Interim Staff Guidance
Human Factors TWG 5
Computerized-Based Procedures and Soft Controls

NUREG-0700, Section 8 currently contains guidance regarding the review of Computer-based procedures (CBP). NUREG-0899, Guidelines for the Preparation of Emergency Operating Procedures lays the foundation for all emergency procedure development. Both should be referenced extensively in the review of a computer-based procedure system.

Other references, including NUREG/CR-5228, Techniques for Preparing Flowchart-format Emergency Operating Procedures, contain relevant procedure guidance that can be utilized or generalized for the review of computer-based procedures.

The focus of existing guidance is chiefly directed for the review of Emergency Operating Procedures (EOPs). This Interim Staff Guidance (ISG) is generalizable to any procedure type that is presented on a video display unit (VDU).

The term Paper-based procedure (PBP) is meant to refer to all procedures that are printed on a media such as paper or other material, in text, graphic or flow-chart format.

General

Computer-based procedures were developed to assist personnel by computerizing paper-based procedures. The purpose of a CBP is to guide operators' actions in performing their tasks in-order-to increase the likelihood that the goals of the task are safely achieved (NUREG-0700, Section 8).

For operations procedures presented in the Main Control Room (MCR) computer-based procedures should be designed as an integral part of the Main Control Room. The design of CBPs should include function analysis and function allocation to determine the procedure system's level of automation. CBP can be designed to include very little automation, no more than words presented on a VDU. CBPs can be designed with much higher levels of automation, including the ability to monitor plant parameters and prompt for control actions.

Procedure automation should always provide some benefit for the procedure user, not just the procedure writer or the document control clerk. The procedure user should always be in control of the procedure system. The computer system should be designed to provide the user with enough information for the user to know they are in control of the procedure system (as well as in control of the plant – Main Control Room operations). This can be achieved irrespective of the level of automation by developing system and task design that ensures the human operator is in command, involved in ongoing operations, and appropriately informed to maintain awareness of the situation and other status of automated functions.

When used, automated functions should be predictable, offer the user an appropriate range of options, monitor operator actions to minimize, resist, and tolerate errors, and be capable of being overridden by the user.

Criteria

Automation

Automation should not select the procedure to be used. For operations procedures, the operator is responsible for selecting the procedure. A computer-based procedure system can recommend a procedure for use via simple menuing, prompts or other means and allow the operator to select a procedure. The CBP can act as a scheduler, as example, to prompt to perform routine surveillances.

The computer-based procedure system should not automatically initiate control actions. Particular plant systems should have automatic actuations, isolations, etc. built into their logic, the automatic control function should not be generated by the computer-based procedure system. The CBP system can prompt the operator to take a specific action. The licensed operator, with full knowledge of the plant situation, is responsible to take or not take an action (update to NUREG-0700 Section 8, Introduction) (see also the Soft Control/Display Objects section of this ISG).

The computer-based procedure system should not be persistent to the point of not allowing the operator to bypass a step, interrupt a sequence of steps, or stop a procedure as appropriate (see also the Situation Awareness section of this ISG).

The operator should have an easy means, at any time, to transition to a menu to select a procedure.

Computer-based procedures should not be dynamic. This means the procedure should not change based on plant conditions. The computer-based procedure should be written and verified in its entirety, per station procedure, prior to being turned over to the respective user group. (See also the section on Mode Errors of this ISG.)

Procedures of a certain type, annunciator, normal, EOP should be written to the same level of automation.

Procedures of a certain type should be presented consistently across various display media; as example, EOPs should not be presented as text on a CBP and as flowcharts in a backup.

Readability (also refer to NUREG-0899, Section 5.3)

It is well discussed in scientific literature that reading text from a computer screen provides poorer reading speed and comprehension than reading from paper. It is important that all computer based procedures be written and formatted to be readable and usable on the display devise of choice.

Examples of display devices include desk-top computer, lap-top computer, hand-held computer, etc. Existing NUREG-0700 criteria, including screen resolution, character font and other display parameters should be considered to optimize the readability of the procedure on the screen size being used for procedure presentation.

If the procedure is presented on more than one page then continuous scrolling is required. (Some document processors and document formatters do not always scroll continuously, instead they jump from one page to the next, thereby increasing the likelihood that a procedure step should be missed.)

Only up/down scrolling is permitted. Left/right scrolling is not permitted.

Computer-based procedures should have provisions for place keeping. (NUREG-0899, Section 5.5.4)

Computer-based procedures that include data sheets should provide a method for data entry; else, rely on paper based data sheets.

Revising Computer-Based Procedures

Computer based procedures should include a means to document procedure steps the licensee wrote as commitment to NRC so the step should not be changed or eliminated without proper review. However, identification of such steps should be very subtle or invisible to the user since they are primarily meant to inform the procedure writer(s), reviewers, and approvers.

A revised computer-based procedure should be written and verified, per station procedure, prior to being turned over to the respective user group. Draft versions of procedures should not be accessible to users on their normal interface.

Mode Errors

Mode errors occur when there is a lack of knowledge and understanding about the current and future state and behavior of the automation. Mode errors should be reduced by limiting the number of modes a computer-based procedure system can have (NUREG-0700 Section 7.3-1). Guidance for limiting computer-based procedure modes follows:

- Computer-based procedures should not be dynamic. Procedure steps should not change once written and approved. (Without going through the appropriate procedure revision process.)
- Computer-based procedures should be written and verified with support from the appropriate target audience.
- Procedures of a particular set should be written to the same level of automation.

Automated CBPs should give indication to the user when the procedure steps are continuing in a loop. Certain procedures have loops built into them, the reasons why the procedure is in a loop should be made obvious to the user.

Cross-referencing procedures

[Follow the guidance of NUREG-0899 Step 5.2.2.] In addition to NUREG-0899 guidance, a CBP that references a second procedure is considered to be the "source" procedure. The referenced procedure is considered to be the "target" procedure.

Target procedures can be accessed through the use of a hyper-text link. When utilized, the target procedure should present all identifying information to the user such that the user has unambiguous knowledge that the displayed procedure is truly the target procedure. (See NUREG-0700, Section 8, Introduction, section titled: "Procedure Identification Information" for a list of identification information.)

Other high level data (meta-data) need not be presented to the user. The CBP should provide a means to access all meta-data. Examples of meta-data can include: author, plant name, Unit, type of procedure, etc.

Version control
The CBP system should always present the most recent version of a procedure to the user.

Display devices
Emergency operating procedure display devices should be functionally dedicated. Normal operating procedures can be presented on a multi-use display device (update to NUREG-0700, introduction p334).

Modernization
When implementing a CBP into a Main Control Room via a modernization project, the HSI conventions should include local standards that are in-place at the site where the Computer-based procedure should be implemented. Failure to understand these local conventions can result in conflicting sets of mental models and lead to an operational error.

Situation Awareness
All computer based procedures should provide the user with a minimum set of information to allow the user to know the state of the plant as appropriate to the procedure.

As example:

- The Procedure title should be continuously displayed on the screen at all times (NUREG-0700 8.1.6-5).
- The status of high level procedure goals should be continuously presented (NUREG-0700 8.1.6-5).
- Each procedure should be organized into sections of related steps (NUREG-0700 8.1.5-2). Additional information such as Section titles can be presented to provide the user with context (NUREG-0899, Section 5.5.7).
- If one procedure is entered via a reference from another procedure that reference should be presented on the screen (NUREG-0899 Section 5.4.4)
- EOP entry conditions should be continuously displayed at all times (NUREG-0700, Section 8.1.1-6).
- EOP immediate operator actions (if any) should be presented following the entry condition and acknowledged by the operator (reference NUREG-0899, Section 5.4.6).

- Operator decision points: (reference: NUREG/CR-5228 Section 5.3.1, Section 6.4.1, Section 6.4.2)
    - Should be written in the form of a question.
    - May have graphical elements associated to distinguish decisions from action statements.
    - Should provide the operator with the ability to provide input
    - Should provide the operator with feedback regarding which alternative was selected.
    - Constitute a CBP hold point.
- Steps in the procedure that include Cautions or Warnings should constitute a hold point and require operator action to proceed (update of NUREG-0700, Section 8.2.2-8).
- Verification steps are used to ensure that objective(s) of a task or sequence of actions has been met (reference NUREG/CR-5228 Section 13.2.1 see additional guidance here as well).
- If the CBP is such that conclusions or recommendations are presented, the CBP should provide easily retrievable information regarding how it reached its conclusions.

Backup procedures

On the loss of a CBP the crew should transition to a backup. The backup can be PBP or a CBP on a safety related platform.

The user should enter the back-up procedure at the Step 1 of the procedure, including any Cautions, Warning or additional information prior to Step 1 (update to NUREG-0700 item 8.5-3).

Full sets of back-up procedures should be maintained to ensure the ability to perform all emergency operating procedures and safety-related functions, including support and annunciator procedures.

Backup procedures should be available to those who need them in a manner and location that is timely for their use.

Backup procedure sets are subject to the same procedural controls as the primary procedure system, and should be maintained consistent with each other.

Emergency operating procedures

If emergency operating procedures (EOP) are designed to include automation the following guidance is appropriate. The CBP should:

- Inform the operator when presenting concurrent steps, such as steps in two different legs of a BWROG flowchart EOP.
- Inform the user of "Result Not Obtained" (RNO) and present contingency actions.
- Monitor procedure entry conditions, cautions, warnings, branches, and exits.
- Be integrated with alarms, system status (RG1.47), and critical safety functions (SPDS).

Additional EOP guidance:

- Continuously applicable steps should be identified to the operator.
- Concurrent use of multiple procedures should be addressed.

Hold points

Hold points are defined as predetermined pauses in the prosecution of a CBP requiring user permission, by way of an explicit control action, to direct the CBP to proceed. It is understood that an operator can manually insert a CBP hold point at any time.

A summary of hold points described other places in this document include automatically stopping the procedure and alerting the user for permission to proceed when:

- Unvalidated or Invalid data is the only type of data the CBP has available.
- A caution or warning is present at the procedure step ready to be executed.
- Procedure steps that require the operator to make a decision.
- As part of good operating practice to ensure the user maintains situation awareness.

Additionally:

- Any procedure step that requires operator input.
- Upcoming decisions or actions could involve a risk to plant safety, personnel safety or investment protection, and operator involvement in deciding whether to move forward would be expected to significantly reduce the risk.
- A manual operator action or verification is needed e.g. where the CBP does not have access to the needed information or there is significant judgment or cross-checking required to make an informed decision.
- The next step requires a peer check.
- Actions taken at the next step could impact compliance with plant Technical Specifications.

Quality

The qualification of the software used to implement a CBP needs to be commensurate with the complexity and safety of the procedures.

Soft controls

Soft controls are expected to be integrated into the design of some computer-based procedure systems. Current guidance provided in NUREG-0700 Section 7 should be followed. This ISG should reiterate, clarify, update and add new guidance. Existing NUREG-0700 criteria should be referenced.

Display Objects

Soft controls are the "display objects" that are programmed to have control functions. Soft controls are computer-based. A physical hand switch that operates a digital signal is not considered to be a soft control. A keyboard is a hard control (update to NUREG-0700, Section 8, Introduction).

Examples of soft controls are hyper-text links, text entry boxes, drop down lists, graphic pushbuttons, scroll bars (soft slider), radio buttons, etc. Soft controls come in many shapes and sizes. As example, current day word processing software contains toolbars, some with dozens of soft controls. Common word processor soft controls include controls to save a document, spell check a document and to change the font. It is recommended that CBP soft controls be limited in number and type. And that if new controls are designed, the graphic is representative of the function it performs.

Soft controls have a single control function. Control functions include "start pump," "close valve," "open breaker," "throttle-open valve," etc. Navigation (clicking a hyper-text link) is a control function.

Different soft control functions require different numbers of human actions to initiate the soft control function. Clicking a hyper-text link (navigation, either between a CBP or within a CBP) requires only one control action. To control plant equipment the operator should be required to take at least two actions. Throttling a valve can require numerous actions, usually more than two, to achieve the desired valve position vis-à-vis the parameter controlled.

Vendors and/or Licensees should develop writer's guides that precisely define the number of actions required to operate a particular control to achieve a particular control function. Existing NUREG-0700 guidance should be followed.

Soft control behavior

Soft controls have behaviors, in that they change based on how they are acted on. As example: a pushbutton can darken when "depressed." These behaviors provide needed feedback to the user regarding the state of the control.

Soft control behavior should not violate behavior of hard control stereotypes, especially in Main Control Rooms that are partially modernized.

Soft controls in and of themselves should not be indicators of system or parameter status.

Soft controls should not initiate an action until the physical control action is completed. As example, discussion of a mouse pointer:

- if a pointer is positioned over a control, the control should change to indicate it is now the "focus" of the potential action
- If the left mouse button is depressed and released the control action should be completed and the action initiated.
- If the pointer is moved off the control before or during the mouse button release, the control action should not take place.

For touch screens, the control action should not take place until the finger is lifted from the object. If the finger is slid to a different part of the VDU, the control action should not be initiated. (See NUREG-0700, Section 7, pages 339-340.)

Interface management versus operational controls

Interface management soft controls should be unique from operational soft controls.

Interface management soft controls should not have component or system level control function capability. As example, a menu can be used to select a procedure but not to start a component or system.

Confirmations

When a CBP includes soft controls, the HSI should provide clear indication of system response. Multiple indications of system response are sometimes appropriate for presentation. When starting a pump: amps, flow, level, discharge pressure, etc. may all be appropriate for presentation depending on the purpose of the control action (See NUREG-0700, Section 7 page 339 "Monitoring Control Feedback" for additional information. Also, item 7.3.1-7).

Monitor, minimize, resist and tolerate human actions

CBPs that allow users to perform control functions should enable automated monitoring of the operator action to confirm the action is consistent with the procedure step. This can be performed by way of using verification steps (NUREG-0899, Section 5.7.2)

If the action taken is not consistent with the intended step the procedure system should stop at the step in question and provide clear feedback regarding how the action was, potentially, incorrect and recommend a path forward. If the operator confirms the action taken was correct, the CBP should tolerate the input and continue. (The CBP should log the input.)

If appropriate, a procedure change request should be initiated.

Hyper-text links

Guidance regarding hyper-text links is found in NUREG 0700, Section 2. Guidance regarding Operator Aids is found in NUREG-0899, Section 5.2.3. Additional information is found below.

Hypertext links are not meant to disrupt the flow of the procedure but to enhance the information available to the operator by linking to supplementary information.

Target pages are the pages that are displayed when a hypertext link is utilized. Target pages should open in a new "window" or dedicated screen area. Multiple windows should not open to obscure an existing window. Windows should contain an imbedded control to allow the operator to close the window.

Target pages should have titles that correspond one-to-one with the hyper-text link name.

If the ability exists to select multiple parameters for display in different windows, the parameters should be able to be organized per the user's preference, in one or multiple windows. The information should not obscure nor be obscured by other displayed information.

If one procedure links to another such that the second procedure should be singularly prosecuted until completion (task or entire procedure) the second procedure can open full screen at the target step.

- When linking procedures of this nature remember to link to applicable Notes, Cautions and Warnings that may be prior to the procedure step in question.
- Use "breadcrumbs" at the top of the window to show the operator the path that is being taken from procedure to procedure.
- Only the last procedure in the series can be dismissed. In other words, the last one opened is the first one closed.

Data Validation

Existing guidance regarding invalid and unvalidated data is referenced below. Where new information is presented it is identified as such.

NUREG-0700

1.1-23 Indication of Display Failure

Information system failures (due to sensors, instruments, and components) should result in distinct display changes, which directly indicate that depicted plant conditions are invalid.

Additional Information: The information system should be designed so that failures in instrumentation are readily recognized by operators. When panel instruments, such as meters, fail or become inoperative, the failure should be apparent to the user (e.g., through off-scale indication). This may be more difficult to determine in complex graphics, and thus, should be carefully evaluated.

New: a means other than color change should be used to indicate VDU displayed information has failed.

1.4-9 Invalid Data

Variables that are subject to validation (e.g., checks for accuracy) should be identified and an indication should be provided when these data are invalid.

Additional Information: When data fails to meet the specified criteria for validity and thus is suspected of being of poor quality, an indication of validation failure should be provided.

New: when invalid data is encountered by a CBP the procedure step should not be automatically completed. A hold should be placed on the prosecution of the procedure until the operator has the ability to validate the parameter information and manually continue the procedure. A method for continuing the procedure should be presented to the operator.

1.4-10 Unvalidated Data

When checks for accuracy could not be performed, the unvalidated status of the data should be clearly indicated.

Additional Information: When checks for accuracy cannot be performed (e.g., a processor or redundant sensors are not available) the data is unvalidated. (Unvalidated data may be determined to be either valid or invalid as a result of the data validation process.) Under some conditions, unvalidated data may be useful to trained users in determining the safety status of the plant and determining whether human intervention is needed. Clear indications of the data's unvalidated status should be provided so the user can exercise judgment in interpreting it.

New: when unvalidated data is encountered by a CBP the procedure step should not be automatically completed. A hold should be placed on the prosecution of the procedure until the operator has the ability to validate the parameter information and manually

continue the procedure. A method for continuing the procedure should be presented to the operator.

1.4-11 Data Entered by Personnel
Data entered by personnel should be identified such that it is easily distinguished from sensor data or validated data.

5 SAFETY FUNCTION AND PARAMETER MONITORING SYSTEM

Failure indications address the ways in which the user is informed of the presence of potential failures or malfunctions in the system. These indications aid the user in identifying and diagnosing failures. Data validation techniques are used in plant I&C systems to assess the validity of plant data by comparing the data from different sources. Data that pass the test are said to be valid (i.e., of reliable quality), while data that fail are determined to be invalid (i.e., not reliable and possibly indicative of a system malfunction). Data that cannot be tested, such as when processors or redundant data are not available, are said to be unvalidated (i.e., of unknown quality). Analytical redundancy refers to one method for testing the validity of data. It is the intercomparison of measured variables, through the use of mathematical models based upon known physical relationships among variables. Another method of data validation is the direct comparison of values from redundant sensors. Guidelines for reliability, test, maintenance, and failure indication features are given in Section 5.3.

5.3-1 Display Reliability
The display should not give false indications of plant status.

Additional Information: Both the processing of display information and the display device should be highly reliable. The operating and failed states should be indicated to users as described in NUREG-0800, Section 1.1-23.

5.3-2 Data Reliability/Validation for Critical Plant Variables
Critical plant variables should be reliable and should be validated in real time.

Additional Information: There are several methods of ensuring that critical variables are reliably presented to the operators. These methods should be used as appropriate to achieve a high data quality and veracity. Lack of data validation places the burden of identifying valid readings on the operator. One method of achieving this would be to have an estimate of data quality and a data quality indicator associated with each critical variable, including derived synthetic variables. Other recommended methods include: range checks for failed instruments; comparison of redundant sensors; and analytical redundancy.

Range checks for failed instruments can ensure that failed instruments are identified and that they are not averaged with other, valid readings, possibly masking the failed instrument. Comparing and possible averaging redundant instruments can improve the quality and reliability of data. Analytical redundancy refers to the intercomparison of measured variables, through the use of mathematical models based upon known physical relationships among variables to determine whether there are inconsistencies in the values of the measured variables. For example, 'reactor power,' 'reactor coolant temperature rise through the reactor core,' and 'reactor coolant flow rate' are interrelated variables based upon the physical principles of heat transfer. A measured value for

coolant flow should be consistent with the analytically calculated value for coolant flow derived mathematically from the corresponding measured values of reactor power and coolant temperature rise.

5.3-3 Display of Data Reliability/Validation for Critical Plant Variables
The status of the data should be displayed to the operator with an appropriate data quality indicator (e.g., valid, invalid, or unvalidated; or a derived numerical estimate). *Additional Information:* Operators should also have available (e.g., on a separate display page) the individual sensor readings, so they can pinpoint an indicated problem, if the validation fails.

NUREG-0696:
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 quantitative methods may be used to compare values. When an unsuccessful validation of data occurs, the SPDS should contain means of identifying the impacted parameter(s). Operating procedures and operator training in the use of the SPDS should contain information and provide guidance for the resolution of unsuccessful data validation. The objective is to ensure that the SPDS presents the most current and accurate status of the plant possible and is not compromised by unidentified faulty processing or failed sensors.

NUREG-0835
- Validated, unvalidated, and invalid data should be identified, and be distinguishable from each other.
- Coding of invalid data should be distinct from the coding of data that has not been successfully validated.
- Procedures and training should be provided for guiding operators in the treatment of invalid data, and the resolution of unsuccessful data validation.