

EPRI 1015312/MPR-3092

Revision E
July 2008

Deleted: Revision D

Deleted: June 2008

A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP Software Common Cause Failure

Deleted: 7-19

EPRI Document 1015312

Prepared for

Nuclear Energy Institute/Industry Representatives and Highly Integrated Control Room - Human
Factors Working Group

A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP Software Common Cause Failure

EPRI 1015312/MPR-3092

Revision E

July 2008

Principal Contributors

R. Alvarado
D. Blanchard
R. DeWeese
R. Fuld
C. Kerr
J. Konefal
F. Quinn
K. Scarola

Deleted: *A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP Software Common Cause Failure*

Deleted: *A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP 7-19 Software Common Cause Failure*

Inserted: *A Methodology to Determine the Acceptability of Manual Operator Actions Response Times for a BTP Software Common Cause Failure*

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

Deleted: July 2008

Inserted: July 2008

Deleted: June 2008

Prepared for

Nuclear Energy Institute/Industry Representatives and Highly Integrated Control Room -
Human Factors Working Group

Contents

1 Introduction 1-1

1.1 Background..... 1-1

1.2 Purpose 1-1

1.3 Historical Crediting of Manual Operator Actions 1-2

2 Methodology..... 2-1

2.1 Analysis 2-2

2.2 Verification 2-6

2.3 Validation 2-7

2.4 Human Performance Monitoring 2-8

3 Conclusion 3-1

Deleted: 1 . Introduction . 1-1¶
 1.1 . Background . 1-1¶
 1.2 . Purpose . 1-1¶
 1.3 . Historical Crediting of Manual Operator Actions . 1-2¶
2 . Methodology . 2-1¶
 2.1 . Analysis . 2-2¶
 2.2 . Verification . 2-6¶
 2.3 . Validation . 2-6¶
 2.4 . Human Performance Monitoring . 2-7¶
3 . Conclusion . 3-1¶

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

1

Introduction

This white paper recommends a methodology to determine the acceptability of manual operator response times to be used in Diversity and Defense-in-Depth (D3) evaluations for new plants and existing plant modifications.

1.1 BACKGROUND

This white paper provides industry recommendations to address Problem Statement 5 from Task Working Group (TWG) #5, Highly Integrated Control Room – Human Factors (HICR-HF):

Manual Operator Actions: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

Note that HICR-HF Problem Statement 5 was previously addressed as Problem Statement 2 within TWG #2, Diversity and Defense-in-Depth (D3). However, this problem statement was moved to TWG #5 in November of 2007 by the USNRC Steering Committee for further resolution. It is currently planned for TWG #5 to provide guidance on this Problem Statement in July of 2008 for industry comment and October of 2008 for industry and Staff use.

Deleted: May

Deleted: July

1.2 PURPOSE

The purpose of this white paper is to define a methodology, applicable to both existing and new plants, for evaluating the acceptability of manual operator action as a diverse means of coping with Anticipated Operational Occurrences and Postulated Accidents (AOO/PA) that are concurrent with a software Common Cause Failure (CCF) of safety related digital systems. This software CCF is discussed in the Background of Branch Technical Position (BTP) 7-19, (March 2007) *Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer - Based Instrumentation and Control Systems*:

Deleted: bility to credit

Deleted: the Reactor Trip System (RTS) and/or Engineered Safety Features Actuation System (ESFAS)

“Digital instrumentation and control (I&C) systems can be vulnerable to common-cause failures caused by software errors, which could defeat the redundancy achieved by hardware architecture.”

To provide additional guidance for BTP 7-19, the U.S. NRC staff for TWG #2 provided Digital Instrumentation and Controls Interim Staff Guidance (ISG), DI&C-ISG-02, Revision 1 in September of 2007. Pages 1 through 4 of DI&C-ISG-02 specifically discuss (1) Adequate Diversity and (2) Manual Operator Actions.

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

This white paper supports the ~~recommendation~~ by the industry for development of an alternate ISG by TWG #5:

Deleted: following change

Deleted: ed

Manual operator actions taken from the Main Control Room (MCR) are acceptable for **abnormal operational occurrence or plant** accident mitigation **concurrent with a BTP 7-19 software common cause failure**. The actions should be based upon, and ultimately included within, the licensee's EOPs. A methodology may be employed to determine whether the time required for operating crews to take manual actions in response to a BTP 7-19 software CCF is less than the time available. The time available is based upon best estimate¹ thermal-hydraulic analysis and the acceptance criteria of BTP 7-19. The time required is determined by **Diversity and Defense-in-Depth (D3) and** Human Factors Engineering (HFE) analysis. Validation should be performed by use of a part-task/limited-scope simulator or the reference plant simulator, which accurately represents the events for which manual operator actions are credited, in real time.

This paper provides a methodology for the HFE analysis, the verification, and validation techniques **for BTP 7-19 software common cause failure scenarios** recommended by industry. This methodology is recommended for incorporation into additional staff guidance for this area.

Analysis, verification, and validation performed in accordance with this methodology may demonstrate that manual operator actions are not acceptable in response to a variety of BTP 7-19 software CCFs concurrent with an AOO/PA. In these instances, diverse automation may be required for coping with the BTP 7-19 software CCF.

1.3 HISTORICAL CREDITING OF MANUAL OPERATOR ACTIONS

There are numerous instances where manual operator actions are credited in the safety analyses of existing operating units for response to an AOO/PA. The specific instances and operator action times will vary depending on the individual plant licensing basis. Operator action times and their bases are typically discussed in the context of the individual design basis safety analyses within the Final Safety Analysis Report (FSAR), e.g., Chapters 6, 15, and 19. Typical examples include:

- Switchover from Emergency Core Cooling System (ECCS) injection mode to recirculation mode in response to a loss-of-coolant accident (LOCA);
 - Depending on plant design and the size of the LOCA, this could be expected to occur within 30-minutes after event initiation.
- Boron dilution during shutdown;

¹ For the purposes of this document, best estimate means that analytical estimates are realistic and reflect a best estimate of real time plant response and personnel behaviors, based upon experience, training, operation, design, analytical iteration, and engineering principles. Best estimate also means that undue conservatism has not been applied to analysis to accommodate severity factors, but that appropriate conservatisms are applied for an infrequent, beyond-design-basis BTP 7-19 software CCF condition. Concurrently, best estimate does not mean that all conservatisms are removed or minimized from analysis, or that the initial or continuing conditions of the event under analysis are optimal.

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

- If operator action is used to mitigate the boron dilution event, the Standard Review Plan states that there should be 15-minutes available for an operator to take action from the time that an alarm is received until there is a loss of shutdown margin.
- Inadvertent ECCS actuation at power;
 - In this event, the concern is that the pressurizer fills to the point that there is water relief from the Code safety valves, causing a valve to stick open and resulting in a LOCA. The operator actions would be to identify and terminate the event, or alternately make a power-operated relief valve available for water relief. The action time would be on the order of a few minutes, possibly less than 10-minutes depending on the licensing basis.
- The following major operator actions are typically modeled in the Steam Generator Tube Rupture (SGTR) event;
 - Operators must first identify and isolate the ruptured generator. This has to take place in minutes following initiation of the event. Depending on the plant-licensing basis, it would typically be less than 30-minutes.
 - Next, operators will cool down the RCS to establish subcooling margin. This facilitates RCS depressurization, which in turn reduces break flow from the primary to the secondary. Again, depending on plant licensing basis, this will occur in minutes.
 - After cooling to establish RCS subcooling margin, the RCS will be depressurized to reduce the break flow and restore inventory. This will also take place in minutes.

The previous actions have established adequate RCS subcooling, verified a secondary side heat sink and restored the reactor coolant inventory to ensure that safety injection (SI) flow is no longer needed. SI can then be terminated. This series of manual actions mitigate the primary to secondary break flow. This happens in minutes.

In addition, the following items are examples of current licensing bases crediting manual operator actions at times less than 30-minutes after event initiation:

- Loss of subcooled margin requires manual trip of Reactor Coolant Pumps in less than 15-minutes and manual control of Emergency Feed Water for natural circulation in less than 30-minutes.
- Manual reactor trip for some ATWS events is required in less than 15-minutes.
- LOCA scenarios credit operator actions in less than 15-minutes to prevent High Pressure Injection pump runout.

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

- Manual start of Emergency Feed Water is credited in less than 15-minutes for High Energy Line Break events.
- MSLB/MFLB events credit operator actions to isolate the effected SG and to trip the reactor in less than 15-minutes.
- Low Temperature Over-Pressurization events credit operator actions in less than 15-minutes.

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

2

Methodology

During performance of the D3 coping analysis, it may be determined that crediting manual operator actions to cope with software common cause failures should be considered. If so, then implementing a methodology to determine the acceptability of manual operator action response times would be required. If this analysis is performed, then the D3 coping analysis submitted for U.S. NRC review should include a discussion of attributes described in NUREG-0711 for the justification of operator actions that are credited for response to an AOO/PA concurrent with a BTP 7-19 software CCF in a safety related digital system. The methodology for this justification is the key subject of this white paper.

Deleted: T

Deleted: the RTS or ESFAS

For manual operator actions credited in the D3 coping analysis for response to an AOO/PA, the applicant should demonstrate that the Human Systems Interface (HSI) to be used by the operators for prompting and taking actions is unaffected by the BTP 7-19 software CCF. The HSI (devices and procedures) that support credited manual actions should be designed in accordance with accepted Human Factors principles and guidelines, including required HFE design attributes and approved plant training programs. Guidance for demonstrating acceptable HSI is provided by DI&C-ISG-02, as well as other regulatory documents, and is outside the scope of this white paper.

To credit operator actions for the purpose of coping with an AOO/PA and a concurrent BTP 7-19 software CCF, the applicant should follow a four-step approach:

1. Analysis
2. Verification
3. Validation
4. Human Performance Monitoring

The methodology described in this white paper is based upon operator actions that are directed by procedures. The crediting of these operator actions should be discussed as early as practical in licensing submittals. However, it is recognized that these procedures are often not available until late in the design process. Therefore, the analysis to credit these operator actions should be based upon a documented sequence of operator actions that is essentially equivalent to an operator procedure. The documented sequence of operator actions should be verified by use of the EOPs when they become available. If the EOPS are significantly different than the documented sequence of operator actions used for the D3 and HFE analysis, then the D3 and HFE analysis should be re-performed. EOPs should be used in the Validation and Human Performance Monitoring Process (Sections 2.3 and 2.4).

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

The **D3 and** HFE analysis and validation should be based upon the Operations Department Staff that is reasonably expected to be in the MCR for a BTP 7-19 software CCF, considering the frequency of AOO/PAs and the expected duration for each differing MCR staffing level. The MCR Operating Staff size used for analysis and validation may be the same as the minimum MCR Staff defined in the plant's Technical Specifications. However, if a minimum MCR Staff is expected infrequently and for a limited duration, then a larger crew size may be justified for analysis and validation purposes. The assumptions and bases for the MCR crew size used for **D3 and** HFE analysis should be documented and consistent with the HFE staffing analysis described in the plant licensing basis. Using the reasonably expected MCR crew size for this analysis is consistent with the best estimate analysis methods allowed by BTP 7-19 and consistent with the training practices for operating crews.

If credited manual actions require additional operators beyond those reasonably expected to be in the MCR, the justification for this additional staffing should be provided in the HFE analysis. This justification should also include any time duration requirement for availability of additional personnel.

2.1 ANALYSIS

This section describes the method of analysis used to justify that the required manual operator actions can be performed within the time available for AOO/PAs with concurrent software CCFs, so that these manual actions may be credited in the D3 coping analysis.

To assure the acceptance criteria of BTP-19 is achieved, the analysis must demonstrate that the time AVAILABLE to perform manual actions, based on the thermal hydraulic analysis of plant AOO/PA response, is greater than the time REQUIRED for the operator(s) to perform the action, based upon an HFE analysis of operator response time. The thermal hydraulic methodology for determining the time AVAILABLE is beyond the scope of this white paper. However, the thermal hydraulic analysis should be discussed in the D3 coping analysis. The methodology provided in this white paper may be used to determine the time REQUIRED for manual operator action in response to an AOO/PA concurrent with a BTP 7-19 software CCF.

In determining the time REQUIRED for operator action, the applicant should consider two methods of AOO/PA coping:

- Conventional EOP Recovery
- Special Event EOP Recovery

Applicants may use either or both recovery methods. The applicant's operator response time analysis should show that, for the AOO/PA being analyzed concurrent with a BTP 7-19 software CCF, the documented sequence of operator actions directs operators to the recovery method that achieves the credited operator response.

Conventional EOP Recovery

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

EOPs typically require routine confirmation of expected RPS/ESFAS automation, and normal emergency procedure contingency actions will lead operators to manually initiate these functions. For example, the first step in a typical top level EOP is “Verify Reactor Trip”, and the first contingency action is “Manually trip reactor”. Therefore, maintaining the conventional method of emergency response, even with a software CCF, may be appropriate for designs where the software CCF has minimal impact on the HSI needed to execute the conventional EOPs, and the time AVAILABLE is sufficient to reach the mitigating action(s) in the time REQUIRED for the normal execution path through the EOPs.

Deleted:

Special Event EOP Recovery (from a BTP 7-19 software CCF)

For designs where the Diverse Actuation System (DAS) is blocked by the normal actuation of the primary protection system, an alarm that shows the DAS has taken some automatic action would be one example of a prompt that is unique to software CCF conditions.

Another example would be a process alarm, such as high-high pressure, that indicates a plant condition that could never be reached unless there was a software CCF in the RPS.

Under all conditions, entry to the EOPs will require an operator prompt. However, unique prompting alarms may be desirable to ensure timely recognition of the software CCF and quickly direct the operators to the appropriate EOP or a specific mitigating action within the Emergency Procedure. Therefore, unique prompting alarms can be effective in reducing the time REQUIRED to reach critical mitigating actions.

Deleted: U

As with other high order alarms in the Control Room, unique prompting alarms will be derived from the sensing of plant process parameters and will not be derived from the sensing of software conditions. Use of high order alarms to direct operator action in the Control Room is well established for conditions indicative of an anticipated transient without scram (ATWS), a reactor trip, a turbine trip, and various other priority plant conditions. In keeping with this established practice, the unique prompting alarms will be treated as highest order alarms, directing the operator to action or confirmation of a specific condition which could indicate a BTP 7-19 software CCF condition.

Unique prompting alarms will be designed as the highest priority alarms with unique human factors aspects for high salience such as distinct location, unique alarm sound, or unique color. Unique prompting alarms will also be designed to minimize the occurrence of spurious alarms.

Unique prompting alarms must alert the operator to plant conditions indicative of a BTP 7-19 software CCF concurrent with the AOO/PA so as to prompt a procedurally unique and unambiguous action by the operator.

Response to unique prompting alarms will be followed by performance of a Special Event EOP Recovery and then performance of detailed procedural symptom based recovery.

Deleted: ¶

Deleted: For designs where the Diverse Actuation System (DAS) is blocked by the normal actuation of the primary protection system, an alarm that shows the DAS has taken some automatic action would be one example of a prompting alarm that is unique to software CCF conditions. Another example would be a process alarm, such as high-high pressure, that indicates a plant condition that could never be reached unless there was a software CCF in the RPS.¶

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

For each AOO/PA the applicant should document the basis for crediting the unique prompting alarm. This should include justification that the software CCF does not affect the alarm, and justification that the alarm is directly correlated to the desired procedurally unique operator response.

Unique prompting alarms should be processed and displayed by equipment that is diverse from the postulated software CCF. In addition, the alarm processing design should minimize the potential for spurious alarms that could prompt erroneous operator actions (e.g., two separate alarms or instrument channels). The D3 coping analysis should include justification that the potential for spurious alarms has been minimized. Alarm diversity and alarm processing are I&C design issues that are outside the scope of this white paper.

Applicants should account for the possible loss of computerized procedures (if determined to be needed by the D3 coping analysis) due to the software CCF and the required use of backup procedures not subject to the software CCF for either Conventional or Special Event EOP Recovery analysis.

For either method of recovery, the time REQUIRED to perform manual actions should be estimated using analytical methods explained below, as based upon those described in ANSI/ANS-58.8, with consideration for best estimate methods permitted by BTP 7-19 for this beyond design basis event:

1. **Indication** - The time interval between the start of an AOO/PA and the first indication of the AOO/PA to the plant operator. If a unique prompting alarm is credited in the analysis, then this alarm is considered the first indication of the AOO/PA.
2. **Diagnosis** - The time interval between the first indication of the AOO/PA and the earliest time for which credit can be taken for initiation of a safety-related operator action.

- Conventional EOP Recovery

The minimum diagnosis intervals defined by ANSI/ANS-58.8, Table 1, are based upon the likelihood of occurrence of FSAR design basis events (DBEs) and are consistent with the conservatism expected for plant FSAR safety analysis. During this interval, the operator verifies automatic responses, observes plant parameters, and plans subsequent actions in response to the DBE.

- Special Event EOP Recovery

For designs that rely on a unique prompting alarm, EOPs and training should enforce a single unambiguous operator action in response to a unique prompting alarm. The appropriate trained response to a unique prompting alarm does not require diagnosis. Training frequency for the corresponding AOO/PA(s), although the BTP 7-19 Software CCF is postulated as an infrequent event, will meet or exceed training

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

frequency for PC-2 DBEs. The operator responds to prompting as trained so that the diagnosis time interval is reduced to zero in the analysis of the time REQUIRED.

3. **Operator Action** – The time interval for operator action, a component of the total time REQUIRED, is calculated as the sum of the fixed sub-interval and a variable sub-interval per ANSI/ANS-58.8, Section 4.2. The fixed sub-interval allows time for (1) the receipt of prompting information that identifies the need for action, and (2) the identification of appropriate action. The variable sub-interval is based upon the number of discrete manipulations that comprise the appropriate actions.
4. **Manipulation** - The time required to complete a single operator action. ANSI/ANS-58.8 “allows a minimum of one minute for each discrete manipulation required to complete a single operator action”.

ANSI/ANS-58.8 does not clearly define “discrete manipulation” or “single operator action”. For this, ~~the analysis may be initially constructed by assuming a one minute interval for each set of monitoring actions or control actions that are functionally grouped, or grouped through their HSI. This initial construction of one minute intervals should be followed by an informed process to refine the manipulation intervals. This process would include the participation of operators, technical experts, designers, and human factors experts and require analysis of the manipulation intervals to include such considerations as HSI layout and performance, real-time equipment performance, human reliability, and control room environmental factors. The final analysis submitted for verification should reflect these and other reasonable considerations for realistic manipulation intervals and should be achievable in the time REQUIRED.~~

Deleted: best estimate analysis of

Deleted: should be applied

Deleted: to

~~The following examples are provided as guidance for defining discrete manipulations. However, the HFE analysis should provide justification for the consideration of any multiple monitoring or control actions credited as a single manipulation:~~

Deleted:

- An EOP step for activating a flow path, which requires opening a suction valve, opening a discharge valve and starting a pump, would be considered one manipulation if all of the controls are grouped on a single screen or well defined section of a conventional control panel. Alternately, each control would be considered a separate manipulation if the operator would need to navigate a screen not well defined for abnormal operation, navigate to multiple screens, or work at multiple panel sections to take the action. Certain control actions may need to be considered as separate manipulations, requiring consideration of the actual time interval to account for real time operation of the equipment (e.g., long valve stroke times).
- An EOP step for monitoring a critical safety function would be considered one manipulation if all required indications are presented on a single display or well-defined section of a conventional control panel, with clearly marked abnormal conditions. Alternately, monitoring each process parameter would

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

be considered a separate manipulation if the operator would need to navigate to multiple screens or multiple panel sections to obtain the information, if there are no clear markings for abnormal conditions, or it is required to consider the actual time interval for real time operation of the equipment (e.g., slowly changing process variables with no trend indications).

- For the unique prompting alarms discussed in Item 2 above, analysis may credit a single manipulation if the alarms are on the same screen or on the same panel section. However, if the operator must navigate to multiple screens or multiple panel sections, confirming each alarm would be considered a separate manipulation.
- A decision node or confirmation in the manipulation phase would be considered a single manipulation and would not be considered diagnostic time.

This guidance is only applicable to manual actions taken from the plant MCR. As discussed in ANSI/ANS-58.8, all credited manual actions required in 30-minutes or less should be capable of being performed in the MCR. The D3 coping analysis should justify any operator actions credited outside the MCR, including consideration of time constraints, equipment accessibility, and personnel hazards. Guidance for credited actions taken outside the MCR is beyond the scope of this white paper.

Based upon the guidance above, which is based upon realistic assumptions and consistent with best estimate analysis methods, the calculation methods of ANSI/ANS-58.8 should be used to determine the earliest time following an AOO/PA at which credit can be taken for the initiation of an operator action. The complete D3 coping analysis, which provides time AVAILABLE and time REQUIRED and includes a discussion of the HFE program as it supports this analysis, should be submitted for U.S. NRC review.

2.2 VERIFICATION

The analysis of the time REQUIRED to perform a documented sequence of manual operator actions should be confirmed by use of a table top design and a walk-through/talk-through verification. The personnel responsible for verifying the analysis should be different than the persons responsible for the analysis. Undocumented assumptions and analytical methods that may be obvious to the preparer(s) of the analysis are likely to be less so to individuals who are not familiar with the analysis.

Table top verification should be rigorous and conducted by operators, system technical experts, and human factors experts. These personnel should be instructed to verify that the analysis is logical for its purpose, contains a sufficient level of detail (including adequate notes), and presents no physical or spatial difficulty for performance. The language and the level of information presented in the documented sequence of manual operator actions should be compatible with the minimum number, qualifications, training, and experience of the operating staff.

Deleted: for

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

Operators and system technical experts should be instructed to ensure that the documented sequence of manual operator actions, independent of time REQUIRED, is technically correct and will achieve the desired technical result(s).

Walk-through/talk-through verification should be conducted by operators, designers, system technical experts, and human factors experts. These personnel should be instructed to verify the correspondence between the documented sequence of manual operator actions and the existing or planned displays and controls to be used by the operator, including correspondence in labeling, units of measure, and operation of controls. Walk-through of displays and controls for existing plants should be conducted in both the Reference Plant Simulator and the Reference Plant to ensure fidelity. Walk-through/talk-through of planned displays and controls for new plants should be conducted to the extent practical, according to the state of the design and supplemented as necessary by use of such aides as arrangement diagrams, vendor drawings, and panel fabrication drawings.

The documented sequence of operator actions should also be verified by human factors experts to be written in accordance with the governing procedure writers' guide.

The analysis of the time REQUIRED to perform individual steps and the overall documented sequence of manual operator actions should be verified to be reasonable, realistic, repeatable, and bounded by the analysis documentation.

The verification of the analysis of the time REQUIRED for the documented sequence of manual operator actions should have a formal mechanism for feedback such that results, including any problems identified during the verification, are brought to the attention of the developers of the analysis and management for the responsible operations department and design organization.

Verification results should be documented and provided for U.S. NRC review during the license application or amendment process. Verification results should be such that there is high confidence that the time REQUIRED for performance of the documented sequence of manual operator actions will be well within the time AVAILABLE.

Deleted: available

2.3 VALIDATION

The Validation of the time REQUIRED to perform the documented sequence of manual operator actions should be conducted using a Part-Task Simulator, a Limited-Scope Simulator, or the Reference Plant Simulator in real time. Operating crews should walk through and execute the documented sequence of manual operator actions. This validation should be documented as an Inspections, Test, Analyses, and Acceptance Criteria (ITAAC) for plants licensed under 10CFR 52 or as a License Condition for operating plants. Walk through of the manual operator actions for existing plants should confirm correspondence between the Reference Plant and the Reference Plant Simulator. This walk through should also address any differences between the Reference Plant and the Reference Plant Simulator. Various types of personnel should be involved in the validation process. The applicant should measure operator response times (PERFORMANCE times) of at least three (3) available licensed operating crews in

Deleted:

Deleted: To perform this validation, t

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

representative event simulations. **The operating crews should be observed while performing the procedures by technical experts and human factors experts.**

The Simulator must be capable of real time, high fidelity plant simulation for the BTP 7-19 software CCF concurrent with an AOO/PA with operator manual actions are credited. The simulator must also accurately represent the HSI available and the postulated HSI failure(s) for the software CCF condition. The PERFORMANCE time will be compared to the time AVAILABLE (thermal hydraulic analysis result) and time REQUIRED (HFE analysis result from the Section 2.1 analysis).

Deleted: here

Deleted: then

The use of a Part-Task Simulator or a Limited-Scope Simulator is consistent with the guidance of ANSI/ANS-3.5, *Nuclear Power Plant Simulators for Use in Operator Training and Examination*, Appendix D, Guidance on Part-Task and Limited-Scope Simulator Features and Fidelity.

The validation acceptance criteria for the validation data are as follows. For each AOO/PA, the mean PERFORMANCE time of all measured crews should be less than or equal to the time REQUIRED. In addition, the PERFORMANCE time for each crew should be less than the analyzed time AVAILABLE. These criteria are consistent with best estimate methodology discussed in Point 2 of BTP 7-19.

Acceptable validation results will provide the basis for meeting license application or amendment request approval requirements of the NRC staff. Unacceptable validation results will require modification of the D3 coping strategy. For example, a modified strategy might consider different prompting setpoints or prompts from different plant parameters, so as to allow more time for operator action. Another modified strategy might consider procedures that are more efficient in reaching the credited mitigating action.

Deleted: alarm

Deleted: ing alarms

Deleted: that would

If a successful manual action strategy cannot be achieved, diverse automation will be required. Modification to the D3 coping strategy will require reanalysis, resubmittal for USNRC Staff review, and revalidation.

The validation of the analysis of the time REQUIRED for the documented sequence of manual operator actions should have a formal mechanism for feedback such that results, including any problems identified during the validation, are brought to the attention of the developers of the analysis and management for the responsible operations department and design organization.

Deleted: .

2.4 HUMAN PERFORMANCE MONITORING

Licensees should include ongoing operator training and Human Performance Monitoring on the Plant Reference Simulator for all operating crews to maintain operator skills in performing **credited manual operator actions for AOO/PAs and concurrent CCF conditions**

Operator training frequency for Special Event EOP Recovery should be performed to meet or exceed training frequency for PC-2 DBEs. Although the BTP 7-19 Software CCF is postulated as an infrequent event, training simulations for the concurrent AOO/PA with a frequency

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D

appropriate for PC-2 DBEs is intended to ensure that operator response to the BTP 7-19 software CCF concurrent with an AOO/PA is prompt and unambiguous.

Training should also be provided to design organization personnel for the purpose of understanding the critical link between manual operator actions performed in response to a BTP 7-19 software CCF and the plant equipment used to implement these actions. Configuration management should be implemented in the design organization to ensure formal control of the design process interface with the D3 coping analysis.

Classroom and Reference Plant Simulator training should ensure that trainees understand the philosophy behind the approach of the documented sequence of manual operator actions. The structure and approach to event mitigation, including control of safety functions, accident evaluation and diagnosis (for Conventional EOP Recovery), and the achievement of safe, stable or shutdown, conditions should be well understood by the trainees.

Human performance monitoring may include the use of seminars and workshops for the purpose of discussing human performance issues associated with manual operator actions credited within the D3 coping analysis for mitigating BTP 7-19 software CCFs.

Human performance monitoring for the documented sequence of manual operator actions should have a formal mechanism for feedback such that results, including any problems identified by the operating staff during operations or training are brought to the attention of the Reference Plant Operations Department management and the Design Organization. Annual operator surveys may be a practical method for encouraging this feedback.

Deleted: credited manual operator actions for AOO/PAs and concurrent CCF conditions.

- Deleted:** Revision E
- Inserted:** Revision E
- Deleted:** Revision D

3

Conclusion

This white paper provides a methodology to determine the acceptability for manual operator response times to be used in the Diversity and Defense-in-Depth (D3) coping analysis for design of a new plant and for a modification to an existing plant. This approach should be used to demonstrate that operator actions credited in the D3 coping analysis can be taken with high confidence of success.

Deleted: Revision E

Inserted: Revision E

Deleted: Revision D