or investment protection, and operator involvement in deciding whether to move forward would be expected to significantly reduce the risk
- A manual operator input, action, decision or verification is needed (e.g., where the system or machine does not have access to the needed information or control)
- The step involves a subjective evaluation that necessitates operating crew involvement (e.g., when a step begins with "If pressure is decreasing…" an operator may need to evaluate the trend and determine whether the pressure is consistently trending lower by an amount that is operationally significant, as opposed to a momentary fluctuation that does not satisfy the intent of the procedure step)
- The step requires a peer check or authorization from another crewmember (note that some of the current procedures used at operating plants already have peer checks built in – these may be candidates for hold points if the procedures are converted to PBA)
- Actions taken at the next step could impact compliance with operating limits (e.g., the plant Technical Specifications)
- A hold is needed in order to reinforce operator cognizance of procedure and process status (i.e., the automation has reached a point where the operator should assess the situation, such as transition points between process modes or phases of operation)

Hold points should be used where needed, but they should not be over-used. If too many hold points are inserted such that they occur very frequently and are not meaningful to the operator, the operator may over time become conditioned to simply authorizing continued progress at each point without much thought, thus defeating the purpose of hold points.

Hold points may define blocks of steps in a procedure with PBA. However, the blocks and associated hold points should be defined on a functional or operational basis and should be meaningful to the operator. They typically should not be based solely on having completed an arbitrary number of steps in the procedure.

Note that the hold points discussed here are pre-defined and written into the PBA procedure. As discussed in other guidelines in this section, the operators should also be able to interrupt an automated sequence at any time, prior to reaching a pre-defined hold point. In addition, the automated system should halt the PBA sequence when a condition is detected by the system, in real time, that indicates a problem with the automation or other condition that requires operator attention or involvement. Thus, there are at least three ways in which an automated sequence may be halted:

1. The automation has reached a hold point – these are pre-defined points in the procedure where the system will stop, every time, and wait for operator input or authorization. In most cases, these points would be fixed – the automation will stop at precisely the same point in the procedure every time. However, in some cases a hold point might depend on real-time plant conditions – for example, a hold that occurs when a certain plant condition has been reached during execution of the procedure. In those cases the hold point might be referred to as a "calculated" hold point – the logic for the hold point is still pre-defined, but the time at which it occurs may not be fixed.
2. The operator interrupts the sequence – this may occur at any point in the sequence, as determined by the operator at the time.
3. The system halts the sequence due to an error condition or other problem detected by the system and alarmed to the operator – this may occur at any time depending on when the error is detected. Note that this is different from a "calculated" hold point, which monitors for certain expected conditions as opposed to unexpected errors or alarm conditions.

3.2-7 The system should provide a means for the operator to interrupt an automatic sequence at any point. In response to an interrupt command by the operator, the automation should be designed to provide a safe and effective transition from automatic to manual execution of the procedure steps. This may require that the automation complete part or all of a step before turning over control to the operator. The system should provide information that allows the operator to determine where in the sequence of steps or actions the automation has stopped, what has been completed, and what the next steps should be.

In order for the operator to be in command of the automation, control the pace of procedure execution, and effectively supervise the automation, the operator must be able to interrupt the automation at any time. However, it is important to ensure that this transition from automatic to manual execution does not create problems in carrying out the procedure steps. For example, if the automation has just taken an action that must be followed by a subsequent action within a short period of time to avoid an undesired result (e.g., damaging equipment), the automation may need to complete the second action before stopping the sequence and turning over control to the operator.

3.2-8 After interrupting an automated sequence, the operator should be able to resume automatic execution if desired.

The operator should be able to interrupt an automated sequence without having to necessarily complete the remainder of the steps manually. For example, an operator may simply want to stop the process momentarily to provide time to verify correctness or appropriateness of the automated actions or to check other conditions that could impact further progress. If the operator concludes the automation can continue, it should be possible (as limited by process constraints) to restart it from the point where it stopped.

3.2-9 The HSI should provide applicable cautions, warnings, notes and alarms related to execution of the procedure. These should alert the operator when a condition is encountered that may prevent the automation from accomplishing its goal, including halts, failures or errors in execution. These should be presented in a manner such that they are easily recognized by personnel.

Feedback in the form of cautions, warnings, notes and alarms related to automation performance should be presented in a manner such that they are easily distinguished from each other and from other display elements. Alarms should be provided to indicate any failures or errors that require operator action.

Section 2.4 provides additional guidance related to CP failures and transitioning to backup procedures.

3.2-10 The HSI should support the operator in determining the cause of an automatic halt or an execution failure.

Personnel should be able to readily determine the cause of a halt or PBA execution failure, including whether the problem has occurred in the PBA system and/or there is a problem with plant equipment, processes, or instrumentation that is impacting the ability of the automation to function.

3.2-11 The HSI should conspicuously indicate the current operating mode of the procedure-based automation, including any automated background tasks or sub-tasks of the main procedure execution. Also, the system should alert the operator if a mode change occurs automatically. The number of modes of operation should be limited to help minimize potential for mode errors.

Procedure-based automation may be in different operating modes or states – for example:

- In automatic mode, executing a block of procedure steps
- In manual mode, expecting the operator to execute each step in sequence
- On hold, waiting for operator input or authorization before proceeding (e.g., at a hold point)

- In an alarm state, with the sequence interrupted due to a failure or abnormal condition detected by the system

In addition, there may be automated tasks that run in the background, such as monitoring of continuously applicable steps or pre-conditions that apply across multiple steps. The operator needs to know whether these tasks are continuing or if they have stopped.

Conspicuous indication of the current mode of operation, and alerting the operator to any automatic mode change, will help prevent personnel from making mode errors, i.e., taking an inappropriate action or failing to take a needed action due to thinking the system is in one mode when it is really in another mode. Keeping the number of operating modes to a minimum also helps minimize the potential for mode errors.

3.3 Operator Training for Interactions with Procedure-Based Automation

This section addresses training of personnel on interactions with procedure-based automation. See Section 2.2.5 for additional guidelines on training related to computerized procedures.

3.3-1 Training should reinforce the role of personnel as the supervisors and managers of PBA.

3.3-2 Training should provide the operators with a thorough understanding of the procedure-based automation, the goals of each procedure, what information is processed and how, what actions it will take, and when it will terminate. How the operator should use the automation, and the conditions under which it should and should not be used should also be included in training.

Personnel must have a good understanding of automation in order to properly manage it. The automation should be predictable and understandable. Lack of understanding of the automation increases the chance that personnel will be surprised by the behavior of the automation, or may provide inappropriate input to the automation.

Training also will enhance confidence in the automation. Personnel will not use automation if they lack confidence in it. Training should also address issues regarding over-reliance on automation. For example, personnel may overvalue the data provided by the automation and become lax in independently confirming the information; again, training can help personnel to recognize the potential for and guard against over-reliance.

3.3-3 Training should ensure that manual skills and proficiency are maintained so that personnel can effectively carry out procedure steps manually when needed.

When personnel routinely use procedure-based automation, over time they may lose their skills and familiarity with manual execution of the procedures. Training can help overcome this by maintaining proficiency in manual procedure execution and the associated skills.

4
SOFT CONTROLS DESIGN GUIDELINES

Soft controls in general, including those integrated with computerized procedures, should be designed and evaluated using accepted HFE methods and principles. This is addressed in Section 4.1. Additional design guidelines for soft controls integrated with CPs are provided in Section 4.2.

4.1 General Guidelines for Soft Controls

NUREG-0700 [14] provides design review guidelines for soft controls. Those guidelines are applicable to soft controls in general, including controls that may be provided as part of a CP system.

EPRI 1010042 [4] provides design guidelines for soft controls, including guidance on selecting soft versus hard controls. Again, that guidance is applicable in general to soft controls, including those that may be integrated with CPs.

4.2 Additional Guidelines for Soft Controls Integrated with CPs

4.2-1 When computerized procedures provide the capability to access soft controls to manipulate plant equipment directly from the procedure, the operator should be provided with or have ready access to the information needed to support effective use of the control, such as the current plant and equipment status.

Soft controls are most often accessed from process or system graphical displays or other displays that provide information on the system and specific equipment that will be manipulated. This helps provide context for the operator when using the control. Similarly, when soft controls are accessed through a CP it is important to ensure that the operator has the information needed to use the control effectively. Such information may be provided directly by the CP system, or through links that allow the operator to readily access and display the needed information while using the control.

4.2-2 The control of plant equipment by an operator using soft controls should require at least two discrete actions.

This helps prevent inadvertent actuation of a control. The discrete actions may include selecting the control, and then executing the desired control action.

5
REFERENCES

[Note: Full citations for all references will be provided later.]

1. DaCruz, Paul. "A Practical Appreciation of the Implementation of a Fully Computerized Monitoring and Control system in N4 NPP Series: An Advanced Instrumentation and Control System." NPIC&HMIT 2006, Albuquerque, NM, November 12-16, 2006, pp. 217-226.
2. DI&C-ISG-04. "Digital Instrumentation and Controls Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues (HICRc)," Interim Staff Guidance DI&C-ISG-04 Rev. 0 (Initial Issue for Use), U.S. Nuclear Regulatory Commission, September 28, 2007.
3. Eiler, Janos. "Computerized Emergency Operating Procedures at the Paks NPP, Hungary." NPIC&HMIT 2006, Albuquerque, NM, November 12-16, 2006, pp. 1185-1190.
4. EPRI 1010042, "Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance", December 2005.
5. EPRI TR-102348 Rev. 1 (NEI 01-01), "Guideline on Licensing Digital Upgrades," March 2002.
6. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996.
7. EPRI 1011851, "Development of Guidance for the Proper Design and Use of Automation in Nuclear Power Plants." December 2005.
8. EPRI 1015089, Minimum Inventory HSIs
9. EPRI 1015312, Graded Approach to HFE
10. Gutierrez, R., Zizzo, D., and Yu, K. "Human factors verification and validation of the advanced nuclear plant control room design." *Proceedings of Global 2005, Tsukuba, Japan, October 9-1`3, 2005, paper no. 392.*
11. Lipner, M. H., Mundy, R. A., and Franusich, M. D. "Dynamic Computer Based Procedures System for the AP1000 Plant." NPIC&HMIT 2006, Albuquerque, NM, November 12-16, 2006, pp. 692-694.
12. NUREG/CR-6634. O'Hara, J., Higgins, J., Stubler, W., and Kramer, J., "Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance" (NUREG/CR-6634). Washington, D.C.: U.S. Nuclear Regulatory Commission, 2000.

13. NUREG/CR-6749. Roth, E. & O'Hara, J., “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 (2002).
14. NUREG-0700
15. NUREG-0711
16. NUREG-0800, Standard Review Plan
17. NUREG-0899
18. NUREG-1122
19. NUREG-1123
20. O’Hara, J., Pirus, D., Nilsen, S., Biso, R., Hulsund, J.-E., Zhang, W."Computerisation of Procedures Lessons Learned and Future Perspectives." OECD HALDEN REACTOR PROJECT. HPR-355. July 17, 2003.
21. Portmann, F., and Lipner, M. H. "An Operational Model for Using a Computerized Emergency Operating Procedures System." *Modern Power Systems,* April 2002.
22. Regulatory Guide 1.206, Section 3.I 18.8, Procedure Development, 2007.
23. Regulatory Guide 1.33
24. Chung, Yun H., Choi, Sung N., and Kim, Bok R. "Preliminary Evaluation of Computerized Procedure From Safety Viewpoints." In CNRA/CSNI Proceedings of Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, September 25-27, 2001, Hluboka nad Vltavou, Czech Republic. NEA/CSNI/R(2002)1/VOL.2, JT00127981, June 11, 2002.