IEEE SA
STANDARDS
ASSOCIATION

STANDARDS

IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities

IEEE Power and Energy Society

Developed by the
Nuclear Power Engineering Committee

IEEE Std 1786™-2022
(Revision of IEEE Std 1786-2011)

IEEE

IEEE Std 1786™-2022
(Revision of IEEE Std 1786-2011)

IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities

Developed by the

Nuclear Power Engineering Committee
of the
IEEE Power and Energy Society

Approved 8 February 2022

IEEE SA Standards Board

Abstract: The application of computerized operating procedure systems (COPS), their design (i.e., form and function), and use is presented in this guide.

Keywords: computerized procedures, human factors, IEEE 1786™, nuclear facilities

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-8470-1 STD25260
Print: ISBN 978-1-5044-8471-8 STDPD25260

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4] Available at: https://standards.ieee.org/standard/index.html.
[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Introduction

This introduction is not part of IEEE Std 1786-2022, IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities.

IEEE Subcommittee 5 on Human Factors, Control Facilities, and Human Reliability (SC5), a unit of the IEEE Nuclear Power Engineering Committee (NPEC), has developed and maintained human factors engineering standards for nuclear facilities since the early 1980s. The SC5 has structured its standards in a hierarchical fashion. The top-level SC5 guidance document is IEEE Std 1023™, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities.[6] IEEE Std 1023 promotes the systematic integration of human performance considerations in the life cycle of commercial nuclear power plants and other nuclear facilities. IEEE Std 1023 is supported by additional standards written to address specific technical needs. IEEE Std 1786-2011 is an additional standard that provides guidance for the application of computerized operating procedure systems (COPS) in nuclear facilities.

The SC5 began considering the need for guidance on computerized procedures in the early 1990s. Since that time, advancing technology and experience demonstrated the viability of such systems, enabling the initial publication of this standard in 2011 with the consensus of industry, vendor, and regulatory participants.

Computerized operating procedure systems are systems used to present plant operating procedures via electronic visual display rather than hard copy (i.e., print) media. Using computers to present nuclear plant operating procedures has been explored at least since the early 1980s, with several commercial power plant applications implemented by the late 1990s. With the further implementation of highly computerized control rooms, the use of COPS will be increasingly widespread.

It is generally accepted that computers are well-suited to such tasks as monitoring, display, and logical evaluation of real-time data. These capabilities can address many of the routine problems that invite human error in the use of conventional, hard-copy operating procedures. At the same time, concerns remain about the impact of computers on the role and performance of human operators, and about the allocation of decision-making authority to computers. This document takes a conservative approach to these issues, such that the following principles are implicit throughout:

- Procedures are written directions for human operators, developed according to established procedure development guidance.
- When procedures are implemented by COPS, the role of COPS is to facilitate the human operator's elective use of those procedures.
- The established operator roles, directions given by a procedure (i.e., their structure, technical content, and so forth), criteria by which procedure content is judged acceptable, and the responsibility of the operator to best implement those directions, should not vary with the procedure media.

The recommendations for COPS can thus be guided, to some extent, by analogy to the organization and use of conventional hard-copy procedures. For example, operators should be able to report their locations in a procedure network at any time, as well as their reasons for being in that location. Capabilities that are not transparent to the operator, such as nondeterministic branching, dynamic structuring of procedure contents, or complex machine reasoning, are thus not recommended for COPS applications.

These guidelines should be implemented within the framework of a formal human factors program, including task analysis of the procedures to be computerized. Consideration of the user's needs and preferences will help ensure that COPS can be employed confidently and effectively.

[6] Information on references can be found in Clause 2.

The guide consists of the primary guidance in Clause 1 through Clause 5, along with three annexes. Annex B and Annex C provide additional information (e.g., tutorials) for guide steps in Clause 4 and Clause 5.

The working group deemed certain topics to be outside the scope of this guide, on the basis that no unique considerations were identified for COPS and that general guidance was better provided elsewhere. These topics include the conduct of plant operations, control room communications, cybersecurity, display and control design, general human factors engineering, operator training, procedure development, system testing, and software development.

This 2022 revision updates the normative references in Clause 2 and the bibliographic references in Annex A to provide more current lists. However, there have been no substantive changes to the normative text of this standard.

Participants

At the time this IEEE guide was completed, the Human Factors Applications and Methods Subcommittee Working Group 5.1 had the following members that attended meetings and contributed to the effort:

David Desaulniers, *SC5 Chair*
Stephen Fleger, *Working Group Chair*
Jeffrey Joe, *Champion*

Ronald Boring
Chris Kerr
Ryan Flamand
Casey Kovesdi
Robert Fuld
Quinn Reynolds
Richard Gutierrez
Robert Starkey

At the time of publication of IEEE Std 1786-2011, the working group had the following members:

Stephen Fleger, *SC5 Chair*
Robert Fuld, *Vice Chair*
Robert Waters, *Working Group Chair*
Chris Kerr, *Co-Champion*
Richard Browder, *Co-Champion*

Brian Babcock
Valerie Barnes
Michael Boggi
David Desaulniers
Matt Gibson
Robert Hall
Jack Hardy
Doug Hill
Jacques Hugo
Robert Leger
Mel Lipner
Scott Malcolm
Jerold Marks
Dan Meekhoff
Julie Reed
Anthony Spurgin
Robert Starkey
Thad Wingo
Jing Xing

The following members of the individual balloting committee voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

S. Aggarwal
George Ballassi
Jason Bellamy
Brian Braithwaite
Keith Bush
Paul Cardinal
Suresh Channarasappa
David Desaulniers
John Disosway
Neal Dowling
Stephen Fleger
Daryl Harmon
David Herrell
Lee Herron
Werner Hoelzl
Ronald Jarrett
Jeffrey Joe
Piotr Karocki
Robert Konnik
Thomas Koshy
Jinsuk Lee
Ting Li
Bruce Lord
Jeffrey McElray
Edward Mohtashemi
Dennis Neitzel
Warren Odess-Gillett
Bansi Patel
Howard Penrose
Jan Pirrong
Gene Poletto
Eric Rasmussen
Gregg Reimers
Hugo Ricardo Sanchez Reategui
Eugene Stoudenmire
Scott Sweat
Marek Tengler
John Vergis
Whitney Ward
Yvonne Williams
Shuhui Zhang

When the IEEE-SA Standards Board approved this guide on 8 February 2022, it had the following membership:

David J. Law, *Chair*
Vacant Position, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Ted Burse
Ramy Ahmed Fathy
J.Travis Griffith
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick
Johnny Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Andrew Myles
Damir Novosel
Annette D. Reilly
Robby Robson
Jon Walter Rosdahl
Mark Siira
Dorothy V. Stanley
Lei Wang
F.Keith Waters
Karl Weber
Sha Wei
Philip B. Winston
Daidi Zhong

*Member Emeritus

Contents

IEEE Guide for Human Factors Applications of Computerized Operating Procedure Systems (COPS) at Nuclear Power Generating Stations and Other Nuclear Facilities

1. Overview

1.1 Scope

This document provides guidance for the application of computerized operating procedure systems (COPS). This guidance concerns the design (i.e., form and function) and use of COPS. In general, this guide does not provide guidance for the technical content of the operating procedures being presented except as needed to address unique aspects of procedure implementation on COPS. Software tools that can be described as computerized procedures but reside outside the control room (such as might be used for maintenance or testing) are also beyond the scope of this document.

1.2 Purpose

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

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*). [7, 8]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

[7] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

[8] The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 7-4.3.2™, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations.[9,10]

IEEE Std 603™, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

IEEE Std 1012™, IEEE Standard for Software Verification and Validation.

IEEE Std 1023™, IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities.

IEEE Std 1289™, IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [11]

active step: In the context of a computerized operating procedure system, a procedure step is active (i.e., has "active" status) while the step is selected on the system for evaluation and possible execution.

computerized operating procedure systems (COPS): Computer applications that present operating procedures to operators using an electronic visual display.

embedded soft control: The capability of a computer application (e.g., COPS) to issue, upon user demand, individual or sequential control commands for plant equipment.

fully determined: A statement (e.g., a procedure step) is fully determined if it is logically complete, such that it gives a deterministic result when evaluated for any given set of inputs.

procedure-based automation: The evaluation and execution of a predefined sequence of procedure steps by COPS.

[9] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (https://standards.ieee.org/).
[10] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.
[11] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

soft control: An element of a computer-generated visual display that is operationally equivalent to a physical device (e.g., a pushbutton, selector switch, potentiometer, component controller, and so forth) that is used to operate plant equipment upon user demand.

3.2 Acronyms and abbreviations

AOP	abnormal operating procedure
ARP	alarm response procedure
COPS	computerized operating procedure systems
EOP	emergency operating procedure
HFE	human factors engineering
NOP	normal operating procedure

4. Conceptual framework

4.1 General

The contents of this clause define the framework for the detailed design guidance that is presented in Clause 5. Additional information is contained in Annex B.

4.2 Human factors engineering principles for COPS

Human factors engineering (HFE) principles should be systematically considered throughout design and development process of COPS, including but not limited to the following:

a) Prospective COPS users should be iteratively involved in the design process so that their needs are adequately addressed.

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

c) The organization and structure of procedures on COPS should be compatible with the organization and structure of currently used paper-based procedures.

d) COPS with sufficient capability may evaluate the logical conditions of one or more procedure steps, if the results in each case are fully determined by the step logic and the available process data. Steps with elements not fully determined require a decision to be made by the operator. COPS should not make such decisions.

e) Results produced by COPS evaluation should be the same as those expected from operator evaluations of the same steps.

f) Loss of COPS should not affect the operator’s ability to safely operate the plant.

4.3 Types of COPS

For the purposes of this guide, three types of COPS are identified, based on successive levels of functional capability. The capability of each type is assumed to include the capabilities of simpler types. Thus, a Type 2 system should address both Type 1 and Type 2 guidance, and a Type 3 system should address the guidance for Type 1, Type 2, and Type 3 systems (see Table 1).

4.3.1 Type 1 systems

Type 1 systems represent procedure text documents for operational use on a computer-generated visual display.

4.3.2 Type 2 systems

Type 2 systems use dynamic process data for embedded display, to evaluate conditions or procedure logic, or to monitor plant conditions during procedure-defined intervals of applicability. Type 2 COPS cannot issue control commands, but they may provide access to soft control capabilities that exist outside of the COPS.

4.3.3 Type 3 systems

Type 3 systems include embedded soft controls that may be used to issue control commands to plant equipment.

Type 3 systems may include automatic sequences of steps (i.e., procedure-based automation) that are determined to require limited operator oversight, and for which there are procedures and training that would allow the operator to perform the steps manually, if necessary or desired.

Table 1 provides examples of capability that may be provided by the different types of systems.

Table 1—COPS capability taxonomy

Capability	COPS		
	Type 1	Type 2	Type 3
Select and display procedure on computer screen.	Yes	Yes	Yes
Provide navigation links within or between procedures.	Yes	Yes	Yes
Display process data in the body of procedure steps.	No	Yes	Yes
Process step logic and display results.	No	Yes	Yes
Provide access links to process displays and soft controls that reside on a separate system.	No	Yes	Yes
Provide embedded soft controls.	No	No	Yes
On operator command, initiate procedure-based automation.	No	No	Yes

4.4 Types of operating procedures

General types of operating procedures that may be represented on COPS include the following:

- Normal operating procedures (NOPs)
- Surveillance procedures
- Alarm response procedures (ARPs)
- Abnormal operating procedures (AOPs)
- Emergency operating procedures (EOPs)

5. Design guidelines

5.1 General

Clause 5 provides general guidance for the design of COPS. Additional explanation for the guidelines is contained in Annex C.

5.2 Guidelines applicable to Type 1, Type 2, and Type 3 systems

For the purpose of this clause, COPS are assumed to be a significant human interface, as defined in IEEE Std 1023™. As such, HFE principles and methods should be considered as applicable to the design of COPS, and the presentation of information by COPS should conform to accepted HFE practices. See IEEE Std 1023 and IEEE Std 1289™ for additional information on the basic considerations of HFE and their systematic application in design. In addition, the following design guidelines apply generally for COPS:

a) COPS should not determine what procedure should be used by the operating crew. The crew should decide what procedure would be used in any given situation. COPS may recommend or prompt the operator to use a particular procedure, but the operator should be able to override this recommendation.

b) COPS should allow, consistent with station administrative procedures, the ability of operators to deviate from procedure steps or from the defined sequence of procedure steps.

c) Access to relevant displays and supporting information should be provided. For Type 1 systems, relevant displays and supporting information should be available at the work location (e.g., control room). Type 2 and Type 3 systems may provide relevant displays and supporting information as part of the functionality of COPS.

d) COPS should provide the capability to look-ahead and look-back within the procedure.

e) COPS should provide a place-keeping function within the procedures.

f) COPS should provide navigation links within or between procedures.

g) COPS should have the capability to record or log progression and operation through the procedures.

h) Procedures currently open for use on COPS should be evident as such.

i) For multiunit control rooms, a unique identifier should indicate the unit(s) to which the procedure is applicable.

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

k) If COPS provide multiple modes of operation (e.g., automatic, manual), then COPS should indicate the current mode of operation.

l) Backup procedures (paper-based procedures [PBPs] or alternate COPS) should be provided in case the COPS degrades or fails.

m) The structure and format of information in COPS should be compatible with backup procedures. See 5.5 for additional information.

5.3 Guidelines applicable to Type 2 and Type 3 systems

In addition to the guidance in 5.2, the following design guidelines apply to Type 2 and Type 3 systems:

a) Where sensor data is available to support the confirmation of procedure prerequisites or initial conditions, then COPS should provide such confirmation.

b) In a procedure that is open for use, COPS should show which step(s) are presently active. “Active” status is advanced between steps by direction of the operator of the COPS.

c) COPS should provide monitoring and status indication for any step with extended or continuous applicability, while that step remains active.

d) Data evaluated by COPS to reach a result should be available to the operator. Logic rules should be provided as well as the data.

e) The capability should be provided within the control room for a read-only view of ongoing procedure activities. While viewing any step is permissible in this mode, the read-only view should indicate the currently active step(s).

f) COPS should provide indication that the system is operating (e.g., a heartbeat).

g) Appropriate isolations between COPS and safety-related systems should be provided when COPS are implemented on a non-safety-related platform. Digital communication independence between non-safety-related COPS and safety-related systems should be in accordance with IEEE Std 603™ and IEEE Std 7-4.3.2™.

h) COPS should support crew implementation of a procedure. COPS may allow more than one concurrently active step in a procedure. Each active step in a procedure should be indicated to all users of the procedure, including those involved in remote viewing.

i) COPS may be designed to have a master procedure, providing status only, to support multiple sessions of the same procedure being opened for use by separate operators.

j) COPS should support concurrent implementation of procedures. COPS may allow more than one procedure to be open for use at a time. COPS should allow active steps to exist concurrently in all procedures that are open for use.

5.4 Guidelines unique to Type 3 systems

In addition to the guidance provided in 5.2 and 5.3, the following design guidelines apply to Type 3 systems:

a) The characteristics and behavior of embedded soft controls should be compatible with the hard and soft controls in the control room.

b) Information needed to support effective use of embedded soft controls, such as the plant and equipment status, should be readily available.

c) Procedure-based automation may be used to execute sequences of fully determined steps between predefined hold points (see 5.5.3) in a procedure. The predefined hold points are defined and validated during procedure development.

5.5 Guidelines for the application of procedure-based automation

5.5.1 General

The guidelines below apply only to Type 3 systems that provide the capability for procedure-based automation.

5.5.2 Step sequences

The following design guidelines apply to step sequences and their automatic execution.

a) Automatic execution of sequences should be initiated manually and utilized at operator discretion.

b) The use of automatic sequences should not be necessary to successfully perform the procedure.

c) The specification of sequences and hold points should be part of the formally controlled procedure contents.

d) COPS should indicate the specific sequence of steps that the automation is to follow, including branching and termination.

e) COPS should update the indicated status of steps within a sequence during the automatic execution of the sequence.

f) Automated sequences should begin and end within a single procedure.

g) COPS should display the current mode of COPS execution (e.g., manual, automatic, ready, running, holding, interrupted, completed, and so forth).

h) COPS should alert the operator if an unexpected mode change occurs automatically.

i) COPS should provide on demand the time history of step execution for automated sequences.

j) Information on conditions that should be met before an automated sequence may begin should be available.

k) The selection of step sequences for automation should include consideration of factors (e.g., duration, complexity) that may impact operator awareness of the situation (e.g., plant operating conditions) and the operator's ability to resume manual control, if necessary or desired.

5.5.3 Hold points

The end of an automated sequence is defined by a hold point. A hold point is a predetermined point in the procedure at which automatic execution stops and waits for operator direction. The following guidelines apply to the use of hold points:

a) Hold points should be placed in order to engage the operator to:

  1) Monitor and confirm the automation’s progress

  2) Maintain awareness of the status of the affected plant systems and operations

  3) Make decisions

  4) Give authorization

b) The location of hold points should be visible within the procedure on the COPS display.

c) COPS should not allow operators to remove or defeat predefined hold points.

d) At any time before the start of an automatic sequence, the COPS should permit the operator to temporarily add hold points between the steps of the sequence. That is, the operator should be able to subdivide a sequence as needed to better manage the controlled process. The hold points inserted by the operator are temporary in the sense that they do not modify the approved procedure.

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

5.5.4 Sequence interrupts

The following design guidelines apply to interrupt features supporting the automatic execution of step sequences.

a) COPS should allow the operator to manually interrupt execution at any point in a sequence. Control commands issued prior to the interrupt may continue in effect or to completion on the controlled system.

b) COPS should automatically interrupt the sequence if a step is not successfully executed or other conditions warrant.

c) Automatic interrupts should include an alerting function.

d) Automatic interrupts should identify the following:

  1) Where the sequence has stopped

2) The source of the interrupt

e) After a sequence is interrupted, the operator should be able to resume automatic execution if desired.

5.6 COPS backup

The following guidelines apply to all types of COPS unless otherwise noted:

a) Backup procedures should be available and readily accessible to the users of COPS.

b) COPS should support timely and effective transition to backup procedures. The time required to transition from COPS to the backup procedures should allow the primary goals of the procedures to be met and should not jeopardize plant safety.

c) COPS users should be trained to recognize when conditions exist requiring transition to the backup procedures such that the transition can be performed in a timely manner.

d) When a system failure or degradation occurs that requires transition to a backup procedure, the operator should be able to determine the following:

1) What procedures were being executed at the time of failure

2) Which step(s) in each procedure were being processed at the time of failure

e) For Type 2 or Type 3 systems, when failure or degradation occurs that requires transition to a backup procedure, the operator should also be able to determine what conditions or steps, if any, were being continuously monitored by the COPS at the time of failure.

5.7 Quality assurance for non-safety-related COPS

The following guidelines apply to quality assurance activities for COPS and its related systems:

a) The software quality assurance (QA) and verification and validation (V&V) guidance of IEEE Std 1012™ should be considered in COPS software development activities, as applicable.

b) For operating procedures provided on Type 2 or Type 3 systems, procedure QA/V&V should include final activities to confirm that the technical contents of each PBP is correctly represented in the corresponding computerized operating procedure. This final confirmation of each computerized operating procedure (including automatic step sequences and hold points, if any) should be based on dynamic process input to the COPS, such as provided by a plant-specific training simulator.

5.8 Process data integrity

The following guidelines apply to data integrity issues for COPS and its related systems:

a) Where quality status information is available for COPS data and the quality of a displayed data item is other than good (e.g., bad, suspect, poor, and so forth), then the information quality should be displayed.

b) The detection of a data quality problem in any upcoming step of an automated sequence should result in a sequence interrupt. Where a data quality problem is indicated, the capability should exist for the operator to individually mark a degraded datum as temporarily usable, so that automated sequence execution may proceed, if appropriate.

5.9 Maintenance and configuration management

The following guidelines apply to activities related to maintenance and configuration management for COPS and its related systems:

a) COPS should allow updates to procedures without impacting plant operations. COPS should be designed such that procedure changes can be made without changing the application software. Means should be provided to control changes made to the procedures over the life of the plant.

b) The configuration control and procedure management processes should warrant the following:

   1) That the procedure contents are verified and validated on the COPS, including links and embedded functionality, prior to being issued for use

   2) That the COPS presents the most recently approved and issued version of each procedure

c) Type 2 and Type 3 systems should facilitate the V&V of changes to COPS software, including the impact of software changes on the usability and accuracy of the procedure content.

d) COPS should support station administrative processes for documenting procedure errors, including procedures that are in use, and implement approved changes.

e) When procedures within COPS are updated, the configuration management program should warrant that compatibility is maintained between the COPS procedures and the backup procedures.

Annex A

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] Chung, Y. H., S. N. Choi, and B. 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,* Sept. 25−27, 2001, Hluboka nad Vltavou, Czech Republic, NEA/CSNI/R (2002)1/vol. 2, JT00127981, June 11, 2002.

[B2] DaCruz, P., "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 (NPIC&HMIT),* Albuquerque, NM, November 12–16, 2006, pp. 217–226.

[B3] DI&C-ISG-04, Rev. 1, "Digital Instrumentation and Controls, Task Working Group #4: "Highly-Integrated Control Rooms—Communications Issues (HICR): Interim Staff Guidance," U.S. Nuclear Regulatory Commission, Washington, DC, March 2009.

[B4] DI&C-ISG-05, Rev. 1, Sec. 1 "Task Working Group #5: Highly-Integrated Control Rooms—Human Factors Issues," U.S. Nuclear Regulatory Commission, Washington, DC, November 2008.

[B5] Eiler, J., "Computerized Emergency Operating Procedures at the Paks NPP, Hungary," *Proceedings of the American Nuclear Society International (NPIC&HMIT)*, Albuquerque, NM, November 12–16, 2006, pp. 1185–1190.

[B6] EPRI 1010076, "Advanced Control Room Alarm System: Requirements and Implementation Guidance," Electric Power Research Institute, Palo Alto, CA, December 2005.

[B7] EPRI 1015313, "Computerized Procedure Systems: Guidance on the Design, Implementation, and Use of Computerized Procedure Systems, Associated Automation, and Soft Controls," Electric Power Research Institute, Palo Alto, CA, August 2010.

[B8] EPRI 3002004310, "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 for Operating Plants and New Builds," Electric Power Research Institute, Palo Alto, CA, December 2015.

[B9] Fleger, S., "A Philosophical Perspective and Summary of IEEE's Human Factors Standard on Computerized Operating Procedure Systems (COPS)," *Proceedings of the American Nuclear Society International (NPIC&HMIT),* San Diego, CA, July 22–26, 2012, pp. 1669–1682.

[B10] ISO/IEC/IEEE Std 15288™-2015, Systems and Software Engineering—System Life Cycle Processes.[12]

[12] ISO/IEC publications are available from the ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland (https://www.iso.org/). ISO/IEC publications are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (https://www.ansi.org/).

[B11] 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 (NPIC&HMIT)*, Albuquerque, NM, November 12−16, 2006, pp. 692−694.

[B12] NUREG/CR-6634, O'Hara, J. M., J. C. Higgins, W. F. Stubler, and J. Kramer, "Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance," U.S. Nuclear Regulatory Commission, Washington, DC, March 2000.[13]

[B13] NUREG-0700, Rev. 3, Sec. 8, O'Hara, J. M. and S. Fleger, "Human-System Interface Design Review Guidelines," U.S. Nuclear Regulatory Commission, Washington, DC, July 2020.

[B14] NUREG-0899, "Guidelines for Preparation of Emergency Operating Procedures—Resolution of Comments on NUREG-0799," U.S. Nuclear Regulatory Commission, Washington, DC, August 1982.

[B15] O'Hara, J. M., D. Pirus, S. Nilsen, R. Bisio, J. E. Hulsund, and W. Zhang, "Computerisation of Procedures Lessons Learned and Future Perspectives," OECD Halden Reactor Project, Halden, Norway, HPR-355, July 17, 2003.

[B16] Regulatory Guide 1.33, Rev. 3, "Quality Assurance Program Requirements (Operation)," U.S. Nuclear Regulatory Commission, Washington, DC, June 2013.

[B17] Spurgin, A. T., D. D. Orvis, D. Cain, and C. C. Yau, "Testing and Expert System: Testing the Emergency Operating Procedures Tracking System," *Proceedings of the 4th Conference on Human Factors and Power Plants*, Monterey, CA, 1988.

[13] NUREG publications are available from the U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, USA (https://www.nrc.gov/).

Annex B

(informative)

Conceptual framework (supplement)

The following information is provided as supplementary information to the guidance provided in Clause 4. Where applicable, reference back to the corresponding subclause is provided.

The concepts of COPS 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 COPS to improve overall plant safety and performance. Ultimately, the roles and responsibilities of plant operators for procedure execution should be consistent with the results of the overall HFE program. In all cases, human operators are responsible for the proper application of operating procedures (see 4.2).

The COPS functionality, 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 crewmembers. Of course, the design of the overall control room, arrangement of the operators' workstations, and design of the associated system interfaces also play an important role here. However, the focus of this discussion is on implementation of different levels of COPS and their interaction with the crew organization, roles and responsibilities, and overall concept of operations.

COPS may perform deterministic evaluations (e.g., YES/NO based on procedure logic and plant data). A well-formed logical statement has only one answer for each possible combination of input values; this is what is meant by a "fully determined step" in 4.2, and more generally characterizes the code of a computer program. As distinct from a logical branch, no decision (in the human cognitive sense) is involved in a fully determined step. However, to break such a rule for any reason (other than a malfunction) would require a decision. So as defined, only a human operator can make cognitive decisions. It is common that procedures written for humans—rather than as programs for machines—have some steps that are not fully determined. That is, the step is vague, the rules or inputs are incomplete (or have become incomplete, e.g., due to sensor failures), or the step somehow depends on unspecified or subjective considerations. Such nondeterministic or at least partly subjective steps can only be resolved by a decision-maker, i.e., a human operator. Thus, for the purposes of this document, COPS is limited to performing steps that are fully determined; i.e., COPS makes (deterministic) evaluations. Humans may perform any procedure step, but only humans may perform nondeterministic steps; i.e., humans must make all (subjective) decisions.

Loss of COPS should not affect the operator's ability to safely operate the plant (see 4.2). COPS should be considered an operator aid for operating the plant, and loss of an aid should not prevent the operator from performing required actions. Failure of COPS should not have any impact on control systems.

Use of COPS cannot change the existing plant procedure use and adherence requirement as discussed in ANSI/ANS N18.7 and ANSI/ANS 3.2. The NRC via RG 1.33 [B16][14] endorses both standards. Plants should maintain Level of Use categories similar to the following:

- **Level 1: Continuous Use.** Reading each step of the procedure prior to performing that step, performing each step in the sequence specified and place-keeping each step as complete before proceeding to the next step.
- **Level 2: Reference Use.** Referring to a procedure periodically during the performance of an activity to confirm that all procedure segments of an activity have been performed, performing each step in

[14] The numbers in brackets correspond to those of the bibliography in Annex A.

sequence specified and, where required, signing appropriate blocks to certify that all segments are completed. The procedure should be at the work location.

- **Level 3: Information Use.** An activity may be performed from memory, but the procedure is available, not necessarily at the work location, for use as needed to ensure the task is being performed correctly and for training.

Operating procedures in Type 2 and Type 3 systems should be Continuous Use (Level 1). Operating procedures in Type 1 systems can be any Level of Use, based upon site administrative requirements.

Consider the example of emergency operations carried out in accordance with the EOPs. Using PBPs in a conventional control room, a supervisor typically reads the procedure and evaluates the prescribed steps, asking operators to obtain plant data and to perform specified control actions. Much of the crew is involved in carrying out the procedure. Use of Type 1 COPS rather than PBPs may not change this situation greatly, because Type 1 COPS allow only limited additional functionality. Type 1 COPS may aid in navigating to procedures or make them available at more locations, but crewmember roles, responsibilities, and communications may be unchanged.

Type 1 Systems: COPS that are presented on a visual display in text or graphical form that are essentially replicas of PBPs. Type 1 systems may include the ability to call up a relevant procedure from a link in the procedure, but the procedure that is presented is the same as, or similar to, an equivalent PBP. Type 1 systems may also include links from a procedure to another display page.

Type 2 Systems: COPS that incorporate additional functionality not found in PBPs or Type 1 systems, such as:

- Integrated display of dynamic plant data
- Display of relevant indications either directly in the procedure itself or on another display page or section of the display
- Access to soft controls via links to an applicable system interface outside of COPS
- Evaluation of step logic and display of the results to support operator decision making

  NOTE—Example: A procedure step requires certain prerequisites to be met before taking an action (e.g., a pump's suction valve needs to be open and discharge valve closed before starting pump). Type 2 systems can monitor a valve's position and notify operator when prerequisites are met for starting the pump. COPS do not perform any associated control actions required by the procedure.
- Evaluation of prerequisites or initial conditions (but the decision is left up to the operator)
- Tracking of initial conditions over multiple steps
- Context-sensitive aids for making branching decisions
- Cautions or warnings based on current and/or changing plant conditions.

Note that, as differentiated from Type 1, Type 2 systems gather and display information relevant to a procedure step. Type 2 systems may process procedure step logic and display results including pass/fail indications. Moreover, Type 2 systems may suggest and prompt the operator to take actions or execute branches in a procedure.

As compared to a Type 1 COPS, the added functionality of a Type 2 COPS may warrant changes to communications protocols, to concepts of operation, and to individual operator roles. Such changes should be systematically developed, validated, and implemented based on a plant operator's inputs, plant-operating requirements, and the specific COPS design. For example, by displaying process data within the procedure, a Type 2 COPS may reduce the amount of three-way communication needed between the supervisor and the operators (e.g., for data with acceptable readings that is visible to all).

When Type 2 COPS incorporate access to soft controls, 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.

Hence, with Type 2 COPS, the operators may become system managers, individually supervising their areas of responsibility. Type 2 COPS in this case may enable them to utilize a higher level of cognition, rather than merely serving as equipment manipulators. In addition, the supervisor can spend more time assessing the overall health of the plant.

Type 3 Systems: COPS that include the capability to issue control commands. The capability to issue control commands from COPS may, in turn, be used to implement procedure-based automation. Procedure- based automation allows the grouping of multiple deterministic steps into predefined sequences. When so directed by the operator, COPS will advance the active step through the selected sequence, evaluating the steps of the sequence based on current plant inputs, and executing appropriate control actions. Sequences terminate at hold points, when operator input or authorization is required for COPS to continue. A sequence also may be halted prior to reaching a hold point (see 5.5.4). Sequence interrupts are generated automatically when the COPS detects an error, or manually at operator discretion.

It is important to distinguish procedure-based automation from other types of automation. Procedure-based automation is somewhat unique in being an automated aid to performing sets of actions that are organized for manual performance. This reflects that operating procedures are, fundamentally, instructions for human operators. In contrast, typical automatic control functions are not necessarily based on, or well-suited for, manual step-by-step performance. Typical examples of plant automation include protective trips, closed- loop control of process variables, startup of standby units on loss of a running unit, and so forth. While Type 3 systems may issue commands that call upon available automatic control or protective actions (i.e., as can otherwise be invoked manually), COPS should not be used to execute automatic control or protective functions that are not otherwise available for manual performance. Procedure-based automation should only be used to perform procedures that are equally suited to (and available for) manual performance. That is, performance without the COPS.

With Type 3 systems other role changes may occur. The automation may perform evaluations and make recommendations to the crew. 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.

Table B.1 uses the example of an emergency operating procedure to illustrate how operator activities in carrying out procedures may be impacted by the different levels of functionality provided with COPS. Note that in an emergency situation, the EOP may be only one of several procedures being executed simultaneously by the operating crew.

Table B.1—Changes to operator activities with different COPS functionalities

EOP Step	Actions taken with PBPs	Actions taken with COPS		
		Type 1	Type 2	Type 3
Continuously recheck conditions that, if they occur, require entry into alternate procedures, overriding the present procedure (e.g., 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.	Type 2 could continuously monitor and display a prompt when conditions are met, indicating the need to follow an alternate procedure.	Same as Type 2.
Determine whether safety injection system has initiated; if not, manually initiate the system.	Operator should check displays for indication of safety injection system initiation; operator should take manual actions to initiate if required.	Same as PBP.	Type 2 can automatically display status of the safety injection system. If not initiated, Type 2 can prompt for initiation. Operator action is still required to initiate safety injection, following a subtier system procedure.	Same as Type 2, but operator can take a single action to command safety injection system initiation. Type 3 then carries out the steps needed to initiate safety injection system, performing multiple valve operations automatically, per the subtier procedure.
Stabilize reactor pressure vessel (RPV) pressure using one or more of several systems including: safety-relief valves (SRVs). 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.	Type 2 can automatically determine and display which systems are available based on system and plant status. Type 2 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 Type 2, but on command from the operator, Type 3 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 limit, 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.	Type 2 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 Type 2.

Annex C

(informative)

Additional design guidance

The following information is provided as supplementary information to the guidance provided in Clause 5. Where applicable, reference back to the corresponding clause is provided.

C.1 Human factors

When procedures are computerized, COPS should be designed using accepted HFE methods and principles (see 5.2). This should include consideration of plant-specific standards and conventions. The impact of any new automation on the roles and responsibilities of the crew should be assessed and addressed in evaluation and training on the COPS.

The information displayed to the user should be formatted and structured so as to be readable and usable on the chosen display device(s). The user should have some control over font size, with a lower limit predefined. When font sizes are changed by the user, the information should automatically reformat to assure displayed information still fits the device screen width. If the text of a step does not fit on a single display screen, then continuous up/down scrolling should be available and obvious to the user. COPS 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.

The secondary task (i.e., interface management) interactions through which personnel interact with COPS 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.

Operating plants typically have existing engineering procedures and processes that address the HFE activities needed to support modifications impacting the control room. In addition, IEEE Std 1023™ provides guidance on an acceptable HFE design and evaluation process that is applicable to new plant designs. NUREG-0700 [B13] provides HFE review guidelines for COPS, and EPRI 3002004310 [B8] provides design guidance for COPS. The latter two documents contain guidelines that are specific to COPS, but they also contain related guidelines that may be applicable to various aspects of COPS, such as display design, user interaction and interface management, alarms, automation, and soft controls.

C.2 Active steps

Within a procedure that is open for use on COPS, the “active step” (see Clause 3) is a status marker indicating which steps are presently selected by an authorized operator of COPS for evaluation and possible execution. The effect of making a step “active” will depend on the particular design of the COPS (see 5.3). However, the following general characteristics are consistent with the intent of this guide and are expected to be broadly typical.

a) One function served by the active step is to support place-keeping in the procedure. Being able to identify which step is active allows a user of COPS to look elsewhere (either within or outside the current procedure) without losing his current place in a given procedure. Similarly, observers of this activity can identify the current location in the procedure, which has direct implications for plant status and operation.

b) Another function served by the active step is to indicate, with respect to the COPS itself, which step is selected, so that inputs to and outputs from the COPS application will be appropriately performed, with regard to the selected step. This is not unlike the function served of a typical cursor in many human-computer interfaces. Items a) and b) together will be considered to characterize the "primary" active step.

c) It may also be desirable for primary active steps to indicate to which COPS user they belong, i.e., which operator has made the step active.

d) When procedure-based automation is used, the primary active step will be advanced within sequences as part of the automatic COPS processing.

e) A single procedure may have more than one active step at a given time. To permit this without undermining the functions of the primary active step, it is likely that more than one type of active step will be defined within a COPS design. For example, so-called continuously applicable steps that are monitored for some period after being made active have a different set of functional requirements, in terms of their active status, than a typical (i.e., not continuously applicable) step. Marking their sequential position in the document may be of little importance, while identifying which of these steps are currently active (being monitored for possible execution) is the key concern. The different types of active steps should be presented so as to prevent any confusion between them.

f) To support the parallel execution of multiple procedures, active steps must exist and be tracked concurrently in multiple documents. For these purposes, it may be desirable for COPS to handle procedure attachments as separate but linked procedures in terms of active step tracking and functionality.

g) Even if attachments are treated as separate procedures, it may further be desirable to display multiple primary active steps in a single procedure or attachment, to support multiple authorized users working in parallel. Notwithstanding the likely challenges this would present, such an implementation would need to ensure that multiple primary steps could be reliably distinguished by users, by observers, and by the COPS itself.

h) Following completion of a step (i.e., evaluation through execution), the primary active step remains active while it is selected as such, i.e., until the next step is selected for evaluation and possible execution, or the procedure is closed.

C.3 Remote viewing

Multiple views of the active procedure(s) in the control room allow the shift supervisor and other operators to be aware of and support ongoing plant operations.

Remote viewing of COPS procedures (see 5.3), including active procedures, may be desired for alternate work locations such as the Technical Support Center (TSC) and Emergency Operations Facility (EOF). The COPS designer may need to consider cybersecurity issues.

Type 1 COPS should be able to be viewed from multiple work locations as well, but these procedures have limited functionality. There may be no linkage/coordination between displays of the procedures at different work locations.

C.4 Application of procedure-based automation by Type 3 systems

Following the principle that the operator should always be in command, the use of procedure-based automation (see 5.5) is always discretionary. The operator decides whether to execute a step sequence automatically or to execute the procedure steps manually. In addition, procedures or operating plans that depend on procedure-based automation for successful completion are specifically not recommended.

Operators are ultimately responsible for the safe operation of the plant. Accordingly, automation and its interfaces should be designed to permit personnel involvement and possible intervention and overriding of the automation. To this end, procedure-based automation defines the systematic use of hold points and sequence interrupts.

The interaction between the automation, operators, procedures, and training should be designed such that the communications between automation and the operators is well understood. The design of the automation should be as logical and intuitive as possible and match operator expectations of how the system functions. Restricting COPS evaluation and automatic step execution to simple, deterministic logic, similar to that performed manually by operators, ensures that COPS behavior is fundamentally predictable.

The system should provide information to enable the operators to determine the current status of automated processes and to evaluate progress toward achieving the goal of the procedure. For an automated sequence of actions, COPS therefore should indicate the specific sequence of steps that the automation will follow and the current status of steps (within an active or immediately pending sequence of steps), including the location of hold point(s) and the current mode of execution.

Information on current plant conditions and equipment status should be provided to permit operators to determine whether the automatic execution of a procedure is proceeding as expected. The way in which the displays present information should support the timely assessment of the automation's progress. For example, if the automation is changing a measured value over time, then the information can be displayed using a graph that shows both the current trend and the target value. 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 purpose of the current sequence of automated steps is to line up a plant system, then progress toward completing the lineup can be monitored, for example, by following the active step through the automated sequence, while observing component states and parameter values on the corresponding system display.

COPS should not only indicate when multiple steps are being performed concurrently, but also make the status of those steps readily available. This is true for concurrent step sequences, for continuously applicable steps, or for initial conditions being monitored across multiple steps. When parallel paths are being followed concurrently (e.g., two legs of an EOP flowchart), the system should provide the progress and current status for each concurrent path. Similarly, when multiple procedures are being executed simultaneously, the system should provide the progress and status of each procedure. For these situations, the system developer needs to consider issues such as the number of monitors available, information overload, clutter, and the need to prioritize displays.

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.

C.5 Soft controls

Soft controls in general, including those integrated with COPS, should be designed and evaluated using accepted HFE methods and principles (see 5.4). NUREG-0700 [B13] provides design review guidelines for soft controls. The guidelines in NUREG-0700 are applicable to soft controls in general, including controls that may be provided as part of COPS.

EPRI 3002004310 [B8] 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 COPS.

Soft controls are most often accessed from process- or system-graphical displays or other displays that provide information on the system and specific equipment to be manipulated. This helps provide context for the operator when using the control. Similarly, when soft controls are accessed through COPS, 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 COPS through links that allow the operator to readily access and display the needed information while using the control or made available through existing control room displays.

The characteristics and behavior of embedded soft controls should be compatible between the COPS and the plant control system. The embedded soft controls do not need to be "identical" to soft controls for the plant control system, but rather "compatible." Compatible elements should complete the same function, with no differences or conflicts that could lead to an error.

Information needed to support effective use of embedded soft controls, such as the plant and equipment status, should be available at the point of use. This guidance can be met by a variety of methods, from having automatic display of associated information, to providing information on a nearby display.

C.6 Hold points

For procedure-based automation, a hold point defines the end of a sequence of steps that can be automatically executed (see 5.5.3).

Automatic execution serves to reduce the human attention and effort that are otherwise needed to reliably perform a defined task sequence. When the operator initiates automatic execution, task control is allocated to the COPS for the duration of the sequence, and the operator assumes a supervisory role with respect to the COPS.

While the sequence is automatically executing, operator attention to the direct control of process steps is typically not required until the next hold point is reached, whereupon operator input is required to continue. Explicit hold points are part of the approved and controlled procedure contents that enable the use of procedure-based automation.

By comparison, each step in a conventional procedure has an implicit hold point, because the operator will actively advance to each successive step, or the execution of the procedure will stop. These implicit hold points are not a literal feature of such procedures (unless, perhaps, elaborated with specific notes or cautions) but the implicit function—that the procedure continues only at operator discretion—is the universal default practice.

This guidance in this document, therefore, concerns only explicit hold points for procedure-based automation. Hold points should be explicit, in this case, because the automatic execution of multiple steps effectively *removes* the "implicit" hold points of a manually advanced procedure. Hold points are thus a basic device by which procedure developers and users will manage the use of procedure-based automation capabilities.

This discussion may also clarify the role of temporary hold points that can be inserted by the operator prior to executing a sequence. Note that "temporary" means only that hold points inserted in a working procedure application by the current user will not be retained in the approved procedure when the application is closed. Since, in a conventional procedure, operators implicitly have the discretion to hold at any step, inserting a temporary hold point will be a normal act of supervisory control when using procedure-based automation.

A hold is needed in order to reinforce operator cognizance of procedure and process status. Hold points should be provided where:

a) Critical tasks are required, which includes upcoming decisions or actions that could involve a risk to plant and personnel safety or investment protection, and operator involvement in deciding whether to move forward would be expected to significantly reduce the risk

b) Reactivity management is required

c) Cautions and warnings are provided

d) 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)

e) The step involves a subjective evaluation that necessitates operating crew involvement. For example, 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.

f) The step requires authorization from a crewmember

g) Actions taken at the next step could impact compliance with operating limits (e.g., the plant Technical Specifications)

h) Transition points between process modes or phases of operation

i) It is desirable to mark the start or finish of discrete phases in a procedure

j) It is desirable to evaluate, confirm, or acknowledge conditions

k) Continued execution of the procedure is indicated

A required hold point ideally should define a sequence that has a meaningful operating basis and an appropriate length to support intermittent supervision. Appropriate length should consider both elapsed time and number of steps. In defining sequences during procedure development, hold points should be used as needed, but not excessively. Frequent, unnecessary hold points will be inefficient and frustrating to users, diminishing the benefits of automation and possibly discouraging proper supervision of the system.

C.7 Operator initiated halts/Sequence interrupts within Type 3 COPS

Being in command does not necessarily mean that the crew 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 should 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 predefined 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 should the need arise.

Operators should be able to interrupt an automated sequence at any time (see 5.5.4), prior to reaching a predefined hold point. In addition, the automated system should halt the 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:

a) The automation has reached a hold point. These are predefined 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 "calculated" hold point—the logic for the hold point is still predefined, but the time at which it occurs may not be fixed.

b) The operator interrupts the sequence. This may occur at any point in the sequence, as determined by the operator at the time.

c) 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.

The COPS should provide a means for the operator to interrupt an automatic sequence at any procedural step. In response to an interrupt command by the operator, the COPS should provide a safe and effective transition from automatic to manual mode. This may require that the control system complete part or all of a step before turning over control to the operator. For example, the COPS may initiate a signal to open a valve, and the operator determines that this action should not occur. The operator can initiate an interrupt to stop COPS processing, but the valve will still open. The operator may close the valve after the interrupt stops COPS processing.

After interrupt, the operator can look forward and backward in the procedure and have all the maneuverability within the procedure as available prior to the halt.

For manual interrupts, 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. The operator should not have to necessarily complete the remainder of the steps manually.

The COPS should support operator awareness of the goal of the sequence. This understanding should support personnel in deciding whether to authorize or direct the automation to begin. If the purpose of the automation is to execute a predefined 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.

COPS 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. Automation should assist the operator in safely and effectively completing a procedure but should not take away the operator's decision-making authority. The operator is always the final authority. Deviations from procedures should be logged for historical purposes. Logging of deviations can provide information to help identify potential improvements to procedures or training.

C.8 Training

There are many existing regulations and guidance documents on operator training. Issues related to the use of COPS by operations personnel are discussed here to supplement existing guidance.

Training should reinforce the role of crewmembers as the supervisors and managers of COPS.

Operator training on use of COPS should emphasize the importance of employing a questioning attitude and should reinforce the need to monitor the processing performed by COPS and to override the COPS if required.

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

For Type 3 COPS with automation, training should address how the operator interfaces with the automation and the appropriate conditions for automation.

Training should provide the operators with a thorough understanding of the COPS, the goals of each procedure, what information is processed and how, what actions it will take, and when it will terminate.

Crewmembers should have a good understanding of automation in order to properly manage it. The automation should follow the sequence of events as would be found in a PBP for the same task (i.e., the same sequence as would be manually performed). Lack of understanding of the automation increases the chance that operators will be surprised by the behavior of the automation or may provide inappropriate input to the automation.

Training should calibrate the operator's confidence in the automation, such that overreliance or underutilization of the automation is avoided.

Training should ensure that manual skills and proficiency are maintained so that crewmembers can effectively carry out procedure steps manually when needed. When operators 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. It is also important that COPS be specific and detailed enough to allow the operator to manually perform the step. In other words, the guidance provided is as important as the training on it.

Transition to backup PBP may also have implications for crewmember roles and should be addressed in crew training.

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

C.9 Transitioning between COPS and backup procedures

COPS are typically implemented using non-safety hardware and software, often using commercial off-the-shelf equipment. As stated in Clause 4, COPS can be used to implement the following types of procedures:

- Normal operating procedures (NOPs)
- Surveillance procedures
- Alarm response procedures (ARPs)
- Abnormal operating procedures (AOPs)
- Emergency operating procedures (EOPs)

COPS implemented as non-safety-related systems cannot be credited in the safety analysis. Backup procedures required for accident mitigation and safe shutdown should be provided as PBPs or on a safety- related system. (See 5.5.)

Backup procedures should be presented in a manner that is compatible with the presentation of the same procedure on the COPS 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 can be implemented in paper form, or on an alternative platform that may not have the same range of capabilities as the COPS 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 COPS 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 COPS. Aids to transitioning to the alternate procedure should be provided. This is especially true when the method employed in the COPS cannot be duplicated in the alternate method. These aids may be in the form of procedure formatting or embedded in the COPS design.

Examples of formatting aids include:

- Place-keeping aids
  - Check boxes in COPS similar to PBPs (e.g., grease pencil markings)
  - Step numbering
- Similar formatting and layout of COPS and PBPs
  - Use of capitalization
- IF…THEN direction

Examples of aids for transition include:

- System health indications
  - The system health indicator could be a system heartbeat indicator on the screen that could be used to inform the operator the system is not frozen. Also, the system health indicator could be a connection indicator that would be used to make the operator aware the COPS is connected to the plant control and information systems network.
- Automatic printout of COPS
  - A printer could be used to automatically print out currently active or in-process procedures. With the printout, the operator would have access to hard copies of active procedures that would include indication of procedure status and completed steps.

For Type 2 or Type 3 COPS, when a system failure or degradation occurs that requires transition to a backup procedure, the operator should be able to determine the following:

a) What procedures were being executed at the time of failure

b) Which step in each procedure was being processed at the time of failure

c) What conditions or steps, if any, were being continuously monitored by the COPS at the time of failure

Operators should be trained to recognize the potential failure modes and degraded conditions of COPS to facilitate their timely transitioning to backup procedures.

This information is required for the operator to be able to make an orderly transition from the failed COPS to the backup procedure. For example, the COPS might automatically store a status summary or snapshot on a regular basis in a form that would remain available after COPS failure, so 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.

Upon transition to a backup procedure from a Type 2 or Type 3, the operator should be able to continue the procedure at a point that is as close as possible to where COPS 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.

Normally the operator would continue the procedure at the point at which the COPS 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 undesirable results). In addition, starting over may cause significant delay in completing safety actions and thus potential for deteriorating and possibly unsafe plant conditions. At the time of failure, the operating crew may need to determine the best procedure step at which to resume.

C.10 Quality assurance

The quality assurance activities (see 5.7) 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:

- Risk significance of the procedures and potential risk impact of failures in COPS
- Complexity of the hardware-software system
- Operator verifications, cross-checks, and confirmations that will be performed during procedure execution that help detect and mitigate effects of COPS errors or failures.

These issues are more systematically addressed by IEEE Std 1012™. Clause 4 of IEEE Std 1012 describes four levels of software integrity based on the severity of anticipated consequences that could result if software fails to execute correctly. Software integrity level is then used to guide the identification of appropriate software QA/V&V activities throughout the software life cycle.

Which software integrity level may apply to a given COPS design depends on the design itself. However, for a COPS design that otherwise meets the guidance of the present document, it may be reasonable for a Type 1 COPS to address level 1 software integrity guidance and a Type 2 COPS to address level 2 software integrity guidance. For a Type 3 COPS, a software integrity level of 2, 3, or 4 may be reasonable, depending on the COPS design and the operating procedures that it may be used to execute.

When procedures are implemented on a platform (hardware and software) that is not safety-related, appropriate IEEE standards for isolation between systems should be consulted. See IEEE Std 603™ and IEEE Std 7-4.3.2™ for additional guidance.

In many cases, COPS will be developed on non-safety-related platforms. Any communication between COPS and safety-related equipment (e.g., data, commands) should be through appropriate gateways. 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 [B3].

COPS are either part of, or are interfaced with, the control and information systems used by the operators to monitor and control the plant. Quality assurance goals, such as redundancy, single-point failure protection, heartbeat, and so forth should be considered. The guidance provided applies to implementation of COPS on non-safety hardware/software platforms.

C.10.1 Type 1 system guidance

For Type 1 COPS, the computer system should be subject to administrative controls suitable for systems that manage data. 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.

C.10.2 Type 2 system guidance

For Type 2 COPS, a process to identify risk significance can be developed to determine the level of rigor of the QA/V&V activities undertaken to demonstrate adequate quality of the hardware and software of the COPS. Additional criteria apply due to the additional functionality provided and the potential for errors in the system, which can lead to errors in procedure execution.

C.10.3 Type 3 system guidance

For Type 3 COPS, additional criteria apply related to automation and inclusion of hold points in automated sequences.

The complexity and risk associated with failures in COPS, which are important factors in determining the level of hardware and software QA/V&V requirements 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.

If the COPS have 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.

C.11 Data integrity

COPS should use validated data for display of process information, step processing, and automation (see 5.8). All data for display should be validated where practicable on a real-time basis as part of the display to control room personnel. For example, redundant sensor data may be compared, the range of a parameter may be compared to predetermined limits, or other qualitative methods may be used to compare values.

C.12 Maintenance and configuration management

The COPS should provide the operator with the capability to identify errors and potentially fatal flaws discovered in its content (see 5.9). This may be accomplished by providing capability to record notes and issues associated with specific procedure steps within the COPS procedure file. The system may also be designed to provide some type of "flag" to indicate procedural issues when the procedure is accessed in the COPS. Control of procedures with errors should follow the site administrative process for procedure control and revision.

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

This is relatively straightforward for Type 1 COPS, which display replicas of PBPs on the computer screen with little additional functionality. It becomes more challenging for Type 2 and Type 3 COPS, 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, which thus should be controlled by the plant's engineering change control process.

Means should be provided to ensure adequate V&V of changes made to Type 2 and Type 3 COPS. The COPS may provide tools that assist with V&V. (IEEE Std 1012™ should be followed for software V&V.) For example, manual changes to Type 2 COPS 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 COPS.

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

The COPS may provide tools for maintaining consistency between COPS and associated backup procedures—for example, a tool that automatically generates new PBPs as backup procedures whenever the COPS is modified, or a tool that automatically generates COPS 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 COPS, or vice versa.