

FAQ Number 13-0002

FAQ Revision 01

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

Plant: Various

Date: 3 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.

Relevant NRC document(s):

NUREG-1921, NUREG/CR-6850

Details:

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

NUREG-1921 and NUREG/CR-6850, specifically they regard 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/scoping values for HEPs for non-significant MCR scenarios. **The guidance is specifically found as follows:**

NUREG-1921, specifically Sections 4.8, 5.1.3, 5.2 and 5.3 as it regards assessment of MCR abandonment, **and Section 4.3 as it regards feasibility assessment.**

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

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

NUREG/CR-6850 is needed. In the interests of reaching agreement between the industry and NRC as to how the modeling can be done 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 ~~difficult~~ **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 fire scenarios that led to evacuation due to loss of habitability (LOH). Several reviews have questioned the validity of applying a single representative HEP (or CCDP) 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 ~~in the scope of this addressed in this FAQ~~ **as they are related to LOC**.

The term "MCR abandonment 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)

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

- 2) Demand for abandonment due to loss of habitability (LOH). (Addressed in this FAQ)
- 3) Operator decision to abandon or not abandon. (For LOH scenarios, not an issue; therefore out of scope of 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. Actions performed at a remote shutdown panel or local control stations to establish front-line systems to mitigate a transient loss of decay heat removal. (Addressed in this FAQ)
 - b. Actions performed to 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)

Comment [O1]: If this action is supposed to represent those actions needed for "switchover" of control outside MCR, we ought to state this explicitly. All switchover actions should be represented. If this action isn't intended to represent that, the "switchover" action(s) needs to be identified explicitly.

Specific circumstances requiring interpretation or new guidance:

- When a screening/scoping 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 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~~

FAQ Number 13-0002

FAQ Revision 01

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

~~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 ~~briefly discusses when provides guidance for it might be appropriate to model ing~~ 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. ~~According to NUREG-1921~~ ~~Namely, such an approach may be sufficient if all operator actions have been shown to be feasible and MCR abandonment is shown to be not risk significant.~~

~~Historically, t~~he 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 ~~approach 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.~~

Comment [02]: This approach is NOT from NUREG-1921. Several authors didn't want this approach to be included. The only reason it was included was because it was a holdover from the NUREG/CR-6850 screening approach.

Comment [J3]: Several cases in 1921 produce an HEP less than 0.1.

Comment [J4]: Even a screening approach requires adequate justification.

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) 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

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

addressed in this FAQ and can be modeled with typical Fire HRA considerations as described in NUREG-1921.

MCR 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. In particular, for LOH 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. As discussed later, this failure is not a concern for abandonment due to loss of habitability (LOH).

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, including the cognitive component
- Failure of equipment required to effect a successful shutdown.

- For LOH, there is no contribution from the failure to diagnose and decide to abandon the control room in time to execute a successful shutdown. As discussed later, this failure is not a concern for abandonment due to loss of habitability (LOH).

Appropriate modeling for each of these is outlined in Figure 1. 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.

Formatted: Font: (Default) Arial

Comment [05]: I realize that we're talking about the PRA Standard here. However, the NRC differs in thinking that there are three aspects: 1) the decision, 2) actions needed for the switchover, and 3) all diagnosis (including supervisory coordination & communications) & actions associated with successful shutdown.

Formatted: Font: (Default) Arial, 12 pt

Formatted: Font: (Default) Arial

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Arial, 12 pt

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Arial

Formatted: Normal, Indent: Left: 0.25", Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Arial, 12 pt

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: (Default) Arial

Formatted: Normal, Indent: Left: 0.25", No bullets or numbering

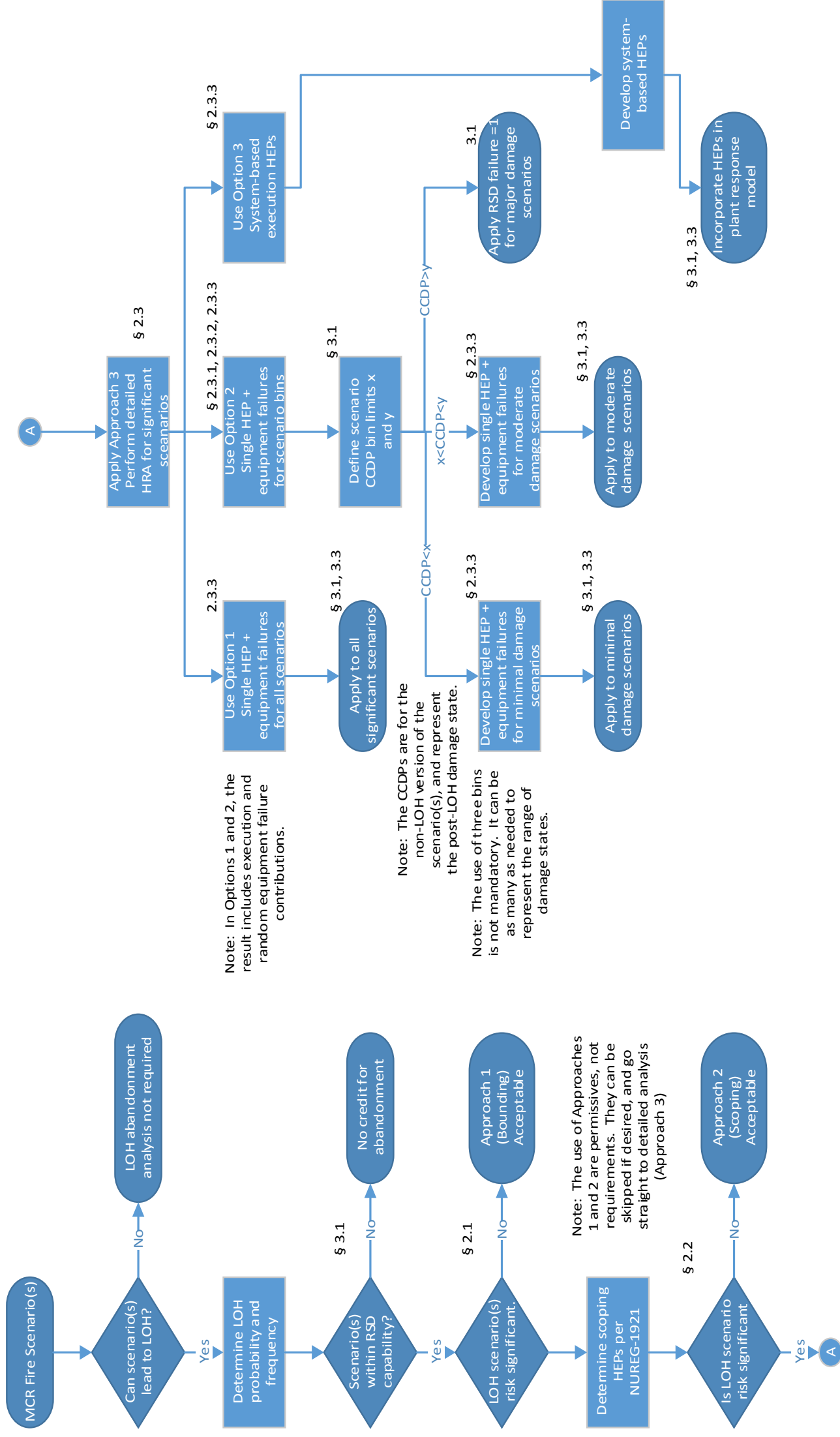
Formatted: Font: Arial, 12 pt

Formatted: Font: Arial, 12 pt

Formatted: Font: Arial

Comment [06]: We need to have discussion regarding the figure. It's not clear first of all, why a single HEP constitutes a detailed HRA analysis. We need to understand the rationale here. Secondly, the discussion under Option 2 of Approach 3 seems to be overblown. We do not understand the need for such a complex addition to the table.

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



FAQ Title Modeling of Control Room Abandonment

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.

Comment [J7]: What does this mean?

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 flow chart is applied to each fire scenario (or group of similar scenarios) that occurs in the control room.

Comment [O8]: I would recommend including this in the FAQ only if there's something new or unique about the treatment for MCR Abandonment, as opposed to the rest of the fire PRA.

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

Comment [O9]: A discussion of feasibility assessment for abandonment should be included somewhere; maybe here or in a separate section.

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

When applied to abandonment due to LOH, 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. 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 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.~~

Comment [J10]: Approach 1 used when not risk significant. The additional discussion confuses the issue and was deleted.

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.

Comment [O11]: NRC will not comment on the yellow material since it is to be replaced. However, note that 1921 can provide smaller or comparable failure probabilities to 0.1 for transfer/ASD for certain plant configurations.

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

Once again, the question is whether, with these scoping values applied, the CDF/LERF associated with LOH 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 ~~if 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 applying the scoping HEP to the scenario(s) frequency of each MCR scenario that leads to LOH and asking if the contribution is significant. ~~If not, then the scoping approach is acceptable.~~

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. Note that there is nothing that prohibits performing a detailed HRA for each of the LOH 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 chart.

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

For abandonment due to loss of habitability it is not necessary to consider the possibility that the control room will not be abandoned. These conditions will result

Comment [J12]: Don't get this sentence

Comment [O13]: Again, we're not sure of the how behind developing the single HFE. Need to understand as discussed earlier with regards to the figure. The PRA Standard says that detailed analysis needs to address the scenario specific aspects that influence operator actions.

Comment [J14]: Deciding to abandon is not an issue in LOH. What is the point here?

FAQ Title Modeling of Control Room Abandonment

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. ~~Thus is why~~, the detailed HRA section of the flow chart does not mention assessment of a cognitive HEP ~~for the choice to abandon the MCR under LOH conditions~~.

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

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 uncover. 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

Comment [O15]: This statement is too strong & I'm not certain how generic it is. Procedural and training support for abandonment for LOH is not strong or clear & we shouldn't say otherwise.

Comment [O16]: I disagree with the implication that procedures or training provide "guidance" on MCR abandonment for LOH.

Comment [O17]: Just because a decision to abandonment the MCR has been made doesn't mean all decision-making is over. A cognitive contribution to operator failure still needs to be addressed for remaining actions.

Comment [O18]: Where are the actions to successfully accomplish switching control from MCR to elsewhere?

Comment [O19]: We don't understand how these categories can be used as there are other important factors as we've discussed in our meetings. Thus, we don't think there's an advantage to formalizing this strategy in the FAQ.

Comment [O20]: Are you absolutely certain there is no diagnosis at all?

FAQ Title Modeling of Control Room Abandonment

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.

- 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.¹ 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. 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

Comment [J21]: What is the mechanism that causes the RCP to spuriously trip?

Comment [O22]: Prior comment on detailed analysis. Need to understand how you're doing this. Are you estimating HEPs for scenarios and somehow rolling them up into a single value? Or is the intent to establish a single HEP in another fashion? How are equipment failures treated?

¹ 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.

FAQ Title Modeling of Control Room Abandonment

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.

- 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.

The LOH 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 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, in applying option 2, 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 flow chart. The application of this method is discussed later in this FAQ, in the discussion of application guidance.

As with Option 1, 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

Comment [O23]: Why are we talking about LOC?

Comment [J24]: Again, how is the single HEP developed? CCDP?

Comment [O25]: What about cognition?

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.

3.0 Application Guidance

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

3.1 Guidance on limitations to the application of abandonment credit

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 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),

FAQ Title Modeling of Control Room Abandonment

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.

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.

Comment [O26]: There is no discussion on option 3. Should provide a section to simply say it's not being discussed in this FAQ.

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.
$y > \text{CCDP} \geq x$	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 $\geq y$	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.

Comment [J27]: The table seems like overkill. Isn't the point to map sequences on MCR abandonment, and to use the most restrictive scenario from the bin for quantification? What else is the table conveying.

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.

Comment [J28]: How is the fact that each bin contains many scenarios factored into this surrogate CCDP?

Comment [J29]: I'm afraid that this part of the approach is confusing to me, especially without explicitly defining z1 & z2.

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 through 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).

Comment [J30]: Don't understand. Fire location and CCDP are separate items, one does not imply the other.

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.

Comment [J31]: LOH is rather well defined. Since this sentence refers to a function, are you discussing LOC, which is out of scope?

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

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