**NRC Staff Comments on Manual Operator Actions White Paper.doc**

## Main document changes and comments

**Page 1: Comment [E1]** **End-user** **1/15/2008 8:41:00 PM**

It appears that the term “CCF” is used in a way that implies that CCF is always a computer interfaces failure. Does the method apply to all CCFs?

**Page 1: Comment [E2]** **End-user** **1/15/2008 9:22:00 PM**

This is the numbering that was used when Standard Review Plan (SRP) Chapter 7 was revised in 1997. The SRP was updated in March 2007. As part of this update BTP HICB-19 was updated and renumbered as BTP 7-19. It is not clear whether this white paper references the 1997 revision of the SRP or the March 2007 revision of the SRP. Please reference the 2007 revision of the SRP and update the white paper to include appropriate changes included in the March 2007 revision of the SRP.

**Page 1: Comment [E3]** **End-user** **1/15/2008 8:45:00 PM**

Consider making clear that paper applies to actions from control room.

**Page 1: Comment [E4]** **End-user** **1/15/2008 8:46:00 PM**

Consider making clear that actions must be included – not merely based on – EOPs.

**Page 1: Comment [E5]** **End-user** **1/15/2008 9:12:00 PM**

Explain why "best estimate" the appropriate analysis to use in this case versus "worst case," credible event?

**Page 1: Comment [E6]** **End-user** **1/15/2008 8:47:00 PM**

Will validation be conducted in real-time?

**Page 2: Comment [E7]** **End-user** **1/15/2008 9:29:00 PM**

This section does not describe a methodology, but a list of durations that may be the part of licensing bases of some operating plants.

**Page 2: Comment [E8]** **End-user** **1/15/2008 9:13:00 PM**

30’ or so from “what?” From time of event initiation, time of event indication?

**Page 2: Comment [E9]** **End-user** **1/15/2008 9:13:00 PM**

Is this minimum amount of time that must be available for an operator to take action or the maximum amount of time the operator has available to take action before loss of margin?

**Page 3: Comment [E10]** **End-user** **1/15/2008 9:15:00 PM**

Less than 30 minutes from what? Event initiation or event detection/indication?

**Page 3: Comment [E11]** **End-user** **1/15/2008 9:15:00 PM**

Less than 15 minutes from what? Event initiation or event detection/indication?

**Page 3: Comment [E12]** **End-user** **1/15/2008 9:15:00 PM**

What methodology should the applicant use to demonstrate that the HSIs are unaffected?

**Page 4: Comment [E13]** **End-user** **1/15/2008 9:16:00 PM**

If the purpose of this paper is to define a methodology for evaluating the ability to credit manual operator action as a diverse means of coping with Design Basis Events (DBE) that are concurrent with a common cause failure (CCF), what is the rationale for including the discussion in section 2.1, ACTIONS CREDITED FOR DESIGN BASIS EVENTS OR ATWS?

**Page 4: Comment [E14]** **End-user** **1/15/2008 9:30:00 PM**

Will the EOPs containing manual operator actions be available during the review of DCDs or COLs?

**Page 4: Comment [E15]** **End-user** **1/15/2008 8:48:00 PM**

Consider changing to minimum.

**Page 4: Comment [E16]** **End-user** **1/15/2008 9:17:00 PM**

Plant's, licensee's , or applicant's overall HFE Plan?

**Page 4: Comment [E17]** **End-user** **1/15/2008 9:33:00 PM**

Any application using this approach should include or reference this methodology and the results of the analyses.

**Page 5: Comment [E18]** **End-user** **1/15/2008 9:35:00 PM**

This seems to be contrary to symptom based EOPS.

**Page 5: Comment [E19]** **End-user** **1/15/2008 8:54:00 PM**

This assumes any failure of computerized HSI is a complete failure – this assumption may not be appropriate. Degraded conditions and partial CCFs needs to be considered.

**Page 5: Comment [E20]** **End-user** **1/15/2008 9:18:00 PM**

How "generalizable " is this terminology (ie., Optimal Recovery, Functional Recovery) and the associated mitigative philosophy to designs other than Westinghouse ? Is it intended that this methodology, based on the optimal and functional recovery strategy, be applied to LWRs only or other new plant designs as well?

**Page 5: Comment [E21]** **End-user** **1/15/2008 8:55:00 PM**

Consider emphasizing that actions need to be completed in available time.

**Page 5: Comment [E22]** **End-user** **1/15/2008 9:19:00 PM**

Not certain what is meant by this statement and the basis/rationale for making it.

**Page 5: Comment [E23]** **End-user** **1/15/2008 9:23:00 PM**

This discussion should be expanded to discuss Common Cause Failure (CCF) recognition and diagnosis time adjustments due to CCF. Loss of computerized procedures should also be included in time adjustments.

**Page 6: Comment [E24]** **End-user** **1/15/2008 9:00:00 PM**

The assumption that diagnosis is instantaneous does not seem realistic. For example, CCF w/DBE will cause an alarm cascade – detection & diagnosis will be delayed somewhat under these conditions.

**Page 6: Comment [E25]** **End-user** **1/15/2008 9:03:00 PM**

How will actual operating experience be considered, especially where actual experience indicates a longer time is more realistic.

**Page 7: Comment [E26]** **End-user** **1/15/2008 9:05:00 PM**

Confirmation should include real-time simulations.

**Page 7: Comment [E27]** **End-user** **1/15/2008 9:26:00 PM**

Confirmation results should be discussed in the application and available to the staff for review.

**Page 7: Comment [E28]** **End-user** **1/15/2008 9:19:00 PM**

Please explain the rationale for delaying the validation to "post license approval."

**Page 7: Comment [E29]** **End-user** **1/15/2008 9:20:00 PM**

Please clarify meaning of "all available qualified crews." Also, what's meant by "representative event simulations?"

**Page 7: Comment [E30]** **End-user** **1/15/2008 9:20:00 PM**

Please clarify the meaning of this sentence.

**Page 7: Comment [E31]** **End-user** **1/15/2008 9:08:00 PM**

Guidance should be included to address situations were the validation does not poduce acceptable results.

**Page 7: Comment [E32]** **End-user** **1/15/2008 9:10:00 PM**

Regulatory commitments seems inappropriate since this the manual operator actions is being credit for meeting regulatory requirements.

## Header and footer changes

## Text Box changes

## Header and footer text box changes

## Footnote changes

## Endnote changes

# Introduction

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

## 1.1 BACKGROUND

This white paper provides industry recommendations to address Problem Statement 2 from Task Working Group (TWG) #2 Diversity and Defense-in-Depth:

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

## 1.2 PURPOSE

The purpose of this white paper is to define a methodology for evaluating the ability to credit manual operator action as a diverse means of coping with Design Basis Events (DBE) that are concurrent with a common cause failure (CCF), as defined in Branch Technical Position (BTP) HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer - Based Instrumentation and Control Systems."

To provide additional guidance for this BTP, the U.S. NRC staff generated draft Interim Staff Guidance (ISG) entitled "DRAFT INTERIM GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER - BASED INSTRUMENTATION AND CONTROL SYSTEMS.

This white paper supports the following change recommended by industry for that draft ISG:

> Manual operator action is acceptable for accident mitigation. The actions should be based on Emergency Operating Procedures (EOPs). Best estimate analysis is used to demonstrate that the time expected for operator actions is less than the time available. The applicant should include a commitment for validating the analysis through use of a plant reference simulator.

This paper provides a methodology for the analysis and validation techniques recommended by industry. This methodology is recommended for incorporation into additional staff guidance for this area.

**Comment [E1]:** It appears that the term "CCF" is used in a way that implies that CCF is always a computer interfaces failure. Does the method apply to all CCFs?

**Comment [E2]:** This is the numbering that was used when Standard Review Plan (SRP) Chapter 7 was revised in 1997. The SRP was updated in March 2007. As part of this update BTP HICB-19 was updated and renumbered as BTP 7-19. It is not clear whether this white paper references the 1997 revision of the SRP or the March 2007 revision of the SRP. Please reference the 2007 revision of the SRP and update the white paper to include appropriate changes included in the March 2007 revision of the SRP.

**Comment [E3]:** Consider making clear that paper applies to actions from control room.

**Comment [E4]:** Consider making clear that actions must be included– not merely based on– EOPs.

**Comment [E5]:** Explain why "best estimate" the appropriate analysis to use in this case versus "worst case," credible event?

**Comment [E6]:** Will validation be conducted in real-time?

# Methodology

For purposes of the analysis, manual operator actions credited in the D3 coping analysis are divided into two categories:

- Actions Credited for Design Basis Events or Anticipated Transient Without Scram (ATWS)

- Actions Credited only for Design Basis Events with Concurrent CCF

The methodology to demonstrate the feasibility of credited actions is described separately for each category, as follows.

## 2.1 Actions Credited for Design Basis Events or ATWS

**Comment [E7]:** This section does not describe a methodology, but a list of durations that may be the part of licensing bases of some operating plants.

There are numerous instances where manual operator action is credited in the safety analyses, and the specific instances and operator action times will vary depending on individual plant licensing bases. These 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 and 15. 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 or so.

**Comment [E8]:** 30' or so from "what?" From time of event initiation, time of event indication?

- Boron dilution during shutdown;

  - If operator action is used to mitigate the boron dilution event, the Standard Review Plan states that there should be 15-minutes available from the time that an alarm is received until there is a loss of shutdown margin.

**Comment [E9]:** Is this minimum amount of time that must be available for an operator to take action or the maximum amount of time the operator has available to take action before  loss of 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 where manual operator actions have been approved to occur at times less than 30-minutes:

**Comment [E10]:** Less than 30 minutes from what? Event initiation or event detection/indication?

- 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.

**Comment [E11]:** Less than 15 minutes from what? Event initiation or event detection/indication?

- 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.

- 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.

If these same actions are credited in the D3 coping analysis, the applicant should demonstrate that the human systems interface (HSI) normally expected to be used by the operators in prompting and taking these actions is unaffected by the CCF. If the normally used HSI is

**Comment [E12]:** What methodology should the applicant use to demonstrate that the HSIs are unaffected?

affected by the CCF, the analysis should demonstrate the adequacy of alternate HSI and the basis for concluding there is minimal impact on operator actions and response time. If this cannot be demonstrated, or if alternate operator actions must be credited, the feasibility of these actions should be demonstrated by the methodology of Section 2.2, below.

The D3 coping analysis, which is submitted for U.S. NRC review, should include the justification of operator actions that are also credited for DBEs.

**Comment [E13]:** If the purpose of this paper is to define a methodology for evaluating the ability to credit manual operator action as a diverse means of coping with Design Basis Events (DBE) that are concurrent with a common cause failure (CCF), what is the rationale for including the discussion in section 2.1, ACTIONS CREDITED FOR DESIGN BASIS EVENTS OR ATWS?

## 2.2 ACTIONS CREDITED FOR DESIGN BASIS EVENTS WITH CONCURRENT CCF

To credit operator action that is only for the purpose of coping with a DBE and a concurrent CCF, the applicant should follow a three-step approach:

1. Analysis
2. Validation
3. Human Performance Monitoring

The credited operator actions should be specified in the EOPs. The analysis and validation should be based on the sequence of steps required to get to the mitigating action based on execution of the EOPs with normal Main Control Room (MCR) staff.

**Comment [E14]:** Will the EOPs containing manual operator actions be available during the review of DCDs or COLs?

**Comment [E15]:** Consider changing to minimum.

The HSI, including devices and procedures, that support credited manual actions are developed in accordance with the overall Human Factors Engineering (HFE) Program. This includes all HFE design attributes and plant training programs provided to enhance operator skills in responding to DBEs and concurrent CCF conditions.

**Comment [E16]:** Plant's, licensee's, or applicant's overall HFE Plan?

If credited manual actions require additional operators, the basis and justification for staff augmentation should be provided in the analysis.

### *2.2.1 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 DBEs with concurrent CCFs, so that these manual actions may be credited in the D3 coping analysis.

To ensure the acceptance criteria of BTP-19 is achieved, the analysis must demonstrate that the time AVAILABLE to perform manual actions, based on the best estimate thermal hydraulic analysis of plant DBE response, is greater than the time REQUIRED for the operator(s) to perform the action, based on an analysis of operator response time. The thermal hydraulic methodology for determining the time AVAILABLE is outside the scope of the I&C/HFE TWGs. This white paper only addresses the methodology for determining the time REQUIRED.

**Comment [E17]:** Any application using this approach should include or reference this methodology and the results of the analyses.

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

- Optimal Recovery
- Functional Recovery

Optimal Recovery, also referred to as event-based recovery, may be appropriate for designs where the CCF has minimal impact on the HSI, allowing no disruption (or minimal disruption) to the EOP execution path. Optimal Recovery requires prompting alarms for recognition of EOP entry conditions. However, for Optimal Recovery there is no need to include specific alarms for the CCF condition itself, since EOPs require routine confirmation of expected RPS/ESFAS automation and EOP 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."

**Comment [E18]:** This seems to be contrary to symptom based EOPS.

Functional Recovery, also referred to as symptom-based recovery, may be more appropriate for designs where the CCF adversely impacts the HSI that is needed for Optimal Recovery EOP execution. For these designs, unique prompting alarms should be provided to ensure timely recognition of the CCF. These alarms should be processed and displayed by equipment that is diverse from the postulated CCF. An alarm that shows the Diverse Actuation System (DAS) has taken some automatic action would be one example of an alarm, assuming the DAS actuation alarm is normally delayed and blocked if the normal RPS/ESFAS actuates correctly (ie. there is no prompting alarm to immediately transition to Functional Recovery procedures when there is no CCF). This unique CCF alarm would be an entry condition to the Functional Recovery procedures, which are based on monitoring and controlling critical safety functions through a minimum HSI inventory.

**Comment [E19]:** This assumes any failure of computerized HSI is a complete failure – this assumption may not be appropriate. Degraded conditions and partial CCFs needs to be considered.

**Comment [E20]:** How "generalizable " is this terminology (ie., Optimal Recovery, Functional Recovery) and the associated mitigative philosophy to designs other than Westinghouse ? Is it intended that this methodology, based on the optimal and functional recovery strategy, be applied to LWRs only or other new plant designs as well?

Applicants may use either or both recovery methods. The applicant's operator response time analysis should show that for each DBE the EOP directs operators to the recovery method that achieves the credited operator response.

**Comment [E21]:** Consider emphasizing that actions need to be completed in available time.

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

1. **Indication** - The time interval between the start of a Design Basis Event (DBE) and the first indication of the DBE to the plant operator.

   The best estimate (realistic assumptions) do not affect this time. For this analysis, the "first indication" is the alarm(s) discussed in the **diagnosis** section, below.

**Comment [E22]:** Not certain what is meant by this statement and the basis/rationale for making it.

2. **Diagnosis** - The time interval between the first indication of the DBE to the plant operators and the earliest time for which credit can be taken for initiation of a safety-related operator action.

   The diagnosis interval defined by ANSI/ANS-58.8 is consistent with the

**Comment [E23]:** This discussion should be expanded to discuss Common Cause Failure (CCF) recognition and diagnosis time adjustments due to CCF. Loss of computerized procedures should also be included in time adjustments.

conservatism expected for plant FSAR safety analysis. However, as explained above, operators are prompted to enter the EOPs by indications/alarms. If there are at least two separate alarms, to avoid operator consideration of erroneous alarm conditions, it is realistic to assume that operators can enter the EOPs with minimal time for event diagnosis.

In addition, for designs that rely on CCF recognition, the alarms should be unique to the CCF condition, and training should enforce one course of operator response action, which is to enter the Functional Recovery EOP. Based on these considerations it is realistic to conclude that the diagnosis time interval is equivalent to the **manipulation** time interval, explained below.

**Comment [E24]:** The assumption that diagnosis is instantaneous does not seem realistic. For example, CCF w/DBE will cause an alarm cascade – detection & diagnosis will be delayed somewhat under these conditions.

3. **Manipulation -** The time required to complete a single operator action. ANSI/ANS-58.8 "allows a minimum of one minute for each discrete manipulation".

   ANSI/ANS-58.8 does not clearly define "discrete manipulation" or "single operator action". For this, best estimate analysis of one minute should be applied to each set of monitoring actions or control actions that are functionally grouped and grouped through their HSI. The following examples are intended to clarify this guidance:

**Comment [E25]:** How will actual operating experience be considered, especially where actual experience indicates a longer time is more realistic.

   - 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 touch 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 to multiple screens or multiple panel sections to take the action.
   - 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 be considered a separate manipulation if the operator would have to navigate to multiple screens or multiple panel sections to obtain the information, or if there are no clear markings for abnormal conditions.
   - For the prompting alarms discussed in Item 2 above, a single manipulation would be considered 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, monitoring each alarm would be considered a separate manipulation.

   The above examples of single and multiple manipulations are provided only for guidance. The analysis should provide documented justification for considering any set of multiple monitoring or control functions as a single manipulation.

   This guidance is applicable only to manual actions taken from inside the Main Control Room (MCR). In accordance with ANSI/ANS-58.8 all credited manual actions required in 30-minutes or less should be capable of being performed in the

MCR. Guidance for credited actions taken outside the MCR is outside the scope of this white paper.

Based on the guidance above, which applies best-estimate (realistic assumptions), the calculation methods of ANSI/ANS-58.8 should be used to determine the earliest time following a DBE 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, should be submitted for U.S. NRC review.

The time REQUIRED for manual operator action determined using the analytical method described above should be confirmed using table top and proto-type walk-through, talk-through. Confirmation results should be documented and available for U.S. NRC audit during the license application review.

**Comment [E26]:** Confirmation should include real-time simulations.

**Comment [E27]:** Confirmation results should be discussed in the application and available to the staff for review.

### 2.2.2 Validation

Validation using the full-scope simulator will be a post license approval commitment (e.g., Inspection, Test, Analysis, and Acceptance Criteria (ITAAC) or condition of license for License Amendment Requests (LARs)). To perform this validation, the applicant should measure operator response times (PERFORMANCE time) of all available qualified crews in representative event simulations. The validation data will then be compared to the time AVAILABLE (basis) and time REQUIRED (result) of the Section 2.2.1 analysis.

**Comment [E28]:** Please explain the rationale for delaying the validation to "post license approval."

**Comment [E29]:** Please clarify meaning of "all available qualified crews." Also, what's meant by "representative event simulations?"

The evaluation criteria for the validation data are as follows. The mean PERFORMANCE time of qualified crews should be less than or equal to the time REQUIRED from the analysis for manual actions. In addition, the PERFORMANCE time for each crew should be less than the analyzed time AVAILABLE. These criteria are consistent with "best estimate" methodology.

The number of crews tested may be reduced based on the statistical consistency of the successive results. The minimum number of crews tested should ensure with 95% confidence that the true mean PERFORMANCE time of all available crews does not exceed the time REQUIRED. In addition, as discussed above, the maximum PERFORMANCE time of each crew tested should be within the time AVAILABLE.

**Comment [E30]:** Please clarify the meaning of this sentence.

Acceptable validation results will provide the basis for meeting the post license approval commitment.

**Comment [E31]:** Guidance should be included to address situations were the validation does not poduce acceptable results.

### 2.2.3 Human Performance Monitoring

Licensees should include ongoing operator training and Human Performance Monitoring to maintain operator skills in responding to DBEs and concurrent CCF conditions. This is a post license approval commitment.

**Comment [E32]:** Regulatory commitments seems inappropriate since this the manual operator actions is being credit for meeting regulatory requirements.