SUPPLEMENTAL INTERIM TECHNICAL GUIDANCE ON MAIN CONTROL ROOM ABANDONMENT ANALYSIS

GUIDANCE ON THE USE OF A GENERIC, SCREENING HUMAN ERROR PROBABILITY OF 0.1 FOR MAIN CONTROL ROOM ABANDONMENT (LOSS OF HABITABILITY)

1.0 INTRODUCTION

The analysis of fires inside the main control room (MCR) involves the sequential examination of individual fire scenarios. Each scenario first considers the success or failure of fire suppression. Successful fire suppression leads to limited habitability issues and does not lead to a demand for abandonment. This type of scenario is not addressed here since it can be modeled with typical Fire Human Reliability Analysis (HRA) considerations as described in NUREG-1921 (EPRI 1023001), "EPRI/NRC-RES Fire HRA Guidelines." MCR fires that are not suppressed result in fire damage (both fire-induced initiating events as well as fire damage to systems, structures and components [SSCs]). The impact of the unsuppressed fire on plant systems and functions is increased, and at some point MCR habitability is threatened. Those fires that lead to a demand for MCR abandonment due to loss of habitability (LOH) are addressed here.

For each scenario leading to a demand for abandonment, the PRA Standard requires consideration of human reliability cognition and execution. In particular, for LOH leading to MCR abandonment, failure to successfully achieve a state that avoids core damage, consists of

- The decision to abandon
- The actions needed for the transfer of control from the MCR to the remote shutdown panel(s) and local station(s) where shutdown actions will be performed
- The actions at the remote shutdown panel(s) and local stations associated with successful shutdown, including any required supervisory coordination and communication
- The functioning of the equipment required to successfully shutdown.

For LOH, it is assumed that there is no contribution from the failure to diagnose the need to abandon and then decide to abandon the MCR in time to execute a successful shutdown (i.e., the first bullet regarding decision to abandon is considered to always be successful).

2.0 PURPOSE

This guidance represents the result of an effort by the NRC, with significant support by the nuclear industry, in conjunction with the industry-proposed Fire PRA Frequently Asked Question (FAQ) 13-0002, "Modeling of Main Control Room (MCR) Abandonment on Loss of Habitability," to address a long-standing concern regarding the use of "screening" human error probabilities (HEPs) for modeling failure to successfully abandon the MCR due to fire in the MCR and transfer functions necessary to maintain safe shutdown capability to ex-MCR location(s). Previous guidance on "screening" exists in NUREG/CR-6850 (EPRI 1011989), "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Plants," and NUREG-1921 (EPRI 1023001), which cited use of a "generic" screening HEP of 0.1 from the Individual Plant Examination - External

Events (IPEEE) era as follows:

> *NUREG/CR-6850 suggests that the use of a single overall failure probability value to represent the failure of reaching safe shutdown using alternative means can be used if the probability value is evaluated conservatively and a proper basis is provided. It notes that this approach was used in several IPEEE submittals and that, in many cases, 0.1 was used as a point value estimate for the probability. Before crediting this approach, the analyst must have applied the criteria discussed in Section 4.3 [of NUREG-1921] for assessing the feasibility of the operator action(s) associated with that HFE. Additionally, Section 4.8 [of NUREG-1921] provides qualitative analysis considerations for modeling MCR abandonment. This approach may be sufficient for some applications, such as cases in which MCR abandonment is not demonstrated to be risk-significant. The analyst also has the option to use the scoping approach or a detailed analysis method, as discussed in the following sections [of NUREG-1921].*

FAQ 13-0002 is intended to be a comprehensive treatment of MCR abandonment due to untenable environmental conditions from fire within the MCR. There is also a need to address abandonment due to loss of control/function in the MCR from fires external to the MCR. However, this more complex issue remains for future development at this time. Meanwhile, licensees have been attempting to use the guidance cited above to employ "generic" screening HEPs of 0.1 for MCR abandonment due to untenable environmental conditions from fire within the MCR with mixed success. Therefore, both the NRC and nuclear industry saw the need for "initial" guidance solely for LOH on a more limited scale to address this concern, i.e., prior to completion of the more comprehensive treatment that will result from FAQ 13-0002.

This guidance represents the result of this effort. It is intended for immediate use by licensees for risk-informed applications involving HRA in Fire PRA solely for abandonment of the MCR due to LOH.[1] It is expected that this guidance will subsequently be incorporated into FAQ 13-0002 which, when completed, will supersede use of this guidance (although no substantive change is anticipated).

3.0 FEASIBILITY ASSESSMENT

Feasibility should be assessed as described in NUREG-1921. It is very useful for the PRA analysis to use the feasibility assessment conducted to satisfy the safe shutdown (qualitative) requirements for MCR Abandonment.

4.0 COMPLEXITY

Complexity is an important concept in NUREG-1921, being discussed explicitly as a performance shaping factor (PSF) in Section 4.6.4 and as an important input to HRA quantification using the scoping approach in Section 5.2. Complexity is discussed in other places in NUREG-1921 (e.g., Sections 4.8, 4.9, and 4.10), either explicitly or implicitly.

The concept of complexity also will be important in determining which safe shutdown strategies

[1] Abandonment of the MCR due to loss of control/functionality will remain to be addressed after completion of FAQ 13-0002 (unless this FAQ is expanded to include this as well).

following MCR Abandonment can be represented with the “0.1 Case” discussed in Section 5 below.

4.1 DEFINITION OF COMPLEXITY

The base definition of complexity provided in NUREG-1921 shall be retained here. The assessment of cognitive and execution complexity, for the purposes of evaluating safe shutdown strategies following MCR Abandonment, should follow the basic principles of assessment laid out in the discussion of the scoping approach in NUREG-1921 (Section 5.2) as further described below.

For cognitive complexity, the guiding principles that should be used are similar those in to the scoping approach, namely, low complexity can be assessed when:

- procedures match well with (i.e., are fully supportive of) the scenario
- operators have been trained (preferably more than classroom training) on the procedure and its actions
- cues, indications, and controls match well to the action requirements and associated procedures
- no coordination (e.g., time sequencing) is required for required action performance
- only limited communication is required for required action performance, such as verifications of action completion
- there is a single location for command-and-control (e.g., the remote shutdown panel)
- either all required safe shutdown actions are performed at a single, dedicated remote shutdown panel; or, if, in addition to the single remote shutdown panel, other locations are required, all safe shutdown actions are independent
- no other workload concerns exist

Similarly, for execution, low complexity can be assessed when:

- procedures match well with (i.e., are fully supportive of) the scenario, including appropriate details
- operators have been trained (preferably more than classroom training) on the procedure and its actions
- cues, indications, and controls (including the human-machine interface such as labeling, local feedback) match well to the action requirements and associated procedures
- no coordination (e.g., time sequencing) is required for required action performance
- communication is limited to reports back to command-and-control when an action is completed, and is supported by high quality equipment that allows for clear and unambiguous communication
- a single location is needed to complete the required action
- there are no workload concerns (e.g., absence of complicated or large numbers of steps to complete action)
- the required action does not involve control of a plant parameter

4.2 RELATIONSHIP BETWEEN OTHER PSFS AND COMPLEXITY WHEN COMMAND AND CONTROL IS LOCATED AT ALTERNATE SHUTDOWN PANEL(S)

When operators leave the MCR for the alternate shutdown panel(s) (ASP), there are several implications for this location shift of command and control with respect to cues and indications, communications, and workload. In particular:

a. with rare, if any, exceptions, the ASP will be limited, as compared to the MCR, with respect to the cues, indications, and controls available,

b. because of the limitations noted in (a), operator activities associated with detection and monitoring of cues and indications, and performance of actions, will be distributed between the ASP and other locations in the plant, requiring more and different types of communication than if all of these activities took place in the MCR,

c. when the operators leave the MCR, the operators "take the plant" with them to the ASP, including all of the requirements for communication with plant personnel (e.g., survey reports from health physics or radiation protection departments, plant managers requesting status updates) and outside organizations (e.g., the NRC, local and state governments), BUT without the same ability to filter or control this communication due to less staff and/or the configuration of the ASP.

All of the above contribute to a very different operating environment or context that contributes to an assessment of complexity, cognitive and/or execution. For example, the scoping approach for alternate shutdown in NUREG-1921 (i.e., the ASD flowchart) addresses this difference in context (e.g., reduced capability and support provided by the ASP, coupled with operator actions that are likely to be performed locally in the plant) by providing HEPs that are the highest among the flowcharts.

In addition, the HRA should pay particular attention to the workload added by the conditions described in item (c) above. When the MCR is staffed normally, there are rules and protocols about when and why control room operators are to be engaged, either directly or by telephone. Under accident conditions, such interactions typically increase. However, additional plant staff can be expected to help MCR operators, either as required (e.g., the Shift Technical Advisor is usually required to be in the MCR within ten [10] minutes) or simply to provide additional support. Such additional support may not be likely or even possible (due to the size and location of the ASP) when the MCR is abandoned.

Therefore, it should be assumed that the expected operating context for operators at the ASP will involve a higher workload than that expected for the MCR under similar accident conditions. Rarely might this assumption be relaxed, and only if it can be demonstrated that:

- additional staff are able and required to assist operators at the ASP such that the ASP operators' workload is reduced, OR
- the ASP location, configuration, or other features are similar enough to the MCR in functioning to limit ASP operator workload

5.0 The "0.1 Case"

The focus of the initial efforts regarding the MCR Abandonment FAQ has been to define what plant conditions and operator action characteristics can be represented by a 0.1 HEP for all operator actions associated with safe shutdown following abandonment. (Note that this representation is different from the original introduction of this approach in NUREG/CR-6850; namely, the 0.1 probability represents ONLY the operator actions and not any hardware contributions, nor does it include the conditional core damage probability [CCDP], although it may be assumed to do so implicitly if the CCDP is close to unity.)

The discussion below outlines the currently recommended approach which involves, first, a base definition which is simple and fairly rigorous. Recognizing that few plants would meet this definition, a few acceptable "relaxations" have been identified.

It should be noted that the base case defined below is not intended to "anchor" the quantification at 0.1 (i.e., the conditions identified might represent a lower combined HEP, if detailed HRA were performed). Rather, it was used as a starting point for defining a set of conditions that supports a consensus 0.1 probability. Once these conditions that define the base case are identified, then acceptable relaxations where the plant response is not challenged by the fire-induced damage can be incrementally identified.

5.1 BASE CASE DEFINITION

The base definition for the 0.1 case for safe shutdown following MCR abandonment matches the NUREG-1921 definition for "simple" (rather than complex) that was cited in Section 4.1 of this document, plus other characteristics discussed above.

Namely, ALL of the following are satisfied:

- all required actions are feasible, independently and taken together
- there is no cognitive complexity
- there is no execution complexity
- all actions[2] are taken from the dedicated, remote shutdown panel(s)[3], i.e., no "local" actions at the component locations themselves.
- controls, cues/indications, and other needs for cognition and execution are provided by the remote shutdown panel (without need for another location)
- procedures provide good support for performance of required actions for the associated scenario
- required actions are trained upon (including appropriately designed "simulations," walkthroughs, etc.)
- each operator action (with appropriate treatment of any dependencies) has a time margin of two (2), using the definition of time margin provided in NUREG-1921.[4] Note that a multiplicative time margin criterion may not be appropriate for very short action times,

---

[2] These actions would include those actions taken, initially, to establish plant conditions to enable plant shutdown, including actions in the MCR (e.g., tripping RCPs).

[3] If, for example, there are multiple panels in **a single location** that is used for safe shutdown.

[4] In NUREG-1921, a time margin of 2 is often expressed as additional available time of 100%.

e.g., < 2 minutes, where some minimum additional, additive margin > factor of two may be appropriate (e.g., at least 2 minutes).

See the section immediately below for acceptable relaxations of this requirement. Overall, however, the intent is that the 0.1 case represents a reasonable screening value for a simple, straightforward, and unambiguous case, with adequate time for both cognition and execution.

Note that no other timing considerations (except those that would already be addressed through the feasibility assessment described in NUREG-1921) are recommended at this time.

5.2 ACCEPTABLE RELAXATIONS

The base definition shown above is intended to be used to communicate that, overall, the operational conditions and characteristics must meet the general definition of a simple, straightforward, and unambiguous case, with adequate time for both cognition and execution. However, it is recognized that plant-specific situations may closely approximate this overall intent with certain acceptable compensating measures. In all cases, a good feasibility assessment, as described in NUREG-1921, should be performed.

A limited set of acceptable compensating measures are provided below. These have been limited in order to maintain the close approximation to the base definition and to recognize that not all measures are adequate compensation. In other words, when multiple relaxations are used then these must be balanced using a whole-picture view to ensure one factor is not overwhelming others inadvertently.

As such, the acceptable relaxations are:

1. A limited number of multiple locations (no more than five), including both the dedicated, remote shutdown panel and local plant locations, IF actions between locations are independent, i.e.,
    a. do not require any coordination or associated communication for successful performance, AND
    b. each action location has all of the necessary cues/indications and controls needed for successful performance.

2. Detailed procedure steps may be replaced by skill-of-the-craft, but only if good training and training frequency and/or experience exists and has been demonstrated.

3. Local control of a single plant parameter or equipment, IF

    a. no coordination or associated communication is required for successful performance of the actions, AND
    b. all indications or cues necessary for control are co-located with the action location, AND
    c. control actions are well-trained and demonstrated, AND
    d. as compared to “control” actions, execution of this action can be considered “simple.”

4. Local control of more than one plant parameter or equipment, IF

a. there are NO dependencies between the operator actions and resulting plant behavior, AND
b. no coordination or associated communication is required, AND
c. all indications or cues necessary for control are co-located with the action location, AND
d. control actions are well-trained, AND
e. as compared to “control” actions, execution of this action can be considered “simple.”

5. Communication between adjacent action locations may be allowed if both areas are not noisy and 3-way communication can be accomplished without loss of time due to the need for repeated communications (due to, for example, competing communications).

6. Communication and coordination responsibilities related to field operator actions may be assigned to the operator responsible for command-and-control (or the equivalent with respect to following procedure and probably an SRO) IF:

    a. The workload related to the fire and other plant concerns has been assigned to another operator or plant manager, or has been compensated for in some demonstrated way (i.e., NO responsibilities for communicating with fire brigade or making notifications), AND
    b. A limited number (i.e., no more than five) locations are involved (with no more than four in conjunction with one ASP, or three in conjunction with two ASPs, with the ASPs meeting the independence requirement), AND
    c. Coordination between field operator actions at multiple locations is limited to verifying a small number (e.g., two) actions that require time sequencing, AND
    d. Required communications are only related to completion of field operator actions (e.g., not related to control a plant parameter or equipment) and involve simple, unambiguous communications, including those communications associated with coordination of multiple operators, AND
    e. Communication equipment is adequate to support unambiguous communication between locations.

7. It is recognized that a multiplicative time margin criterion may not be appropriate for very short action times, e.g., < 2 minutes, where some minimum additional, additive margin > factor of two may be appropriate.

8. For all of the above relaxations, ALL other plant conditions and action characteristics specified in the base case must be met for it to be an acceptable relaxation.

5.3 ILLUSTRATIVE EXAMPLES OF ACCEPTABLE RELAXATIONS

This section provides some examples of acceptable relaxations to the base definition of the 0.1 case described in Section 5.1 above. These examples have been chosen and/or developed to illustrate the general descriptions of relaxations given immediately above in Section 5.2. Furthermore, the examples have been taken from ones provided in drafts of FAQ 13-0002, but have been modified in order to illustrate recommendations on the definition of complexity, the 0.1 case and its acceptable exceptions.

5.3.1 Example 1 (Base Case)

Description of ASP:

The plant has two remote shutdown panels (RSDPs), one for train A equipment and one for train B equipment. Either panel is capable of providing all required instrumentation and control to shut down the plant, i.e., only one train (A or B) is required. The rooms are small and quiet. Provisions are made for controlling traffic and communications for command and control at the Train A RSDP.

Description of required actions:

- All actions required to enable the panels for a fire in the MCR (i.e., the command and control transition actions) are accomplished by means of a bank of disconnect switches in the relay room. Upon leaving the MCR, operators in-route to manning the RSDPs pass through the relay room and throw all switches on a panel.

- Most actions for shutdown are accomplished at the RSDPs, but in addition there are certain local actions that are required.

- Field operators perform the following:

    - FO-1; Locally trip RCPs
    - FO-2; Locally maintain SG pressure at 1000 psig using SG PORVs to control natural circulation; all controls and indications necessary for this action are co-located with the action location
    - FO-3; Locally trip main feed and condensate pumps

Assessment of relevant factors, including performance shaping factors (PSFs):

- Training – All operations staff are trained in these operations bi-annually, both classroom and simulated.
- Procedures - Relevant procedures match well with fire scenarios, and either contain detailed step-by-step instructions, or rely on skill-of-the-craft actions, on which operators have trained.
- Cues and indications - All needed cues and indications are available and salient on the RSDPs, or co-located with associated fields actions.
- Communications – The plant has a hardened, hard-wired communication net, which will ensure quality communications.
- Coordination - All three of the required field operator actions only require simple actions and verifications of action success and do not require any time sequencing (e.g., the pump trips do not require specific timing; the operation of the SG PORVs is not dependent on timing).
- Timing - Timing analysis has been performed for all operator actions (which are independent), and all actions have a time margin (as defined in the scoping approach for

NUREG-1921) of at least 2.[5]

- Feasibility assessment: All required actions for this safe shutdown strategy have been assessed and determined to be feasible. Details of this feasibility assessment are consistent with that described in NUREG-1921.[6]

Assessment of match with definition of 0.1 case:

This example does not exactly match the base definition of the 0.1 case because:

1. There is more than one ASP
2. Local operator actions are required.
3. Multiple locations for operator actions are required.
4. One of the field operator actions involves control of a plant parameter.
5. There might be an impact on cognitive complexity due to an increased workload associated with communications and coordination of operator actions in multiple locations, including two remote shutdown panels and three actions performed in field locations.

However, the example does match up with acceptable alternatives, allowing use of 0.1 to represent all of the operator contributions to failure probability for this sequence or scenario. Namely:

1. While there are multiple locations, including local plant locations and actions between locations,

    i. There are no more than two ASPs with no more than three accompanying local actions
    ii. The actions are independent, i.e.,

        a. They do not require any coordination or associated communication for successful performance, AND
        b. Each action location has all of the necessary cues/indications and controls needed for successful performance.

2. There are either detailed procedure steps or skill-of-the-craft actions, both of which are supported by training and training frequency and/or experience.

3. The operator action that involves maintaining SG pressure at 1000 psig is the only local control action required for safe shutdown, and this involves local control action of a <u>single</u> plant parameter for which

        a. no coordination or associated communication is required, AND
        b. all indications or cues necessary for control are co-located with the action location, AND
        c. control actions are well-trained, AND

[5] Note that information has been assumed since there was no information of this kind in the industry example.
[6] Ditto.

d. as compared to “control” actions, execution of this action can be considered “simple.”

4. No coordination of field operator actions is required; communication is limited to verification of action completion over a hardened, hard-wired communication net, which will ensure quality communications.

5.3.2 Example 2

Plant Background and initial plant conditions:

- Westinghouse PWR
- At the time of the fire the plant is operating at full power steady state.
- Following the detection of a fire, the MCR will activate the fire brigade and performs the first four steps of EOP-0. While in the MCR, the operators will be working in both the EOPs and the fire procedures. Following the decision to abandon the MCR, the EOP procedures are suspended.
- Plant trains biannually on the MCR abandonment procedure.

Assumptions:

- T = 0 is considered to be the start of the fire as well as reactor trip. There is no considerable time delay between the start of the fire and when reactor trip occurs.
- Once the decision to abandon the MCR is made there will be no hesitation of the crew to implement all steps in the MCR abandonment procedure.

Event description:

A fire occurs in one of the back panels of the MCR, i.e., outside the visible horseshoe or its attached backside. At the start of the fire, a reactor trip/turbine trip occurs and there are no fire induced spurious operations of equipment. Following the reactor trip, the plant response is as expected for a transient with reactor trip until smoke fills the MCR causing the MCR to be uninhabitable. Electrical power, AFW and charging are available until they are switched off by the operators in the first few steps of the MCR abandonment procedure just before the crew abandons the MCR due to high smoke levels. There are no fire induced spurious operations of equipment after the operators abandon the MCR.

Description of ASP:

Plant has one dedicated, remote shutdown panel, credited for fire.

General description of required actions:

The fire and the reactor trip occur at the same time. Upon receiving a reactor trip signal, the control room crew will enter E-0 and perform the first four steps of E-0 and transfer to ES-01 within the first 5 minutes of the scenario. All AC power is initially available, reactor trip and turbine trip are successful, and AFW successfully starts and runs. Reactor Coolant System

(RCS) pressure stabilizes following reactor trip and the operators are maintaining successful control over the plant before they leave the MCR.

When the crew enters EOP ES-0.1, they will also open the MCR abandonment procedure. The fire is spreading within the panel and suppression measures are not successful. Because the fire is spreading, and the smoke levels are increasing, the operators start performing steps 1-8 of the abandonment procedure at about 15 minutes. As the scenario progresses, smoke levels continue to build and force the operators out of the MCR at 18 minutes. (This time is determined by CFAST)

The fire PRA context for this scenario is that, after the fire causes a reactor trip, charging, AFW, CCPs, and CCW will remain running until the operators switch them off at 15 minutes (before leaving the MCR.)

Once outside the MCR, the MCR abandonment procedure directs a single RO to perform all actions at the RSP and then directs additional local actions via standalone attachments. The PSFs associated with each Task are shown in Table 2.

Required actions: (note that these are breakdowns of the functionally related tasks into system-related tasks that map better to an HFE that would be modeled in a PRA):

1. Establish RSD Control & Instrumentation (Reactor Operator #1)

    a. Place Control Room isolation switches in LOCAL (before leaving MCR)
        - Hand switch – 1-X
        - Hand switch – 2-X
    b. Place the following system switches in local (all of these actions are performed at the remote shutdown panel)
        - Hand switch – 3-AL
        - Hand switch -4 –CCW
        - Hand switch – 5-FC
        - Hand switch -6 –PW

2. Restore AFW from the remote shutdown panel (Reactor Operator #1) (All actions are performed at the remote shutdown panel):

    a. Align AFW suction from the CST. (CST-XX-1)
    b. Start AFW pump A
    c. Open AFW Valve–XX

3. Restore power to both CCW pumps and charging pumps by closing breaker in south electrical room (Balance of Plant [BOP] operator - local action).

4. Start CCW in CCW pump room, with no requirement for control of CCW flow (Auxiliary Building Operator- local action, first location).

5. Start CCP from north piping penetration room, with no requirement to control charging flow locally (Auxiliary Building Operator- local action, second location).

6. Overall command-and-control at remote shutdown panel (SRO).

7. Control of pressurizer pressure, including control of charging flow at RSD (Operator #2).

Assessment of relevant factors, including performance shaping factors (PSFs):

- Training – All operations staff are trained in these operations bi-annually.
    - Action 1: class room discussion
    - Action 2: No JPM[7] exists
    - Action 3: JPM exists for this Attachment B
    - Action 4: JPM exists for this Attachment C (along with Action 5)
    - Action 5: JPM exists for this Attachment C (along with Action 4)
    - Action 6: No JPM exists

- Procedures - Relevant procedures match well with fire scenarios, and either contain detailed step-by-step instructions, or rely on skill-of-the-craft actions.[8]
    - Action 1: Steps 11 and 12 of the MCR abandonment procedure directly provide the execution steps for this action
    - Action 2: Steps 13-21 direct the crew to restore AFW from the remote shutdown panel.
    - Action 3: Steps 23-28 direct the crew to maintain CCW and charging and associated cooling systems from the remote shutdown panel.
    - Action 4: Ditto from Action 3
    - Action 5: Ditto from Action 3

- Cues and indications:
    - Action 1: Following steps in the procedure to establish instrumentation.
    - Action 2: Following steps in the procedure. Indications that provide feedback on the success or failure of this action are available at the remote shutdown panel.
    - Action 3: Following steps in the procedure. Indications that provide feedback on the success or failure of this action are available at the remote shutdown panel.
    - Action 4: Ditto from Action 3 - Indications that provide feedback on the success or failure of this action are available at the remote shutdown panel.
    - Action 5: Ditto from Action 3 - Indications that provide feedback on the success or failure of these actions are available at the remote shutdown panel.

- Communications[9] – For all actions, operators can communicate via phone lines that are dedicated and unaffected by the fire. The evacuation phone numbers are provided in the MCR abandonment procedure as notes when communication is required. Communication between Reactor Operator No. 1, Reactor Operator No. 2 and SRO (who

---

[7] Refer to Sections 4.6.2 and 4.11 in NUREG-1921 on guidance in using JPMs and making adjustments for a lack of realism in them.

[8] Note: This is an assumption; it is not explicitly stated in the industry example, but it might be inferred from the information below.

[9] The industry example did not explicitly identify what communication is necessary. Consequently, the NRC has added this discussion and specified what means of communication would be needed for an acceptable relaxation of the 0.1 case.

are responsible for command-and-control are co-located at the remote shutdown panel, so their communication is easily done and similar to that in the MCR. BOP operator reports to SRO via phone when required actions No. 3 and No. 4 are successfully completed.

- Coordination[10] - SRO is responsible for coordinating all operator actions. In particular, SRO directs the Auxiliary Building Operator to start CCW pumps and CCPs only after the BOP operator has restored power to these pumps, and ensures that AFW and charging flows are coordinated by RO No. 1 and RO No. 2 at the remote shutdown panel. [Also, see "Communications" above.]

Timing analysis:[11]

Table: Time Margins Calculation for Example Required Actions			
Timing input	Task 3	Task 4	Task 5
System window (T_{sw})	55 minutes	65 minutes	55 minutes
Delay time (T_d)	20 minutes	25 minutes	20 minutes
Cognition time (T_{cog})	2 minutes	2 minutes	2 minutes
Execution time (T_{exe})	5 minutes	5 minutes	10 minutes
Time required[12]	7 minutes	7 minutes	12 minutes
Time available[13]	35 minutes	40 minutes	35 minutes
Time available - Time required	28 minutes	33 minutes	23 minutes
Time margin	4	5	2

Feasibility assessment:[14]

All required actions for this safe shutdown strategy have been assessed and determined to be feasible. Details of this feasibility assessment are consistent with that described in NUREG-1921.

---

10 Note: The industry example does not address this factor.

11 The industry timing analysis needed to be revised for the following reasons: a) The NRC does not agree that T_{cog} can be zero, b) the math on calculating the time required, time available, and time margin (per NUREG-1921) is not fully displayed, and c) using the available information, it does not appear that any of the actions have a time margin greater than or equal to 2, which the NRC considers important to the definition of an acceptable relaxation of the 0.1 case. A timing analysis is needed for required actions #3, #4, and #5, as summarized below. In all cases, the time margin, as defined in NUREG-1921 for the scoping approach, is at least 2.

12 Time required is defined as the sum of the cognition and execution times.

13 Time available is defined as the delay time subtracted from the system window.

14 The industry's examples are not organized to separately discuss the feasibility assessment. Feasibility is assumed here in order to carry through this example.

Assessment of match with definition of 0.1 case:

This example does not match the base definition of the 0.1 case because:

1. Local operator actions are required.
2. Multiple locations for operator actions are required.
3. Time sequencing, and, therefore, coordination of actions is required.
4. One field operator must perform actions in two different locations.
5. There might be an impact on cognitive complexity due to an increased workload associated with communications and coordination of operator actions in multiple locations, including three actions performed in field locations.

However, the example does match up with acceptable alternatives, allowing use of 0.1 to represent all of the operator contributions to failure probability for this sequence or scenario. Namely:

1. SRO is dedicated to command-and-control responsibilities, including any coordination of operator actions, thereby reducing potential workload on operators at the remote shutdown panel.
2. While Auxiliary Building Operator performs Tasks Nos. 4 and 5 at different locations, both of these actions are related to the same higher-level function of restoring injection (as timing analysis confirms an appropriate time margin). Also, within a short timeframe, the order of these actions is not critical.
3. While there are multiple locations, including local plant locations, actions between locations,
    i. There is only one ASP with no more than three accompanying local actions,
    ii. The actions are either independent or a coordination strategy compensates for their dependence, i.e.,
        a. each action location has all of the necessary cues/indications and controls needed for successful performance, AND
        b. either they do not require any coordination or associated communication for successful performance, OR the SRO is dedicated to coordinating Task No. 3 with Tasks No. 4 and No. 5.

6.0 ALTERNATIVES WHEN "0.1 CASE" IS NOT JUSTIFIED

If neither the base definition nor acceptable relaxations for the 0.1 case can be met, then alternative HRA quantification approaches must be used. Detailed HRA is the obvious and preferable alternative. However, the NUREG-1921 scoping approach might be helpful in some cases. Relaxation to the NUREG-1921 approach is proposed below.

6.1 NUREG-1921 Scoping Approach

Following the guidance provided in NUREG-1921, the scoping approach can be used for HRA quantification of safe shutdown strategies involving MCR abandonment. The scoping approach was specifically developed to develop HEPs that are less conservative than screening values, but less resource-intensive to apply then detailed HRA.

As illustrated in the examples attached, HEPs on the order of 0.1 can be obtained using the scoping approach for certain cases (especially when operator actions are required no less than 30 minutes after reactor trip).

Also suggested is a relaxation of the NUREG-1921 criteria for use of the scoping approach. Namely, for those plants that can demonstrate that their ASP has a capability and design similar to that for the MCR, then the EXCR flowcharts can be used to develop HEPs. The EXCR flowchart provides lower HEPs than the ASD flowchart because the ASD flowchart assumes that both cognition and execution are affected by a lesser capability and design of the ASP.

For both the as-published and relaxed applications of the scoping approach in NUREG-1921, additional guidance and examples could be developed to support such applications.

6.2 Detailed HRA

It is recognized that there is limited, specific guidance on how to perform detailed HRA quantification for safe shutdown strategies following MCR Abandonment. However, the existing discussions in NUREG-1921 in the qualitative analysis section (Section 4), quantification analysis section for the scoping approach (Section 5.2), and two appendices on detailed HRA quantification (Appendices B and C) can be coupled with the discussions above to support detailed HRA applications for MCR Abandonment cases.

As a supplement to existing guidance, it is recommended that, if multiple plant locations are involved in the safe shutdown strategy (especially, if coordination is required), then multiple associated timelines be developed, with notations in the timelines and associated explanatory texts on where there are potential dependencies between operators/timelines due to coordination, time-sequencing, hold-points, and so forth. However, it is also recognized, as is stated in NUREG-1921, that, since HRA for safe shutdown strategies following MCR abandonment can be a complicated analysis (which is further exacerbated by the variety of plant designs and safe shutdown strategies), it remains a potential subject for future research.

ATTACHMENT

Examples Illustrating Attainment of HEPs on the Order of 0.1 using the NUREG-1921 Scoping Approach

Fire in MCR	Abandon?	Transfer while in MCR	"Remote" Actions	Status	Probability (Given Fire)	Comment
Fire	1.00E+00	9.80E-01	9.60E-01	OK	9.41E-01	Success via Timely Abandonment, Transfer & Remote Operation
			4.00E-02	CD	3.92E-02	Successful Transfer, but Unsuccessful Operation at Panel or Component
		2.00E-02		CD	2.00E-02	Failed Transfer, no Opportunity for "Remote" Operation
	0.00E+00			CD	0.00E+00	Wrong Decision, MCR Fire Forces Abandonment with no Opportunity for "Remote" Operation
				Sum =	5.92E-02	
Decision Tree	N/A	EXCR	ASD		NOTE: ASD only provides for "implicit" distinction between "remote" actions at panel vs. at component (via timing, complexity, etc.)	

Scenario: Unsuppressable fire in MCR. Operators decide abandonment is warranted and take actions to transfer "remotely" but now solely to a dedicated shutdown panel.
Abandonment, transfer and "remote" operations can be accomplished in > 30 min. All actions, including even those taken "locally," assume complexity is minimal.

Assumptions:
- Decision to abandon is now correct 100% of the time.
- All relevant time margins are at least 100%.
- Decision Path for EXCR Tree (Fig 5-4):
  - D22 - No
  - D26 - Yes
  - D27 - Yes
  - D33 - No
  - D34 - No
  - From Lookup Table X, HEP = 0.02
- Decision Path for ASD (Fig 5-5):
  - D40 - Yes
  - D41 - Yes
  - D42 - Yes
  - D43 - Yes
  - D44 - Yes
  - D49 - No
  - D50 - No
  - From Lookup Table AG, HEP = 0.04

Result from this scenario is a total HEP for failure to successfully shutdown (i.e., avoid CD) due to loss of habitability = 0.0592
Depending on the associated CCDP for this scenario, the joint HEP-CCDP = 0.0592 x CCDP.

	Fire in MCR	Abandon?	Transfer while in MCR	Local Action #1	Local Action #2	Status	Probability (Given Fire)	Comment
3	Fire	1.00E+00	9.80E-01	9.60E-01	9.60E-01	OK	9.03E-01	Success via Timely Abandonment, Transfer & Remote Operation
5					4.00E-02	CD	3.76E-02	Failed Despite Successful Transfer, Since Action 2 Unsuccessful
7				4.00E-02		CD	3.92E-02	Failed Despite Successful Transfer, Since Action 1 Unsuccessful
9			2.00E-02			CD	2.00E-02	Failed Transfer, no Opportunity for "Remote" Operation
11		0.00E+00				CD	0.00E+00	Wrong Decision, MCR Fire Forces Abandonment with no Opportunity for "Remote" Operation
13						Sum =	9.68E-02	
15	Decision Tree	N/A	EXCR	ASD	ASD		NOTE: ASD only provides for "implicit" distinction between "remote" actions at panel vs. at component (via timing, complexity, etc.)	

Scenario: Unsuppressable fire in MCR. Operators decide abandonment is warranted and take actions to transfer "remotely," specifically two independent actions at separate "local" components.
Abandonment, transfer and "remote" operations can be accomplished in > 30 min. All actions, including even those taken "locally," assume complexity is minimal.

Assumptions:
- Decision to abandon is now correct 100% of the time.
- Transfer is effectively just a "one-action" activity (even if requiring multiple "sub-actions").
- All relevant time margins are at least 100%.
- Decision Path for EXCR Tree (Fig 5-4):
  - D22 - No
  - D26 - Yes
  - D27 - Yes
  - D33 - No
  - D34 - No
  - From Lookup Table X, HEP = 0.02
- Decision Path for ASD (Fig 5-5), assumed same for each local action:
  - D40 - Yes
  - D41 - Yes
  - D42 - Yes
  - D43 - Yes
  - D44 - Yes
  - D49 - No
  - D50 - No
  - From Lookup Table AG, HEP = 0.04

Result from this scenario is a total HEP for failure to successfully shutdown (i.e., avoid CD) due to loss of habitability = 0.0968
Depending on the associated CCDP for this scenario, the joint HEP-CCDP = 0.0968 x CCDP.