FAQ Number 13-0002 **FAQ Revision** 0Ik

FAQ Title **Modeling of Main Control Room Abandonment on Loss of Habitability**

Plant: Various Date: 21 May 20133 July 2013

Contact: P. Amico, Hughes Assoc. Phone: 443.745.2360
J. Julius, SCIENTECH 800-862-6702
Email: pamico@haifire.com
jjulius@curtisswright.com

Distribution: *(NEI Internal Use)*

☒ FPRA TF ☐ BWROG ☐ PWROG

Purpose of FAQ:

To clarify the expectation for modeling of control room abandonment for fire scenarios in the main control room (MCR) that lead to a loss of habitability.that would achieve an overall assessment for the analysis of Main Control Room (MCR, aka Control Room) abandonment scenarios of Capability Category II of the ASME/ANS standard as endorsed by RG 1.200, Rev. 2.

Relevant NRC document(s):
R.G. 1.200, Rev. 2; NUREG-1921, NUREG/CR-6850

Details:

NRC document needing interpretation (include document number and title, section, paragraph, and line numbers as applicable):

RG 1.200, Rev 2.NUREG-1921 and NUREG/CR-6850, Sspecifically as itthey regards the following referenced SRs from the ASME/ANS standard, to reach agreement on a consistent approach that, if properly applied as determined by the peer review,[1] will achieve an overall assessment of Capability Category II for the assessment in fire PRA of MCR abandonment in a manner adequate to support risk-informed applications. This is accomplished by performing detailed analyses for the estimation of human error probabilities (HEPs) for risk-significant human failure events (HFEs), and the use of screening values for HEPs for non-significant MCR scenarios.

[1] Throughout this FAQ, reference is made to the methods documented herein achieving an overall assessment of CC-II against the requirements of RG 1.200, Rev. 2 and the endorsed ASME/ANS standard. This means that, upon approval of this FAQ, the NRC and the industry agree that the methods contained herein constitute one acceptable way to meet the requirements of RG 1.200, Rev 2 for a PRA to support risk-informed applications, ***as long as the methods are properly applied.*** This latter determination must be made by the conduct of the peer review.

Therefore, appropriate use of screening HEPs that may, as an individual item, meet other HRA SRs at CC-I would still allow the overall HRA to meet CC-II.

In general, high level requirement FSS-B from Part 4 of the PRA Standard contains supporting requirements applicable to the fire scenario modeling for the MCR. Similarly, HRA-A, HRA-B and HRA-C contain supporting requirements associated with HRA (and some of these refer back to HR-G in Part 2). This FAQ describes two modeling approaches for MCR Abandonment – a screening approach and detailed analysis. Supporting requirements applicable to each of these approaches are listed below.

For a screening approach, ASME/ANS PRA Standard, Part 4 supporting requirements FSS-B2, FSS-D3, and HRA-C1 in conjunction with HR-G1 from Part 2 apply.

For a detailed analysis, the following supporting requirements apply from Part 4 (Fire) and Part 2 (Internal Events) of the ASME/ANS PRA Standard:

FSS-B1 and FSS-B2, plus the following (to the extent that they pertain to main control room (MCR) abandonment), PRM-B11, FSS-D3, HRA-A1, HRA-A2, HRA-A3, HRA-A4, HRA-B1, HRA-B2, HRA-B3, HRA-B4, HRA-C1, HRA-D1.

ASME/ANS PRA Standard, Part 2, all supporting requirements related to post-initiator human failure events plus the following (to the extent that they pertain to MCR abandonment), specifically all SR under HLR HR-E, HR-F, HR-G, HR-H and HR-I.

For each part of the ASME/ANS PRA Standard, ensure the clarifications and qualifications of RG 1.200, Rev 2 are implemented such as the clarifications to HR-D3, HR-G3, HR-G4, FSS-D3 and HRA-D1.

NUREG-1921, specifically Sections 5.1.3, 5.2 and 5.3 as it regards assessment of MCR abandonment.

NUREG/CR-6850, Volume 1 Section 3.2.7 and Volume 2 Sections, 11.5.2, 11.5.3, 12.5.3 and 12.5.5.2 as they regard assessment of MCR abandonment.

Circumstances requiring interpretation or new guidance:

Fire PRAs performed by the industry have modeled main control room (MCR) abandonment scenarios in different ways. NRC has expressed concern about the diversity of approaches being used, and feels that further guidance on implementation, beyond what is currently provided in NUREG-1921 and NUREG/CR-6850 is needed. RG 1.200, Rev 2 (and by implication, Part 4 and the back-referenced requirements of the ASME/ANS PRA standard) provide supporting requirements on the "what" aspect of modeling, but not the how. In the interests of reaching agreement between the industry and NRC as to "how" the modeling can be done such that the "what" is achieved, this FAQ is being issued.

Main control room abandonment is a complex issue in that the PRA modeling consists of a wide range of scenarios and the plant response consists of a collective set of operator actions. In addition to issues related to multiple scenarios and multiple operator actions, there are issues related to limitations in the current human reliability analysis (HRA) methods that make the modeling complex. While fire human reliability analysis (HRA) guidance was recently published in 2012, the focus was on individual actions. It was recognized in NUREG-1921 that the issue of main control abandonment was one requiring future HRA research.

As a result of these issues, Fire PRAs performed by the industry to date have modeled main control room (MCR) abandonment scenarios using different quantification approaches and different levels of detail. For example, in some Fire PRA models a single, overall human error probability (HEP) of 0.1 representing the collective set of operator actions needed to safely shutdown the plant following a fire in the Main Control Room (MCR) or a fire in the cable spreading rooms has been modeled. This single HEP may have been applied to all main control room or other alternate shutdown (ASD) area fire scenarios that led to evacuation, including those due to loss of habitability (LOH) or due to a loss of plant controls (LOC). In some Fire PRAs, no credit is given for abandonment on loss of control (effectively, a single overall HEP of 1.0). Several reviews have questioned the validity of applying a single representative HEP to the range of scenarios that would be encountered, each of which potentially involves many operator actions, even though this may be "allowed" by NUREG-1921. This FAQ provides guidance to the MCR Abandonment modeling on loss of MCR habitability, including when a single HEP is appropriate and when a plant-specific, detailed human error probability (or set of human error probabilities) should be developed for each fire scenario. Further, this FAQ defines specific issues to be addressed.

No new methods are required or suggested with regard to these circumstances, therefore the use of a FAQ to reach agreement on guidance for MCR abandonment modeling is appropriate. Main control room fire scenarios that do not lead to abandonment are not addressed in this FAQ as sufficient guidance exists.

The term "MCR aAbandonment fire scenario on loss of habitability (LOH)" in this FAQ is defined as a fire scenario occurring on the MCR that creates environmental conditions leading to a demand to shift command and control of the plant from the MCR to a remote shutdown panel or a set of local control stations. MCR LOH abandonment scenarios consist of the following elements, with some elements addressed in this FAQ (as noted below) and some elements addressed using existing guidance (requiring no amplification in this FAQ).

1) Fire ignition, growth and suppression (Not addressed in this FAQ)

2) Demand for abandonment (due to loss of habitability (LOH), loss of control (LOC), or other procedural guidance). (Addressed in this FAQ)
3) Operator decision to abandon or not abandon. (Addressed in this FAQ as not relevant to LOH scenarios)
4) Operator actions inside of the MCR to:
    a. Isolate MCR circuits and
    b. Mitigate spurious actuation (e.g. to shut the pressurizer PORV block valve in a PWR). (Addressed in this FAQ)
5) Operator actions outside of the MCR to safely shutdown the plant, including
    a. Remote shutdown panel or lLocal control stations to establish front-line systems to mitigate a transient loss of decay heat removal. (Addressed in this FAQ)
    b. Align and energize support systems as needed by front-line systems. (Addressed in this FAQ)
6) Operator actions outside of the MCR to isolate MCR circuits and to mitigate spurious actuation (e.g. to shut the pressurizer PORV block valve in a PWR). (Addressed in this FAQ)
7) SSC equipment reliability and operability for components used in the plant response. (Addressed in this FAQ)

Specific circumstances requiring interpretation or new guidance:

- When a screening approach is appropriate for MCR Abandonment, and when a detailed analysis is needed.
- Identification of the set of operator actions which are required for safe shutdown, and the set of operator actions that directly mitigate spurious cable faults.
- Definition of the cognitive and execution tasks and associated success criteria for each operator action given the context of the fire scenarios.
- Qualitative analysis associated with individual operator actions and the overall collective set of actions, including the analysis of time-critical actions.
- Feasibility considerations
- Quantification method selection
- Conduct of a reasonableness check

Note that this FAQ does not treat the case where the control room is not abandoned (that is, where the MCR remains habitable and command and control is maintained in the MCR, whether or not individual operators are dispatched to perform actions outside the control room in accordance with procedures). Such cases are not unique to fire, and in fact, are already treated in PRAs for internal events in well-established ways (for example, treatment of ex-control room actions for station blackout, and loss of all DC power). Some fire PRAs have chosen to develop separate HEPs for the "in-MCR fire" case to evaluate the impact of conducting in-MCR actions when a fire has occurred that is not severe enough to cause abandonment, but this is a separate case and can be addressed using the current NUREG-1921 guidance. There is no need to provide further guidance, interpretation or clarification for this treatment of the non-abandonment case in FPRAs.

Detail contentious points if licensee and NRC have not reached consensus on the facts and circumstances:

There have been plants that have used a generic value of 0.1 for the probability of failure to reach a safe and stable state for all scenarios that would require abandonment in order to avoid core damage. The NRC has expressed concern that insufficient evaluation may have been performed to justify the use of this single value given the plant-specific and scenario specific aspects of the actions required in order to achieve this condition. Section 5.1.3 of NUREG-1921 provides guidance for modeling a single HFE for the complete set of all operator actions necessary to provide safe shutdown of the plant from outside of the MCR with an overall human error probability (HEP) of 0.1 once feasibility is confirmed. The approach of applying a 0.1 to all scenarios is a holdover from the simplified modeling of the IPEEE era. Within the range of plant-specific scenarios, there are likely to be scenarios where the 0.1 HEP is bounding, scenarios where the 0.1 HEP is appropriate, and scenarios where the 0.1 HEP is non-conservative.

This latter result is the root of the NRC concern, and further they have concerns that the 0.1 HEP from Section 5.1.3 of NUREG-1921 is lower than the values that would be obtained by applying the scoping approach from Section 5.2 of NUREG-1921. Therefore, although NUREG-1921 is a recent document, NRC objects to the use of the 0.1 for MCR abandonment without further justification beyond what would normally be expected for the use of a screening approach.

Potentially relevant existing FAQ numbers:

None.

Response Section:

Proposed resolution of FAQ and the basis for the proposal:

1.0 Introduction

The analysis of fires inside the main control room ((MCR) ~~or in plant areas designated as alternate shutdown (ASD) areas~~ 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~~fire damage~~ and does not lead to a demand for abandonment. This type of scenario is not addressed in this FAQ and can be modeled with typical Fire HRA considerations as described in NUREG-1921.

FAQ Number	13-0002	FAQ Revision	0Ik
FAQ Title	Modeling of Main Control Room Abandonment on Loss of Habitability		

MCR or ASD fires that are not suppressed are further examined in the context of resulting fire damage (both fire-induced initiating event as well as fire damage to SSCs). In this latter case, the impact of the unsuppressed fire on plant systems and functions is increased, and at some point control room habitability is threatened. Those fires that lead to a demand for MCR abandonment in order to mitigate fire damage and achieve safe shutdown are addressed in this FAQ.

For each scenario leading to a demand for abandonment, the PRA Standard requires consideration of human reliability cognition and manipulation. These two aspects of control room abandonment have additional considerations as follows.

- Failure to diagnose and decide to abandon the control room in time to execute a successful shutdown. The following two types of scenarios have different diagnosis and decision-making considerations.As discussed later, this failure is not a concern for a
- Abandonment due to loss of habitability (LOH).
    - Abandonment due to loss of control (LOC)

- Given the successful decision to abandon, failure to successfully achieve a state that avoids core damage, consisting of;
    - Operator failure to successfully execute the necessary actions
    - Failue of equipment required to effect a successful shutdown.

Appropriate modeling for each of these is outlined in Figures 1 and 2. The process steps in the flow charts are described in the text below, which describe the various approaches and options. The "approaches" address differences in the human reliability analysis modeling, and the "options" describe different ways to incorporate the resulting human failure event into the Fire PRA model. There is a separate flow chart for the loss of habitability (LOH) and loss of control (LOC) cases because there are some fundamental differences in the details of the application of the HRA modeling approaches. However, there are some aspects of the approaches that are

Formatted: Font: Arial

Formatted

Formatted: Font: Arial

Figure 1 - Flow Chart for Abandonment Due to Loss of Habitability (LOH)

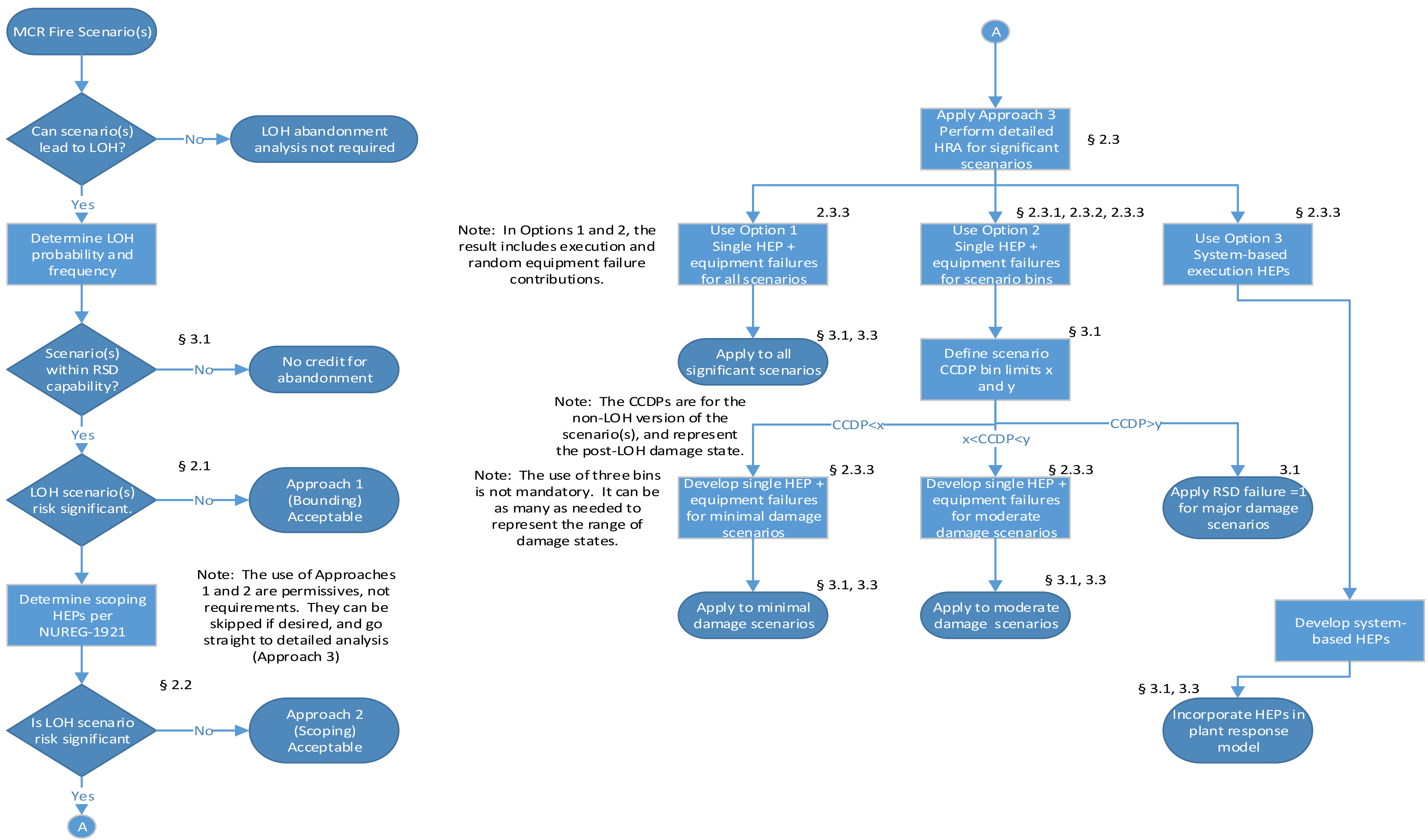
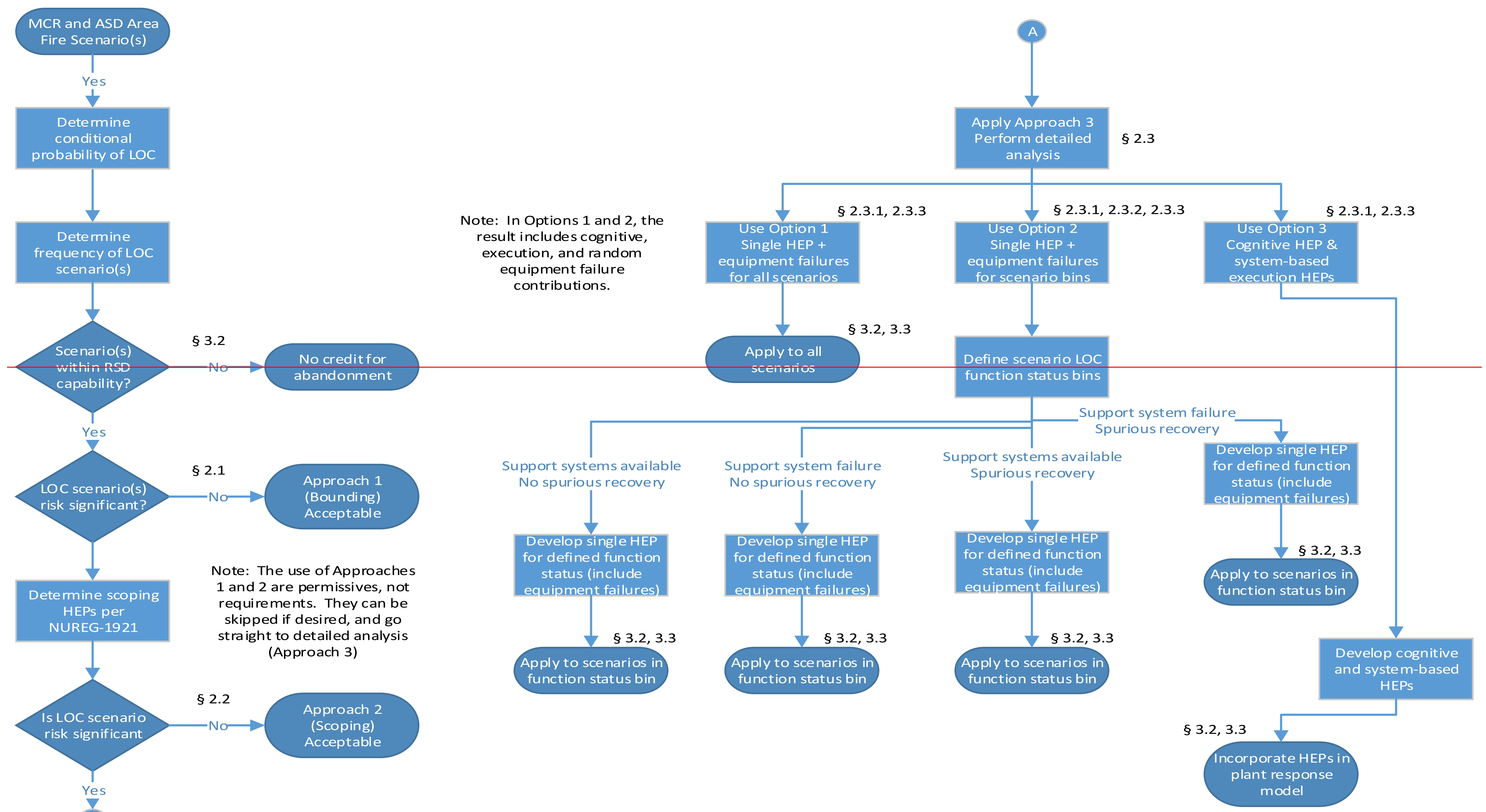


Figure 2 - Flow Chart for Abandonment Due to Loss of Control (LOC)



essentially identical regardless of whether the abandonment is for LOH or (LOC). The various acceptable modeling approaches are discussed in detail in this FAQ. Because there are a variety of ways to quantify the HEP and a variety of ways to incorporate the HFE into the Fire PRA, not all modeling combinations are detailed in this FAQ. One example of an acceptable approach that is not described further is for non-risk significant HFEs to be applied to MCR scenarios using the Option 1 systems modeling approach without using the Option 1 quantification approach.

It should be noted that equipment failures that preclude successful execution also need to be considered in the analysis. As with the HRA aspects, there is more than one approach to modeling this, and these are also discussed in the FAQ. The loss of habitability flow chart is applied to each fire scenario (or group of similar scenarios) that occurs in the control room. The loss of control flow chart is applied to each fire scenario (or group of similar scenarios) that occurs in areas of the plant that are defined as alternate shutdown areas by plant procedures (i.e., the plant procedures specifically direct or allow the crew to leave the control room for a fire in that area if they believe that it is not possible to maintain control of the plant and achieve a safe-and-stable condition using the controls and instruments in the control room).

2.0 Assessment of Credit for Abandonment (Remote Shutdown (RSD))

This section discusses various options for determining the amount of credit to apply to abandonment scenarios. The three approaches discussed provide an increasing level of detail and realism, permitting simplified approaches to be applied to scenarios that are not risk significant.

2.1 Approach 1 - Bounding Approach

Bounding analysis takes no credit for control room abandonment, and can apply to either loss of habitability or loss of control. It assumes that the operators will not abandon the control room until it is too late to perform the actions to successfully shut the plant down. While the use of this approach for abandonment due to loss of habitability is not precluded, it is primarily applied to abandonment due to loss of control.

Loss of habitability creates conditions that result in scenarios where it is physically impossible for the operators to remain in the MCR without risking serious physical harm. NUREG/CR-6850 defines the conditions that would force abandonment. There have been no issues raised with regard to its application. Based on that guidance, it is concluded that it is not credible that the operators will remain in the MCR under such conditions. Therefore, the probability of abandonment due to loss of habitability is not based on the HRA, but rather developed by establishing and justifying the fire conditions that would force abandonment (e.g., smoke, heat) and using probabilistic fire modeling techniques to assess the conditional probability that MCR fire scenarios would lead to abandonment due to loss of habitability. However, it is still possible that the CDF/LERF associated with LOH is so small at a particular plant that it does not contribute significantly to the overall fire risk. If this is the case, then the use of the bounding approach is justified even though it is conservative since the conservatism does not affect the fire risk insights and conclusions from the PRA. As shown on the LOH flow chart, this is determined by combining the frequency of each MCR scenario with the conditional probability that the scenario leads to the environmental conditions that would cause the loss of habitability to occur.

The considerations in using this approach for LOC are similar. Loss of control always represents the same general condition - that the plant cannot be brought to a safe state from the control room. This can result from scenarios that involve only direct fire failures (i.e., Conditional Probability of Loss of Control[2] (CPLOC) = 1.0), from scenarios that also involve fire failure probabilities (e.g., hot shorts, and thus a CPLOC < 1.0), or from scenarios that also involve random failures (e.g., random pump failure, and thus a CPLOC < 1.0). It is possible that the CDF/LERF associated with LOC is so small at a particular plant that it does not contribute significantly to the overall fire risk. If this is the case, then the use of the bounding approach is justified even though it is conservative since the conservatism does not affect the fire risk insights and conclusions from the PRA. As shown on the LOC flow chart, this is determined by combining the frequency of each ASD area scenario with the CPLOC that the scenario leads to core damage.

The use of this approach for abandonment due to either LOH or LOC is bounding in the sense that one would expect that it would yield the highest value of CDF and LERF from LOH and LOC fire scenarios.

Whenther applied to abandonment due to LOH or abandonment due to LOC (or both), the implications to the results of the Fire PRA must be considered. This would be considered a screening-type approach for the MCR abandonment aspects of the HRA, and so would be expected only to be used in scenarios that are not risk-significant unless it can be shown to be realistic for the specific plant., and so would only achieve an overall assessment of CC-II for the HRA technical element if it does not significantly impact risk-significant scenarios. Alternatively, if it can be shown to be realistic and contain the appropriate level of detail then the MCR abandonment would meet CC-II regardless. The former case is standard PRA practice, and no further clarification is required.

If the assumption impacts risk-significant scenarios, realism can be demonstrated through interviews with plant operations staff regarding their training, plant procedures, real or perceived cues, and crew predisposition, which must be

[2] CPLOC is defined as the probability, given that a fire scenario has occurred, of reaching a condition that will lead to core damage in the absence of action to abandon the control room (that is, if the control room is not abandoned in time, core damage will ensue). It represents any additional failure combinations beyond guaranteed failures resulting from the fire that would have to occur before a loss of control condition would exist.

documented in the Fire PRA. If through this process it can be justified that the operators are extremely likely to remain in the control room for too long, then it can be said that the bounding approach is, in actuality, realistic for that plant.not excessively bounding and would meet the requirements of CC-II. If this is not the case, then leaving the bounding approach in the top scenarios would result in a CC-I finding for one or more SRs.

2.2 Approach 2 - Scoping Approach

ALL OF THE MATERIAL HIGHLIGHTED IN YELLOW WILL BE REPLACED WITH A NEW APPROACH, CURRENTLY SUBJECT OF A SEPARATE WHITE PAPER, ONCE AGREED TO WITH NRC.

One of the fundamental modeling questions that has been raised by the NRC is whether the use of the NUREG-1921 screening approach and 0.1 HEP is representative for all MCR evacuation scenarios. The NRC has suggested using the scoping flowcharts presented in section 5.2.7 and 5.2.8 of NUREG-1921 to provide a more detailed HRA analysis. Since these scoping flowcharts generally produce HEPs of 0.2 and 0.4 if there are any actions needed in the first 30 minutes, and even higher values in cases where the time margin is limited, time is an important parameter that must be considered when using the scoping approach and requires performing a check to look for time critical actions where the time required is close to the time available. While the general HRA process and associated HRA methods address this, delays in processing multiple cues and deciding to abandon can impose a significant change to the timelines. This challenge or change is unique to MCR abandonment.

Many plants have used the screening approach for the detailed human reliability analysis (HRA) quantification per Section 5.1.3 of NUREG-1921. Because the screening approach yields values lower than the scoping approach, the screening approach is susceptible to additional scrutiny. However, before jumping to a detailed HRA approach, it should be pointed out that if the MCR Abandonment scenarios developed from the scoping approach are not risk-significant (as defined in the combined PRA Standard) then a bounding, screening or scoping approach is appropriate and can be deemed as achieving an overall assessment of CC-II for the MCR abandonment evaluation (since risk-significant scenarios are not impacted). Similarly, if this is not the case, then leaving the scoping approach in the risk-significant scenarios would result in a CC-I finding for one or more SRs.

In this approach, the Fire PRA should develop the remote shutdown failure probability for main control room (MCR) evacuation scenarios by summing the contribution of hardware failures with the failure probability for operator actions. The hardware failures can be quantified separately (typically as a cutset equation) for each scenario or for a bounding scenario, accounting for the fire-induced damage to equipment. The set of all operator actions necessary to provide safe shutdown of the plant from outside of the MCR can be modeled as a single human failure event

Formatted: Font: Bold, Font color: Red

Formatted: Highlight

with an overall human error probability (HEP) as established by the scoping approach.

This approach can be used for LOH or LOC scenarios. However, when applied to the LOC scenarios, an additional 0.1 needs to be added to the HEP to account for the fact that the scoping approach does not include the cognitive component for the decision to abandon the control room in the HEP. For LOH scenarios the decision to abandon is considered to negligible since the fire conditions would force the abandonment (e.g., smoke, heat). Once again, the question is whether, with these scoping values applied, the CDF/LERF associated with LOH or LOC scenarios is so small that it does not contribute significantly to the overall fire risk. If this is the case, then the use of the scoping approach is justified even though it is conservative since the conservatism does not affect the fire risk insights and conclusions from the PRA. As shown on the LOH and LOC flow charts, this is determined by applying the scoping HEP to the scenario(s) frequency of each MCR and ASD area scenario that leads to LOH or LOC and asking if the contribution is significant. If not, then the scopingbounding approach is acceptable.

The implications regarding CC-II or CC-I for the overall HRA are the same as for the bounding approach.

2.3 Approach 3 - Detailed Approach

There are two levels of detailed analysis that can be applied; a single HFE covering all abandonment scenarios or multiple HFEs to address nuances of the various abandonment scenarios. When applied to all risk-significant scenarios, either one will achieve an overall assessment of CC-II, and in fact applying one of these approaches to all risk significant scenarios is a requirement in order to achieve CC-II. Note that there is nothing that prohibits performing a detailed HRA for each of the LOH and LOC scenarios, even if the bounding or scoping approach would be sufficient. This application of bounding or scoping values to non-significant scenarios is a permissive, not a requirement. This is noted on the flow charts.

Regardless of how the detailed HRA is implemented, it is extremely important to perform a check to look for time critical actions where the time required is close to the time available. While the general HRA process and associated HRA methods address this, the delays in processing multiple cues and deciding to abandon can impose a significant change to the timelines. This challenge or change is unique to MCR abandonment.

2.3.1 Cognitive Failure - Failure to Abandon the Control Room in Time to Execute a Successful Shutdown

There are two cases related to failure to abandon. One is for LOH and one is for LOC.

~~Case 1 - For A~~abandonment due to loss of habitability~~. For the first situation~~ it is not necessary to consider the possibility that the control room will not be abandoned. These conditions will result in scenarios where it is physically impossible for the operators to remain in the MCR without risking serious physical harm. In general, plant procedures and training provide specific cues to indicate an abandonment condition. Further, NUREG/CR-6850 defines the conditions that would force abandonment. There have been no issues raised with regard to its application. Based on that guidance, it is concluded that it is not credible that the operators will remain in the MCR under such conditions. Therefore, the probability of abandonment due to loss of habitability is not based on the HRA, but rather developed by establishing and justifying the fire conditions that would force abandonment (e.g., smoke, heat) and using probabilistic fire modeling techniques to assess the conditional probability that MCR fire scenarios would lead to abandonment due to loss of habitability. This is why the detailed HRA section of the ~~LOH~~ flow chart does not mention assessment of a cognitive HEP.

~~*Case 2 - Abandonment due to loss of control.* For the second condition, it is necessary to calculate the probability of failure to abandon using currently accepted human reliability analysis methods. The procedures for abandonment due to loss of control do not provide specific cues that call for abandonment, but rather allow discretion in this regard. Because of the variation in procedures, training, crew dynamics, and culture from plant-to-plant, a detailed HRA is needed for determining this human error probability. This detailed HRA would be plant specific, as it is not believed that there is a technical basis for a single generic HEP for cognitive failure to abandon on loss of control that could be applied across all plants (or even all plants of a specific design).~~

~~Regardless of which HRA method is used for quantification, the qualitative analysis needs to include procedure reviews and carefully structured interviews with operations staff to assess the process by which this decision would be made (for example, how do they interpret the way to make the decision, what cues or occurrences would they consider in determining if a loss of control had occurred, what conditions would they use to justify remaining in the control room in the face of a loss of control, etc.). Consideration should also be given to insights from training staff on MCR abandonment and the information that may be available from simulator runs, including timing data (although this must be considered in the context of training with potential stops and starts for scenario discussions with the crew).~~

~~Great care must be taken in the application of currently available HRA quantification methods to ensure the qualitative analysis is captured correctly in the quantification. There is no requirement to use any specific quantification method or combination of methods, and consideration should be given to the use of advanced HRA methods that go beyond those that are most commonly used.~~

Formatted: Font: Not Italic

Formatted: Indent: Left: 0.25"

Whatever approach is chosen, the HRA method must address all of the relevant performance shaping factors. It is recognized, in NUREG-1921 that the decision to abandon is a complicated issue that is challenging to model and approaches the limits of applicability of many of the existing HRA methods. This is because the decision to abandon is at the discretion of the operations staff, does not have strict cues specified in the procedures, and there would generally be some reluctance for the operators to leave the control room. Therefore, it is recommended that a minimum HEP of 1E-2 should be applied as the failure probability associated with the decision to abandon following a loss of control if the quantification process results in a lower value.

While the specific conditions being diagnosed would vary by fire scenario in terms of equipment damaged and instrumentation available, given that all the scenarios are loss of control they would, by definition, involve multiple failures of important safe shutdown components. Whether the loss of control resulted from a fire in the MCR versus in another ASD area, the loss of control is likely to be based on the same set of safe shutdown components, and their associated set of instrumentation.[3] Therefore, it is ***not*** necessary to determine the cognitive failure HEP for this on a scenario-by-scenario basis, but in keeping with accepted practice for non-abandonment HEPs, separate cognitive HEPs should be developed for the MCR fire scenarios (that result in LOC, but not LOH) versus the non-MCR ASD area scenarios. A single HEP for failing to abandon on loss of control is also acceptable if it is based on the MCR LOC scenarios. This would be slightly conservative for the non-MCR LOC cases, but in the overall context of cognitive and execution contributions this is unlikely to be a significant conservatism.

Failure to abandon in time to perform the necessary ex-control room actions required to avoid core damage would lead directly to core damage. Note that most plants only permit abandonment for loss of control for fires in certain plant areas, where it has been determined that fire damage leading to loss of control is of significant concern. Abandonment credit is only applied to fires in these areas.

2.3.2 Execution Failure - Given abandonment, failure to successfully achieve a state that avoids core damage

[3] This is a reasonable conclusion based on FPRAs performed to date, which indicate that the situation on loss of control is essentially the same in all cases – critical front line safety functions required to protect the core are lost and there are significant losses of instrumentation and indication in the control room. This is the nature of the combination of the impact of the fire with the routing of cables in the plant. In the areas where loss of control is an issue, control and instrumentation cables related to equipment and parameters tend to be routed in general proximity. So, while it is theoretically possible there could be loss of control scenarios with different levels of available instrumentation and timing, the reality is that this is not the case in actual practice. For this reason, we believe that the use of a single cognitive HEP for all loss of control scenarios is a justified simplification for fire PRAs.

Formatted: Indent: Left: 0.5"

This is the execution aspect of the abandonment action. The human failure event associated with this action consists of both failures to perform the proper actions and also equipment failures that prevent the operators from being successful in avoiding core damage using the abandonment procedures.

Operator Execution Action Categories. The operator actions for each scenario can generally be grouped into three categories:

- Category 1 – Actions Needed for All Scenarios. This category of actions consists of those required to restore decay heat removal (such as AFW in a PWR, torus cooling in a BWR), injection (such as CVCS in a PWR, RCIC in a BWR) and associated support systems; which are the minimum set of systems necessary to provide safe shutdown. Failure to provide any of these actions is modeled in the PRA as leading to core uncovery. These actions are required for all control room evacuation scenarios, can be evaluated using detailed HRA, and then can be incorporated back into the Fire PRA as a single basic event or as multiple events (see options below). The detailed analysis of these execution errors can be accomplished following the NUREG-1921 guidelines.

- Category 2 – Actions Needed for Some Scenarios. This category of actions consists of those that may be required in order to support the Category 1 actions, but in certain scenarios may not be available. For example, there may be a need to restore power to a bus in order to restore AFW. It would be expected in this case that once the power had been restored to the bus, the AFW actions would still be required (that is, AFW would not simply automatically start when power was restored). However, some scenarios may not be accompanied by failure of the bus power, and so failing to perform those actions would not result in failure to restore AFW. As with Category 1 actions, these can be evaluated using detailed HRA, and then can be incorporated back into the Fire PRA as part of the single basic event or as multiple events.

- Category 3 – Additional Actions Needed to Mitigate Spurious Actuations. This category of actions is modeled in addition to the actions taken for all scenarios (Category 1). This category consists of actions required to mitigate spurious equipment actuation and restore the RCS and SG boundaries to a state where the AFW and CVCS systems can provide for safe shutdown. This category of actions for PWRs includes reactor coolant pump trip, isolation of RCS boundary valves (pressurizer PORV, RCS head vent, pressurizer vent, and RCS letdown), isolation of the SG's (closure of open MSIVs, closure of open SG-ADVs, and closure of open SG blowdown valves), and termination of spurious safety injection. An example action for BWRs would be isolation of spurious SRVs. These actions are required only when fire damage causes a spurious event which must be terminated. The HFE's for these events are modeled in the logic along with the component failure modeling the spurious event. The detailed analysis of these execution errors can be accomplished following the NUREG-1921 guidelines.

Therefore, each action required by the abandonment procedure should be considered.

2.3.3 Performing the Detailed Analysis

There are three options that can be used to perform the detailed analysis in the FPRA.~~, all of which are sufficiently realistic that they would achieve an overall assessment of CC-II for the treatment of MCR abandonment even when applied to risk-significant scenarios.~~

- Option 1 - The first option would be to model the failure to achieve successful shutdown as a single HFE, with all the execution actions required for shutdown analyzed as part of that HFE.[4] That is, it is acceptable to develop a single HEP, developed from a detailed human reliability analysis, that assumes that all the actions required for shutdown are always needed for all scenarios. In this case, all of the Category 1, 2, and 3 actions would be included in the single HEP, and applied to all abandonment scenarios. This would be somewhat conservative, but not overly so~~, and so would still be expected to meet CC-II~~. When using Option 1, developing the HEP is only part of the modeling. While the HRA is detailed, the logic modeling is simplified by applying the failure as a single event leading to core damage. For this reason, it is necessary that the overall probability of core damage encompass both the probability of human failure in the execution steps and the failure probability of the equipment. Therefore, for each execution activity the random failure probability of the required equipment needs to be added to the HEP, unless it can be shown numerically that the contribution is insignificant.

  This option would be most useful to those plants that have already chosen to use 0.1 as the generic failure probability for abandonment. The information that is gathered in order to demonstrate feasibility provides sufficient basis to perform a reasonably detailed HRA in order to develop an HEP to either confirm the applicability of the 0.1 or to replace it with an appropriate value. ~~Note that if the single value is to be used for both LOC and LOH, it needs to be shown that the cognitive failure portion applicable to LOC is not significant to the total HEP.~~

[4] Note that this is unlikely to be all actions taken during abandonment. It is expected that some actions that are taken are to protect equipment, and failure to perform those actions would not result in core damage. Therefore, these would not need to be considered in the analysis.

- Option 2 - It is noted that in reality different scenarios may result in only a subset of the actions being required (even though there is a loss of control, a particular system may not fail, and so the actions taken to recover that system may not be required for that specific scenario). It is therefore acceptable to develop different "flavors" of the single HEP, developed from a detailed human reliability analysis, with scenario-specific considerations. Under this option, the scenarios would be "binned" into groups where a single execution HEP could be applied to the entire bin. ~~Because of fundamental differences in the LOH versus LOC context, the binning approach would be different.~~

  The LOH ~~case~~situation would have a wide range of damage conditions to consider, since in fact LOH could result from a fire in a relatively unimportant area of the control room (that is, minimal impact on the functions required to successfully shut down) all the way to areas where the damage ~~is very close to, but not all the way to, an LOC condition~~is very significant in terms of lost systems, functions, and indication. Thus, the difficulty in achieving successful shutdown once the control room was abandoned would vary greatly. Because of this, ~~I~~in applying option 2~~ to LOH~~, a useful surrogate for the extent of damage (and thus the difficulty in shutdown) is the CCDP of the equivalent scenario that does not lead to LOH. This is shown under Option 2 on the ~~LOH~~ flow chart. The application of this method is discussed later in this FAQ, in the discussion of application guidance~~ for abandonment due to LOH~~.

  ~~The LOC case is different, in that the extent of damage and the CPLOCs are very similar. There are, however, key differences in the complexity of the response that could result from an LOC scenario. Taking the three categories of actions previously discussed, the Category 1 actions are always required, but Category 2 and 3 may not be. Therefore, the scenarios can be binned as follows:~~

  - ~~Only Category 1 actions required~~
  - ~~Only Category 1 & 2 actions required~~
  - ~~Only Category 1 & 3 actions required~~
  - ~~Category 1, 2, & 3 actions required~~

  ~~This is shown under Option 2 on the LOC flowchart.~~

  As with Option 1, ~~whether it is for LOH or LOC, ~~developing the HEP is only part of the modeling. While in this option there are multiple versions of the HRA modeling, the logic modeling is still simplified by applying the failure as a single event leading to core damage to each scenario. For this reason, it is necessary that the overall probability of core damage for each variation encompass both the probability of human failure in the execution steps and the failure probability of the equipment. Therefore, for each execution activity the random failure probability of the required equipment needs to be added to the HEP.

- Option 3 - Another way to address scenario-specific considerations would be to break down the actions in the abandonment procedure by system/function and have a separate HFE for failing to recover each system/function. This approach would address the case where, for a given scenario, a system did not fail due to fire. If the system did not fail, the failure of the action would not fail the system, and this would be handled in the logic model. The model would have to account for fire-induced failures that were not recoverable, so that the HFE was not improperly credited.

It is also necessary to determine that all of the actions will work if properly executed, so the analysis needs to account for fire damage that would fail the action regardless of what the operators do, and not credit the remote shutdown in those cases.

~~*2.3.4 Special Topic - Cognitive Error of Commission - Premature/improper abandonment of the control room*~~

~~There is one other consideration when assessing control room abandonment that needs to be addressed. If the plant procedures allow the operators to abandon the MCR when the operators believe that they have lost control of the plant, there is always a possibility that they will misinterpret the available information and determine that there is a loss of control when, in fact, this is not the case.~~

~~This applies only to the situation where abandonment due to LOC would be permitted under plant procedures. As discussed above, most plants only permit LOC abandonment for fires in areas where the potential for a fire-induced LOC is high (the ASD areas). When fires occur in such areas, it is possible that a fire may lead to significant impact on plant equipment, but not result in LOC. In such cases, it is possible that the operations staff may misinterpret the situation and believe that a LOC has occurred, and decide to abandon.~~

~~While it is possible to calculate the probability of premature abandonment using currently accepted human reliability analysis methods, in almost all cases this will not be necessary. The procedures for abandonment due to LOC do not provide specific cues that call for abandonment, but rather allow discretion in this regard. While there is a variation in procedures, training, crew dynamics, and culture from plant-to-plant, the combination of the discretion allowed and the general reluctance of operators to leave the control room (as indicated by interviews conducted at a number of plants), it is considered much more likely that the operators would fail to abandon on LOC than that they would abandon the control room for something less than total LOC. As justification for this conclusion, interviews should be conducted to confirm that the predisposition to remain in the control room for the most likely "non-LOC" scenarios is true.~~

~~In addition, it should be noted that a premature abandonment does not lead directly to core damage. Rather, it only results in the inability to take advantage of the remaining available actions that could be successful from the control room. In this situation, core damage can still be averted using the actions in the abandonment procedure, so that core damage only occurs if the control room is prematurely abandoned ***and*** execution actions also fail, taking into consideration that some of the MCR functions and automatic actions would still be available since a loss of control has not occurred. Given these considerations, there is no need to consider premature abandonment unless there is compelling evidence that plant procedures and training, and resulting operator pre-disposition, is such that an error-forcing context exists. If this condition is met, then not including premature abandonment would still achieve CC-II, since the exclusion would not result in missing any important risk contributors.~~

~~None of this prevents a licensee from deciding that they desire to explicitly model premature abandonment using currently accepted human reliability analysis methods if they so desire, or if there is compelling evidence that an error-forcing context exists with respect to premature abandonment. However, this is an even more challenging application for the use of the most commonly applied HRA quantification methods than the case of failure to abandon on loss of control. Therefore, even more care must be taken in determining the context and how to apply it, and very serious consideration should be given to using advanced HRA methods that have been developed in recent years and would be more applicable to this type of error. That being said, there is no requirement to use any specific quantification method or combination of methods, but whatever approach is chosen must address all of the relevant performance shaping factors and used in such a way that its application to quantification of a cognitive error of commission can be justified.~~

~~While the specific conditions being diagnosed would vary by fire scenario in terms of equipment damaged and instrumentation available, it is ***not*** necessary to determine an HEP for this on a scenario-by-scenario basis. A single HEP for premature abandonment is acceptable. Abandoning the MCR prematurely means that the only actions credited in the MCR are those immediate actions called for in the abandonment procedure as being performed as part of the abandonment process. No other MCR actions would be credited. Note that these actions may not work (see section on failure to achieve a state that avoids core damage, given abandonment).~~

3.0 Application Guidance

This section provides additional guidance related to the implementation of the abandonment credit in the FPRA model.

3.1 Guidance on limitations to the application of abandonment credit ~~for abandonment due to loss of habitability~~

Most remote shutdown capabilities are designed to achieve successful shutdown only under general transient conditions and may not have considered the impact of multiple spurious operations on the equipment relied upon for remote shutdown. Therefore, in general, no credit for remote shutdown should be applied for conditions such as ATWS, LOCA, interfacing systems LOCA, or main steamline break conditions (e.g., unisolated stuck open atmospheric relief valves for PWRs) or in cases where fire damage (e.g., multiple spurious operations) could result in unrecoverable loss of the remote shutdown capability. Therefore, if the fire causes these conditions and they are not recoverable as part of the abandonment procedure, then core damage should be assumed. An assessment of the conditions that would preclude success would be determined for the specific plant, and the model developed to reflect that abandonment credit could not be applied to fire scenarios that caused these conditions. This is represented on the ~~LOH~~ flow chart by the decision diamond labeled "Scenario(s) within RSD capability?" where an answer of No leads to the terminus labeled "No credit for abandonment."

Example: Three plants have the following situations under the condition of a fire induced PORV LOCA (a fire scenario that causes spurious opening of a PORV along with failure of a block valve). None of them can reach a safe condition from outside the control room with the LOCA in progress.

- Plant A – The design of the circuit is such that there is no action that can be taken to clear the fault and allow the PORV to reclose. For the LOH scenarios that cause this condition, no credit can be given for shutdown from outside the control room (core damage will occur).
- Plant B – The design of the circuit is such that it is possible to pull a fuse to clear the fault and allow the PORV to reclose, but that action is not in any procedure. For the LOH scenarios that cause this condition, no credit can be given for shutdown from outside the control room (core damage will occur), but if the plant modifies the procedure to include pulling the fuses and it is determined to be feasible, then credit can be applied.
- Plant C – The circuit includes a disconnect switch that will always clear the fault and allow the PORV to reclose, and the action to throw the disconnect switch is part of the abandonment procedure. For the LOH scenarios that cause this condition, credit can be given for shutdown from outside the control room.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Font: Arial

3.2 Guidance on the use of detailed HRA option 2 - binning

Any of the execution failure analysis options previously discussed can be applied to failure during abandonment due to loss of habitability. However, the use of Option 2 does have certain advantages for the abandonment due to loss of habitability case. The various scenarios that would cause abandonment due to loss of habitability can result in widely different levels of plant damage, from almost no effect on key safety systems up to and including a loss of control. The extent of fire damage is indicated by the non-abandonment CCDP of the scenario. The failure of execution could therefore be based on CCDP that is obtained before taking the abandonment credit. The higher the CCDP, the more actions that would be required upon leaving the control room. For example, the scenarios can be placed in three bins, and then three shutdown execution failure HEPs used. The selection of the three values would be based on Option 2 of the execution failure analysis approach previously discussed.

Calculated CCDP (non-abandonment)	Abandonment CCDP used for risk quantification	Basis for CCDP used
CCDP < x	z_1	A CCDP of less than "x" is consistent with a less challenging event that would not have time critical actions.
y >CCDP ≥ x	z_2	A CCDP of "x" or greater but not greater than "y" indicates a more significant consequence associated with challenges caused by the fire.
CCDP ≥ y	1.0	A CCDP of "y" or greater indicates significant consequences with the potential for time critical action. The treatment of such events given abandonment of the MCR could also be expected to have large uncertainty. A conservative treatment assumes such events are not recoverable.

The values for x and y would be specified on a plant specific basis by reviewing the scenario CCDP results for the non-abandonment MCR scenarios and identifying logical break points for damage. This would result in the scenarios each being assigned to a bin. The values for z_1 and z_2 would be based on the most restrictive scenario in each bin. For the top bin, it is clear that the most restrictive scenario would be non-recoverable, so 1.0 would be used for this bin.

Note that the selection of only three bins, as discussed above and shown on the flow chart, is only an example. Should it be determined though examination of the LOH scenarios at a given plant that there are a greater number of damage states that could be considered, then additional damage states could be defined.

This approach could also be applied by using fire location in the MCR as opposed to CCDP (i.e., which panels are affected and the associated damage to plant systems).

3.2 Guidance on the application of abandonment credit for abandonment due to loss of control.

The first consideration in granting credit is the location of the fire in relation to the instructions in the abandonment procedure. Most procedures direct abandonment only in the case of fires in specific plant areas (generally referred to as the alternate shutdown, or ASD, areas). If the procedure is written in this fashion, then credit can only be applied for fires in these areas.

The second consideration is the plant condition under which the remote shutdown is to occur. Most remote shutdown capabilities are designed to achieve successful shutdown only under general transient conditions and may not have considered the impact of multiple spurious operations on the equipment relied upon for remote shutdown. Therefore, in general, no credit for remote shutdown should be applied for conditions such as ATWS, LOCA, interfacing systems LOCA, or main steamline break conditions (e.g., unisolated stuck open atmospheric relief valves for PWRs). Therefore, if the fire causes these conditions and they are not recoverable as part of the abandonment procedure, then core damage should be assumed. An assessment of the conditions that would preclude success would be determined for the specific plant, and the model developed to reflect that abandonment credit could not be applied to fire scenarios that caused these conditions.

Finally, there is the question of applying the remote shutdown credit to the specific scenarios. There are two modeling techniques that can be used, and the selection of the most realistic approach for any given plant may depend on the results of the operator interviews.

- One technique is to apply the credit to all "recoverable" scenarios in the area based on the fact that all cutsets generated by the scenario prior to the application of the remote shutdown represent core damage. Therefore, they involve a loss of control of the plant. The operators do not know whether the failures that result in this condition are due to fire damage or random causes, they only know that there is a fire in an abandonment area, and the plant is headed to core damage. Under these conditions, it can be assumed that abandonment may be ordered. Although this allows credit to be taken for all scenarios, it also does not grant any credit for any in-MCR actions that may be possible prior to abandonment, other than the immediate actions and the specifically identified in-MCR actions that are performed while abandoning.

- The second technique is to apply credit based on the CPLOC, which in a way is a measure of "how close" the plant is to core damage as a result of only the equipment damage directly associated with the fire (this is not strictly true, because some of the contribution to the CPLOC is due to some of the fire damage being probabilistic - i.e., hot shorts, so in fact the cutset CPLOC actually includes fire damage that has occurred).

~~In this approach, the credit is applied only to the high CPLOC scenarios on the premise that these will cause a greater level of confusion and a more likely judgment that control has been lost and a decision made to abandon. The determination for when this point might be reached (in terms of the situation the operators may be facing in the control room) would need to be established on a plant specific basis through operator interviews intended to ascertain what the operations team would consider to be indicative of a "loss-of-control" condition. Then, the scenarios would be reviewed to determine ifthere is a level of CPLOC that can generally be associated with that level of damage. For example, the operators could indicate that they would base the decision to abandon on certain parameter values and trends and certain controls not responding. The review of the dominant scenarios in the alternate shutdown areas could identify that (at this plant) this extent of damage is generally associated with scenarios of CPLOC greater than a particular value (before crediting abandonment). Therefore, in this example case, abandonment credit should be taken for scenarios with pre-abandonment CPLOC greater than that value. Conversely, the extent of damage associated with scenarios of CPLOC less than that value (without abandonment) is such that the operators would believe that they still had control of the plant until it was too late to successfully shut down remotely, and thus no credit would be applied. The determination of the appropriate CPLOC would need to be made for each plant based on the abandonment criteria and the operator interviews.~~

3.3 Dependency

As some of the cutsets leading to loss of control due to fire may contain human failure events, dependency analysis needs to be considered in the application of credit for abandonment. For example, in a PWR, if the fire causes a loss of secondary heat removal and the reason that secondary heat removal is not recovered is because of a failure to recover AFW (i.e., the cutset includes a HFE for failure to recover an AFW pump train), then the decision on whether to abandon would be affected by the operator's failure to diagnose that there is a loss of all secondary heat removal. This would influence the decision to abandon, and would therefore need to be evaluated and accounted for in the dependency analysis.

If appropriate, provide proposed rewording of guidance for inclusion in the next Revision:

Not applicable. There is no current guidance beyond RG 1.200.