Guidelines for the design and implementation of computerized procedures

BY ROBERT T. FINK, CHARLES D. KILLIAN, LEWIS F. HANES, AND JOSEPH A. NASER

The increased use of computerized procedures in nuclear power plant control rooms is driving the need to provide guidance regarding their use.

COMPUTERIZED PROCEDURES (CP) are drawing increased interest for use in nuclear power plants as a means of enhancing operator performance and of taking advantage of the more extensive digital instrumentation and controls (I&C) technology that is being incorporated into control rooms. CP systems have been accepted by a number of regulatory authorities and are in use at several nuclear power plants around the world, and more are planned for future installations. Current and planned installations include the COMPRO system, at the Beznau nuclear plant in Switzerland and the Temelin nuclear power plant in the Czech Republic;[1,2,3] the N4 Computerized Procedure System, at Electricité de France's Chooz and Civaux nuclear plants in France;[2,4] the plant safety monitoring and assessment system (PLASMA), at the Paks VVER-440 units in Hungary;[5] the Computerized Procedure System, planned for Korea Hydro & Nuclear Power Company's APR 1400 plants in Korea;[6] and the On-Line Procedures System, planned for Taiwan Power Company's Advanced Boiling Water Reactor at the Lungmen Power Station in Taiwan.[2,7]

The implementation of more CP systems is expected as operating plants upgrade their I&C systems and modernize their control rooms. The modernization of I&C systems typically results in information and control architectures that enable the implementation of CPs with higher levels of functionality than have been possible in the past. CP systems also will be part of the control room designs for new nuclear plants.[8]

Although the implementation of CPs and the level of functionality they provide are increasing, the availability of guidance to help designers and regulators determine the acceptability of various CP systems has, unfortunately, not kept pace. NUREG-0700, Revision 2,[9] provides human factors review guidelines for CP systems, but these guidelines and their technical bases were developed years ago and do not address the higher levels of automation being incorporated into modern CP systems. Also, the NUREG-0700 guidelines are directed toward a detailed human factors review of CP systems and do not address design and quality assurance issues associated with them.

The lack of updated guidance that addresses current CP system design and licensing issues leads to uncertainty for designers and plant owners regarding whether various design features and capabilities under consideration for CP systems will be acceptable to regulators. Also, particularly for higher-level systems that incorporate greater levels of automation, designers and potential users of CP systems do not have adequate guidelines or criteria to judge the acceptability of new system designs.

In order to fill this gap, the Electric Power Research Institute (EPRI) has been working with the Nuclear Energy Institute (NEI) and the Nuclear Regulatory Commission to develop guidelines and criteria for CP systems. This is part of an overall industry-NRC initiative designed to address a number of issues related to digital I&C systems and highly integrated control rooms for new and existing plants. The NEI Human Factors Task Force identified CPs as one issue to be addressed, and EPRI took the lead in the development of consensus guidelines for use by the industry and the NRC in designing and evaluating CP systems for both new and operating plants. The EPRI guidelines are contained in EPRI 1015313,[10] which will be published later this year.

Computerized vs. conventional procedures

Varying levels of functionality have been incorporated into CP systems in order to address some of the limitations found with conventional paper-based procedures (PBP). Those limitations include the following:

- The information presented is static and does not reflect actual plant conditions.
- Procedure steps are presented in a fixed sequence, which sometimes requires numerous iterations throughout the procedures.
- Place-keeping within a procedure must be done manually, resulting in an administrative burden.

Continued

Robert T. Fink (<rfink@cdfservices.com>) is Vice President of CDF Services, Inc.; Charles D. Killian (<ckillian@cdfservices.com>) is a consultant for CDF Services; Lewis F. Hanes (<lhanes@columbus.rr.com>) is an independent consultant; and Joseph A. Naser (<jnaser@epri.com>) is a Technical Executive for the Electric Power Research Institute.

The authors wish to acknowledge the members of the Nuclear Energy Institute's Human Factors Task Force, who contributed significantly to the development and refinement of the EPRI guidelines described here. Also gratefully acknowledged are members of the Nuclear Regulatory Commission's Highly Integrated Control Room–Human Factors Task Working Group, who participated in discussions with the NEI Task Force and reviewed and commented on the draft of EPRI 1015313.[10]

■ Cautions or warnings can be confusing if they are not applicable to all system states in which the procedures may be used.
■ Updating all copies of procedures when changes are required and maintaining configuration control can be challenging.

Experience with operating CP systems and the results of research studies show that CP systems can provide a number of performance benefits.[1,2,3,11] Among the positive impacts of CPs on operator performance are the ability to perform tasks more quickly; reduction of overall workload; minimization of cognitive workload; and reduction of errors in transitioning through or between procedures.

In addition, most operators accept CPs readily, finding them easy to use and recognizing their positive impact on performance. Operators have said that CPs help ease the burden of selecting appropriate procedures, navigating through the procedures, performing place-keeping, and receiving information at an appropriate level of detail. Also, CPs aid in performing timekeeping functions (for example, monitoring parameter-dependent steps for their applicability, and providing notification to the operator as to when actions should be performed); monitor operator actions, helping to identify deviations from the expected; and perform many of the low-level cognitive tasks associated with gathering data and following procedures, such as resolving step logic, keeping track of steps of continuous applicability, and assessing cautions and critical safety functions, thereby allowing the operator to focus on higher-level monitoring tasks.

Experience with operating CP systems and the results of research studies show that CP systems can provide a number of performance benefits.

Challenges associated with CP use

Along with the benefits of CPs cited above, various challenges have also been identified with their use. Where applicable, these challenges should be addressed in the design and implementation of CP systems. Among the challenges are transitioning to backup procedures (for example, PBPs) in the event of CP system malfunction; the narrower "field of view" provided by CP systems than with PBPs, which reduces the number of steps viewable in parallel and makes "looking ahead" more difficult; and 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 brought on by the system's use and proper functioning over an extended period of time. In addition, the use of CP systems can have a potential negative impact on crew communications and coordination. For example, with some CP systems, one person can handle a procedure with little assistance, thereby reducing communications and awareness among crew members of the status and progress through the procedure. With PBPs, however, several crew members might be involved in executing the procedure, making communication an important part of the process.

In general, the level of functionality provided by CPs and the way this functionality is employed in the design and by the operating crew can have an impact on the roles, responsibilities, and interactions of the crew members (examples of this are provided in EPRI 1015313). This should be considered in human factors engineering (HFE) evaluations and the development of the control room design (new or modified) to ensure consistency with the plant's overall concept of operations.

The guidance in EPRI 1015313 is intended to aid in the design and implementation of CP systems in order to take advantage of their intended benefits, while at the same time to adequately address and mitigate the potential challenges associated with CP implementation.

Types of CP systems

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

Before the different types of CPs are discussed, it is necessary to clarify what is meant by computerized and conventional (paper-based) procedures. EPRI 1015313 distinguishes between the two as follows:

Paper-based procedures—Procedures provided on conventional hard-copy media.

Computerized procedures—Procedures presented on a computer-driven video display unit (VDU), potentially including additional functionality beyond simply replicating PBPs on a VDU (further discussion follows).

Categories of CPs

Three different categories of CPs are defined in EPRI 1015313 according to the functionality that is provided. Note that these categories are defined only for the purpose of structuring the guidance and clarifying its applicability, and that these terms may be used differently in other contexts.

Electronic procedures (EP)—CPs that are presented on a computer-driven VDU in text or graphical form and 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 navigation links from a procedure to another display page where relevant indications and/or controls are located, or they may display process data values on the same screen through static links to a process database. EP systems, however, do not perform any data processing, logic processing, or decision-making.

Computer-based procedures (CBP)—CPs that incorporate additional functionality not found in PBPs or EPs. This could include 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, tied to the particular procedure step; automatic processing of step logic and display of the results; automatic checking of prerequisites or preconditions (but leaving the decision-making action 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; automatic tracking and display of place-keeping aids; and/or cautions or warnings based on current plant conditions.

Unlike 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, but they do not by themselves make the decision to act. The operator must make those decisions with CBPs.

CBPs with procedure-based automation (PBA)—CBPs that include the ability of the system or machine to automatically carry out multiple procedure steps when directed to do so by the operator. Once a sequence of automated steps has been authorized or commanded by the operator, the PBA system can make decisions as to whether or 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—such as starting a pump or closing a valve—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 can also 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. There are sequences of actions in plants today that are initiated and carried out automatically—for example, protective actions, such as the shutdown of a major pump or other piece of equipment, when preset conditions are sensed by the equipment's protective features. Reactor and turbine-generator trips and engineered safeguards actuations are also initiated automatically by the protection system and do not require operator action to commence. In contrast, PBA involves sequences of actions that can be performed automatically, on command by the operator, or manually, at the operator's discretion.

Levels of CP functionality

As can be seen from these definitions, there is a wide range of functionality that can be provided in a CP system, and that level of functionality can have an impact on the operator's role in executing the procedures. EPRI 1015313 provides a detailed example of this for the case of a boiling water reactor emergency operating procedure, listing the major steps in the procedure, and indicating how the corresponding actions are taken with PBPs and with each of the three categories of CPs.

The CP categories defined above help in identifying the guidelines and criteria that should be applied during the design and implementation of a CP system, according to the functionality that is provided. The following section summarizes the guidelines provided in the EPRI report and their applicability to the different categories of CPs.

CP design, implementation

Technical basis for the guidance

Several sources of information were used to develop the guidance in EPRI 1015313. The first source used was EPRI 1010042,[12] which contains guidance on CPs and automation. An industry working group made up of representatives from plant owners/operators, suppliers, and consultants directed the development of the guidance in that report, which was peer-reviewed by a cross-section of working group members and other industry experts.

A second source was the guidance contained in EPRI 1011851,[13] which also was peer-reviewed by industry experts, on the use of automation in nuclear power plants.

Contents of the New EPRI Guidelines (1015313)

Introduction
- Scope of the guidance
- Benefits and challenges associated with computerized procedures (CP)
- CP functionality and concept of operations
- Technical basis for the guidance

General design and implementation guidelines
- Human factors engineering design
- Quality assurance and operator real-time verifications
- Potential sources of errors or problems in executing CPs
- Quality assurance, validation and verification, and backups
- Other digital system design requirements
- Data integrity
- Monitoring and verification by the operating crew
- CP maintenance and configuration management
- Transitioning between CPs and backup procedures

Additional guidelines for procedure-based automation (PBA)
- General design guidelines
- Guidelines to support operator monitoring and interaction with PBA
- Operator training for interactions with PBA

Soft controls design guidelines
- General guidelines for soft controls
- Additional guidelines for soft controls integrated with CPs

References

Finally, as part of the EPRI guidance development effort, an updated literature search and evaluation of previous studies on CPs and automation was conducted.

The new guidance has undergone extensive review by members of NEI's Human Factors Task Force, which consists of representatives from utilities, suppliers, new plant consortia, and consultants. The draft report also received a limited review by the NRC's Highly Integrated Control Room–Human Factors Task Working Group (TWG 5; see previous article in this section, page 80) as part of interactions between the industry and the NRC on issues related to digital I&C systems and highly integrated control rooms. Comments were received from the NRC and discussed with the TWG, and appropriate modifications were made to address those comments. At the time of this writing, no specific plans were in place for the NRC to formally endorse or adopt the new EPRI guidance in the near term, but the commission is expected to consider it in the future, after other higher-priority issues have been resolved.

Worth noting is that the IEEE Power and Energy Society, under its Nuclear Power Engineering Committee's Subcommittee SC-5 on human factors, is developing a standard that provides human factors guidance for computerized operating procedure systems.[14] The subcommittee has used the new EPRI guidelines as a starting point for developing this standard.

PBA involves sequences of actions that can be performed automatically, on command by the operator, or manually, at the operator's discretion.

Overview of the guidance

EPRI 1015313 addresses the full range of design and licensing issues associated with CP systems, including overall HFE design, CP system quality assurance, data integrity, interaction with procedure-based automation, transition from CPs to back-

up procedures, and CP maintenance and configuration management (see accompanying table). Following are brief descriptions of the guidance provided in several key areas.

HFE design

General HFE design guidelines address the application of accepted HFE methods and principles in the CP system design and its integration into the overall design of the main control room. Also addressed is the consistency of the CP system design—including the level of automation—with the roles and responsibilities of the operating crew members and the plant's overall concept of operations. The application of a graded approach to HFE design and evaluation activities is discussed, along with guidelines on items such as information that should be continuously displayed, the readability and usability of the information displayed, and means of place-keeping in the procedures.

The guidelines on quality assurance and verification and validation for CP systems are based first on the category of CP involved.

Quality assurance, V&V, and backups

The guidelines on quality assurance and verification and validation (V&V) for CP systems are placed in context by first reviewing the potential sources of errors in executing CPs, and then comparing these to sources of errors in executing PBPs. Sources of errors can include problems with the quality or integrity of the data or information used in processing the procedure; problems with the completeness of the data or information used in processing the procedure; and problems in processing the step logic and procedural instructions.

It is pointed out in the guidelines that these sources of errors are present with PBPs as well as with CPs, and the guidance is then focused on what is unique or different with a CP implementation that may require different or additional measures to protect against errors when CPs are used.

The guidelines on quality assurance and V&V for CP systems are based first on the category of CP involved. For electronic procedures, which basically display replicas of PBPs on a computer display, the guidelines indicate that the CP system should be subject to administrative controls similar to those on other computer systems that manage data important to safety.

For computer-based procedures (CBP), the guidelines indicate that the level of rigor and the depth of the quality assurance and V&V activities should be determined using a graded approach that considers the risk significance of the tasks that the procedures support and the potential risk impact of failures in the CP system, the complexity of the hardware and software of the CP system, and the operator verifications, cross-checks, and confirmations to be performed during procedure execution to help detect and mitigate the effects of CP system errors or failures.

The guidelines note that even within the CBP category, the level of functionality can vary considerably—for example, the level of automated data gathering and step processing, or whether the CBPs include the capability to control plant equipment—and this will have an impact on the complexity and risk associated with failures in the procedure system. For CBPs that incorporate procedure-based automation (PBA), additional guidance is provided that is specifically directed at the PBA (further discussion follows).

The guidance also addresses the need for the use of backups in case of the failure of a CP system. The backups can be PBPs, or CPs provided on a separate platform that is not subject to the same failures. Guidance is provided for determining the minimum set of backup procedures that should be provided in case of the failure of CPs that support risk-significant tasks, including procedures needed for accident mitigation, safe shutdown, emergency response, severe-accident management, or the performance of other risk-significant manual actions identified in the probabilistic risk assessment.

Monitoring and verification

A number of guidelines are provided on provisions for operator monitoring and verification of CPs. These guidelines apply to CBPs, including those with PBA, but they do not apply to EPs. As noted earlier, operator monitoring and verification of information used by CBPs, results obtained by any automatic processing of information, and any decisions made or suggested by CBP systems are an important part of protecting against errors.

The guidelines address the following:

- Identification of information that should be continuously displayed to support operator monitoring of progress through the procedures.
- Capture in the CBP of all relevant information needed to support procedure step processing and decision-making, including information that may not have been explicit or well-defined in the equivalent PBPs.
- Support of the crew in appropriate supervision and peer-checking of operator actions when using CBPs.
- Incorporation of operator verification of automated processing when there is subjectivity involved in correctly evaluating the procedure step logic.
- The need for the operator to remain in control and to be the final authority, with the ability to reject recommendations of automated processing and take an alternate path when necessary.
- The need for training to address the potentially different roles for individual crew members when using CBPs versus PBPs, including the role of the supervisor, and to address the potential impact on crew communication and coordination.

Procedure-based automation

General guidelines for the design of integrated human-automation systems are provided in the guidance, reflecting basic principles that are applicable to PBA as well as to other automated systems. These are followed by guidelines specific to PBA, including a number of guidelines related to operator monitoring and interaction with PBA, particularly automated sequences or blocks of procedure steps. The guidance addresses the need to provide information to assist the operator in determining whether preconditions have been met to allow an automated sequence to begin and in deciding whether to execute the block of steps automatically or manually. The presentation of information on the status of the automated process—including the status of parallel processes, such as the monitoring of continuously applicable steps or preconditions being monitored across multiple steps—is also addressed.

The guidance addresses the need for predefined hold points at which the PBA stops and waits for the operator to authorize continued progress through the procedure. Criteria are suggested for determining where hold points should be placed, with the recognition that they should be used where needed but not overused to the degree that they are not meaningful to the operator.

Other issues addressed by the guidance include providing the capability for the operator to interrupt an automated sequence at any time—ensuring a safe and effective transition from automatic to manual execution of procedure steps—and operator training for interaction with PBA.

Soft controls

Soft controls (controls mediated by software rather than hardware that allow manipulation of plant equipment) may be integrated into a computerized procedure

system, selecting and giving the operator easy access to the controls needed to carry out a procedure step. The EPRI document provides a few additional guidelines that are specific to soft controls integrated with CPs. For general guidelines on soft control design, the reader is referred to other industry guidance documents.

References

1. Portmann, F., and M. H. Lipner, "An Operational Model for Using a Computerized Emergency Operating Procedures System," *Modern Power Systems* (2002).
2. O'Hara, J., J. Higgins, W. Stubler, and J. Kramer, "Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance," NUREG/CR-6634, Washington, D.C.: U.S. Nuclear Regulatory Commission (2000).
3. Roth, E., and J. O'Hara, "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).
4. 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," *Proceedings of the American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2006),* Albuquerque, N.M., November 12–16, 2006, on CD-ROM, American Nuclear Society, La Grange Park, Ill., pp. 217–226 (2006).
5. Eiler, Janos, "Computerized Emergency Operating Procedures at the Paks NPP, Hungary," *Proceedings of the American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2006),* Albuquerque, N.M., November 12–16, 2006, on CD-ROM, American Nuclear Society, La Grange Park, Ill., pp. 1185–1190 (2006).
6. Chung, Yun H., Sung N. Choi, and Bok R. Kim, "Preliminary Evaluation of Computerized Procedure From Safety Viewpoints," *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 (2002).
7. Gutierrez, R., D. Zizzo, and K. Yu, "Human Factors Verification and Validation of the Advanced Nuclear Plant Control Room Design," *Proceedings of Global 2005,* Tsukuba, Japan, October 9–13, 2005, Paper no. 392 (2002).
8. Lipner, M. H., R. A. Mundy, and M. D. Franusich, "Dynamic Computer Based Procedures System for the AP1000 Plant," *Proceedings of the American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC&HMIT 2006),* Albuquerque, N.M., November 12–16, 2006, on CD-ROM, American Nuclear Society, La Grange Park, Ill., pp. 692–694 (2006).
9. O'Hara, J., W. S. Brown, P. M. Lewis, and J. J. Persensky, "Human-System Interface Design Review Guidelines," NUREG-0700, Rev. 2, Washington, D.C.: U.S. Nuclear Regulatory Commission (2002).
10. "Computerized Procedures: Design and Implementation Guidance for Procedures, Associated Automation and Soft Controls," EPRI 1015313, draft in progress, to be published by EPRI, Palo Alto, Calif., in 2009.
11. O'Hara, J., D. Pirus, S. Nilsen, R. Biso, J. E. Hulsund, and W. Zhang, "Computerisation of Procedures, Lessons Learned, and Future Perspectives," HPR-355, OECD Halden Reactor Project (2003).
12. "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," EPRI 1010042, Electric Power Research Institute, Palo Alto, Calif. (2005).
13. "Development of Guidance for the Proper Design and Use of Automation in Nuclear Power Plants," EPRI 1011851, Electric Power Research Institute, Palo Alto, Calif. (2005).
14. "Human Factors Guide for Applications of Computerized Operating Procedure Systems at Nuclear Power Generating Stations and Other Nuclear Facilities," P1786, IEEE Nuclear Power Engineering Committee, Subcommittee SC-5, draft in progress. NN