MODELING MAIN CONTROL ROOM ABANDONMENT DUE TO FIRE-INDUCED LOSS OF CONTROL IN FIRE PROBABILISTIC RISK ASSESSMENT

Pierre Macheret[1], Erin Collins[2]

[1] *JENSEN HUGHES, 376 East Warm Springs Road, Suite 210, Las Vegas, Nevada, 89119, pmacheret@jensenhughes.com*
[2] *JENSEN HUGHES, 3610 Commerce Drive, Suite 817, Baltimore, Maryland, 21227, ecollins@jensenhughes.com*

In fire probabilistic risk assessments, the human reliability analysis (HRA) of main control room abandonment due to fire-induced loss of control hinges in great part on the timing performance shaping factor, i.e., the evaluation of the time required vs. time available to perform human actions. The present paper summarizes key aspects of a method that was recently applied for such an HRA performed on a boiling water reactor. That evaluation involved 1) defining abandonment criteria for loss of control, and 2) characterizing the multiple timing parameters using an approach where the state of knowledge about each parameter was structured to permit a robust evaluation of the most uncertain parameter. This structured method was intended to improve transparency and traceability, which in turn helped ensure the robustness of the results and confidence that the abandonment risk was adequately represented.

I. OBJECTIVE

In fire probabilistic risk assessments (PRAs), fire scenarios in the main control room (MCR) or the cable spreading room are often risk-significant because cables of redundant safe shutdown trains are co-located in these areas. Such fires may lead to loss of control requiring MCR abandonment and transfer of command and control to a different location in the plant, for example at a remote shutdown panel (RSDP) where alternate shutdown (ASD) activities can be undertaken.

For these scenarios, human actions may require a relatively detailed human reliability analysis (HRA) to provide a sufficiently detailed picture of the plant risk profile. The objective of this paper is to summarize key insights gained from a recent HRA conducted on a boiling water reactor (BWR). The focus is on the timing performance shaping factor (PSF). The approach followed includes two main phases:

- A first phase where the main safety functions of the plant (i.e., reactivity control, pressure and inventory control, decay heat removal) are evaluated to identify the criteria that will lead the operators to realize that control from the MCR is lost and that abandonment is necessary.
- A second phase focusing on the modeling of human failure events (HFEs). This phase must account for uncertainties in timing data, which may lead to a relatively large range of plausible human error probabilities (HEPs). In addition, there are complications due to the interdependence of actions. For example, the timing available for one action may be affected by the timing of another. To overcome these difficulties, an approach is followed that involves 1) the structured evaluation of timing parameters, going from those that have the least amount of uncertainty to those that are the most uncertain, and 2) the construction of a timeline identifying the order of actions and which clarifies their underlying relationships. The application of this approach culminates in an equation where the information on parameters already ascertained is used to estimate the most uncertain parameter. Using this approach helps ensure the robustness of the results and increases the confidence that the abandonment risk is appropriately represented.

II. ESTABLISHMENT OF CRITERIA FOR ABANDONMENT

In contrast to loss of habitability (LOH) fire scenarios, for which the decision to abandon is obvious to the operators because of the physical conditions in the MCR and for which there are very clear criteria in NUREG/CR-6850 (Ref. 1) related to concentration of smoke or room temperature that would result in an inability for the operators to effectively remain in the MCR, loss of control scenarios include the possibility that the decision to abandon may not be taken in a timely manner. That is, this decision may occur too late for core damage to be avoided when command and control is transferred to the RSDP, and as such, the probability of failing to abandon the MCR in time needs to be evaluated in the fire PRA.

To do this, criteria for abandonment upon loss of control in case of a fire need first to be established.

Such criteria may already be defined in the MCR abandonment procedure used at the plant. However, it is not unusual for the abandonment procedure to avoid prescribing firm criteria, leaving the determination of this decision to operations. For the BWR evaluation that was performed, abandonment was warranted only for fires occurring in the MCR or the Cable Spreading Room (CSR). In addition, the procedure instructed the operators to abandon the MCR after confirmation that the fire had not been contained within 10 minutes of detection. This provision expressed the notion that a fire uncontrolled within 10 minutes would eventually lead to loss of control and that MCR abandonment should not be further delayed. Except for this specificity, the procedure did not have explicit failure criteria for abandonment, and as a consequence some had to be established for the fire PRA, in order to be able to include the abandonment activities in the model.

The development of such criteria is now discussed.

Generally speaking, operators would be expected to abandon the MCR reluctantly, given that it contains the key controls of the plant, has all the procedures readily available, and is the location used every day to control and manage plant operations. Therefore, it is only if control of essential safety functions is lost that the operators will abandon. Among these safety functions are: 1) reactivity control, 2) inventory and pressure control, and 3) decay heat removal.

Reactivity control is not expected to be lost during a fire on a BWR. This is because a challenging fire will typically cause an automatic early reactor scram. In addition, manually scramming the reactor is one of the first actions of the abandonment procedure, and subsequent actions provide a diverse means to quickly ensure reactor trip.

Decay heat removal is essential to ensure that the plant can be brought to safe and stable conditions. However, on BWRs, decay heat removal is not needed until several hours after the onset of the fire. By that time, the fire would be under control and it is not expected that loss of decay heat removal alone would lead to abandoning the MCR.

This leaves inventory control, along with pressure control, as the key safety functions that will determine whether, in case of a BWR fire, the operators need to abandon the MCR due to loss of control and in a relatively short time window. Key items to note are as follows:

- Early injection into the reactor vessel ensures that the fuel rods are maintained at an adequate temperature for several hours. Thus, with high-pressure injection functional, it is unlikely that the operators would need to abandon the MCR.
- Should all credited high-pressure injection systems fail at the beginning of the fire, the operators need to emergency depressurize and establish low pressure injection to avoid core damage. Thus, the failure of high-pressure injection is deemed a necessary criterion for the operators to consider abandoning the MCR.
- The criterion above is however not sufficient alone to warrant abandonment. If the operators can get the reactor to reach, in time, conditions that will allow low-pressure injection systems to provide inventory makeup, MCR abandonment will not be needed. With no safety relief valve (SRV) or main steam isolation valve (MSIV) spuriously opening, this requires manual depressurization. Also, a low-pressure injection system must be available. If spurious opening of SRVs or MSIVs causes a rapid reactor pressure decrease, rendering manual depressurization superfluous, a low-pressure injection system must still be available to provide reactor inventory makeup and avoid core damage.

The above determination that the timeliness of MCR abandonment is controlled by the inventory and pressure control safety functions is used as the basis for developing abandonment criteria. Taking into account the means available to provide water makeup to the reactor vessel, abandonment by loss of control is expected if the following conditions are met:

- Loss of all fire PRA credited high-pressure injection systems in the MCR.

AND

- Emergency depressurization is not available from the MCR.
  OR
- Loss of all fire PRA credited low-pressure injection systems in the MCR.

Stated otherwise, MCR abandonment is not warranted if the criteria above are not met, that is, if:

- High-pressure injection is available.

OR

- Emergency manual depressurization from the MCR is available.
  AND
- Low pressure injection is also operational from the MCR.

III. MODELING OF HUMAN FAILURE EVENTS

III.A. Timing Performance Shaping Factor

HEPs are affected by PSFs, such as timing, human-machine interface, stress, complexity of actions, etc. For the present study, the focus is on the timing PSF. Due to the complications caused by the interdependence of actions (with the timing of an action influencing the time available to perform other actions), this PSF is deemed the most complex to address. The focus on the timing PSF is not to diminish the importance of other PSFs, however. These PSFs require by themselves a specific evaluation, but they are not the object of this paper.

The variables involved in the timing PSF are illustrated in Figure 1, which is based on Ref. 2.

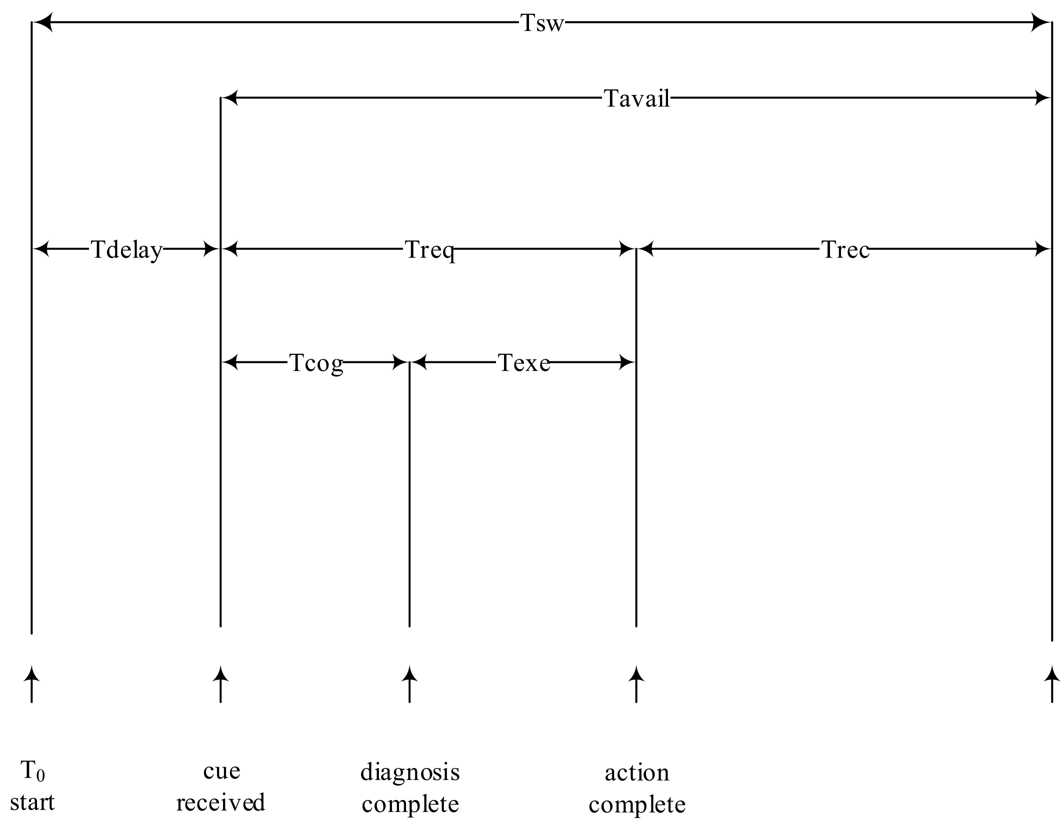

Fig. 1. Human failure event timeline illustration diagram

In Figure 1, the timing elements are as follows:

T_0 = 0, start time or start of the event. A common assumption in PRAs is that failures (and in case of the fire PRA, fire-induced failures) occur at time t=0. Thus, equipment failures that will lead to MCR abandonment by loss of control are assumed to occur at time T_0.

Tsw = system time window. This is the time beyond which the action is no longer useful.

Tdelay = time to cue acknowledgement.

Tcog = cognition time for detection, diagnosis, and decision making.

Texe = execution time. This includes manipulation of equipment, and, as relevant, travel time, donning of personnel protective equipment, and collection of tools.

The knowledge of Tsw, Tdelay, Tcog, and Texe is sufficient to characterize the timing of an HFE. However, complementary timing parameters, which are given below, are also useful for a good understanding of the MCR abandonment HRA:

Treq = Tcog + Texe. This is the time required to perform the action.

Tavail = Tsw – Tdelay. This is the time available to perform the action.

Trec = Tsw – Tdelay – Treq = Tsw – Tdelay – Tcog – Texe. This is the time available to recover the action if performed incorrectly.

III.B. Functional Grouping of Human Failure Events

Multiple actions are associated with MCR abandonment. These actions can be categorized into various groups, as follows:

- Decision to abandon the MCR. As explained previously, the failure to abandon in time in case of loss of control would lead to core damage and needs to be accounted for in the fire PRA.
- Immediate actions after decision to abandon. Before abandoning, the operators will, to the extent possible, take actions intended to facilitate ASD activities from the RSDP. For example, such actions typically include confirming reactor scram, tripping the turbine, closing MSIVs, making a plant-wide announcement that the MCR is being abandoned, and instructing personnel to report to their designated locations for ASD operations.
- Actions aimed at activating the RSDP. This includes getting keys to access the RSDP location, collecting any necessary tools or protective personnel equipment, traveling to the RSDP, ensuring that the RSDP controls are in their correct initial position, and activating the RSDP.
- ASD operations. These include short-term and long-term operations. As discussed previously, with the confirmation that the plant has been successfully tripped, the focus of the operators for short-term actions will be on inventory and pressure control. Ensuring reactor injection may require, as needed, aligning support systems such as electrical power and cooling systems. Long-term operations include decay heat removal, and actions intended to ensure that safe and stable conditions are reached and maintained, such as refilling diesel fuel tanks, replacing nitrogen bottles to support SRV operation, etc.

Because the focus of this paper is on the timing PSF, long-term actions are not considered further and only short-terms actions are now discussed.

Modeling MCR abandonment HRA within a fire PRA is a separate and detailed topic (Ref. 3), but the approach to defining HFEs can be summarized here. To facilitate modeling, individual actions are first grouped functionally to the extent possible. That is, actions related to inventory and pressure control are modeled under the same HFE. Similarly, actions related to aligning power sources are also modeled under a common HFE. Depending on the design of the plant and the nature of the ASD actions, the grouping of actions may be different. For example, it may happen that the actions supporting inventory control are performed in two different locations, one where an operator aligns an injection system locally but the decision to start injection is made at the RSDP. In this case, it may be more appropriate to model two separate inventory control HFEs. For the BWR evaluation that was performed, all key systems could be aligned and controlled from the RSDP, and the functional grouping of actions led to identifying three HFEs, as follows.

- ASDCOG: Cognitive failure to abandon the MCR upon loss of control.
- ASDINV: Failure to implement the inventory and pressure control actions at the RSDP.
- ASDBUS: Failure to start the supporting diesel generator (DG) at the RSDP.

The immediate actions following the decision to abandon up to the time of activation of the RSDP include tasks that 1) support reactor pressure and inventory control and are included in ASDINV, 2) support the establishment of a power source and are included in ASDBUS, and 3) support MCR abandonment but do not require being modeled by a specific HFE. This latter subset of actions includes, for example, traveling from the MCR to the RSDP, or actions to operate systems not credited in the Fire PRA (for example, a procedural step to establish HVAC in a room, which the PRA has demonstrated is not essential). Even if not modeled by a specific HFE, these latter actions take away some of the time that could be used to support the actions modeled with an HFE, and this incompressible time, designated here as T_{RSDP}, must be accounted for in the modeling.

In conclusion, the functional grouping of HFEs for the example BWR MCR abandonment HRA resulted in a set of three HFEs plus one additional parameter, T_{RSDP}. As indicated in Section III.A., the timing PSF of an HFE is fully determined by four parameters: Tsw, Tdelay, Tcog, and Texe. The total number of variables to be estimated in the evaluation of the timing PSF is therefore $3 \times 4 + 1 = 13$.

III.C. Uncertainty of Timing Parameters

The evaluation of the timing PSF requires the estimation of the 13 parameters identified above. These parameters are known with varying levels of uncertainty. To ensure that the available knowledge about the parameters is fully utilized, it is beneficial to use a structured approach where they are evaluated in order from the least uncertain to the most uncertain.

A ranking of 10 of these parameters by increasing level of uncertainty is given below. These are "free" parameters in the sense that they can be considered independent from each other.

The following abbreviations are used: "ABN" designates HFE ASDCOG, "INV" designates HFE ASDINV, and "BUS" designates HFE ASDBUS. For a given HFE, its system time window, time to cue acknowledgment, cognition time, and execution time are expressed using the nomenclature of Figure 1, with the abbreviation of the HFE in parentheses. For example, Tsw(INV) is the system time window for HFE ASDINV and Tcog(ABN) is the cognitive time for HFE ASDCOG.

- Texe(ABN): By definition, the cognitive failure to abandon the MCR upon loss of control focuses on a decision failure. There is no execution involved in that HFE. Therefore, Texe(ABN) is known to be zero.
- Tdelay(ABN): This timing parameter represents the time to cue acknowledgement that MCR abandonment may be required. It is estimated to be equal to 0. In practice, it is likely that the fire would be first detected, and then would lead to fire damage (starting with plant trip) within several seconds or minutes. For the evaluation of ASDCOG, this buildup time is condensed into a single point in time, where at t=0 the operators are cued to the existence of the fire, the plant trip occurs, and all injection is lost. This conforms to the PRA assumption that equipment failures that will lead to MCR abandonment by loss of control occur at time $T_0 = 0$. (Section III.A). The time needed for the operators to understand that the conditions for abandonment are effectively met is accounted for in Tcog(ABN). A value of Tdelay(ABN) equal to 0 also ensures consistency with the thermal hydraulic simulations that are used to calculate Tsw(INV).
- Tsw(INV): This is the time to core damage, where at t = 0 all injection means are lost and the criteria for MCR abandonment are met. This time is calculated based on thermal hydraulic calculations, performed for example using the Modular Accident Analysis Program (MAAP). There is not one unique value for Tsw(INV), but rather a range of values, due to the fact there are several accidents that meet MCR abandonment criteria. For example, loss of all injection combined with fire-induced multiple spurious opening of SRVs would lead to core damage much earlier than loss of high-pressure injection and depressurization failure. Because Tsw(INV) bounds the timing of all MCR abandonment actions shown in Figure 2, the various accident configurations may require the

development of several "flavors" of HFEs, each with its own HEP reflecting the timing of the configuration being evaluated.

- T_{RSDP}: The duration from the time MCR abandonment is decided to the time of RSDP activation can be relatively well estimated, based on operator interviews and job performance measures (JPMs) (which give an estimate of the time it takes to perform an action based on timed trials).
- Texe(BUS) and Texe(INV): the ASD execution steps (start the DG and establish inventory makeup) are detailed in the supporting abandonment procedure. These are used as a basis for time estimates, complemented by JPMs, if available, and operator interviews, which provide insights on the level of difficulty of the tasks.
- Tcog(BUS) and Tcog(INV): Once at the RSDP, the potential for cognitive errors may be limited because the procedure details the steps to be taken for ASD operation. That is, execution errors are the dominant cause of error. However, depending on the fire-induced failures and the structure of the abandonment procedure, the operator may need to prioritize certain inventory recovery actions over other actions that are less time critical, or may need to implement certain load shedding actions to start the diesel, therefore the potential for cognitive errors still exists. A review of the procedural steps complemented by operator interviews will help estimate the time needed for such decision making.
- Tcog(ABN): The cognitive time for the decision to abandon the MCR relies on the operators determining that the criteria for abandonment are met. This involves realizing that all immediate injection means are lost. The operators are trained on the MCR abandonment procedure and are aware that the RSDP can be used to provide injection. An estimate of this cognitive time is made based on a review of the abandonment procedure and on operator interviews.
- Tsw(ABN): This is the time window for the decision to abandon the MCR. This parameter is the most uncertain. In contrast to Tsw(INV), it is not determined by thermal hydraulic calculations. For that reason, it is better ascertained by substituting it with another parameter, Trec(ABN), which represents the time available to recover from an incorrect decision of not abandoning the MCR. This is based on the considerations that: 1) Trec = Tsw – Tdelay – Tcog – Texe (Section III.A), 2) Tdelay(ABN) = 0, and 3) Texe(ABN) = 0, as discussed above. Therefore, Tsw(ABN) is completely determined with the knowledge of Tcog(ABN) and Trec(ABN) via the formula: Tsw(ABN) = Tcog(ABN) + Trec(ABN). The estimation of Trec(ABN) is further discussed in Section III.D.

Out of the 13 parameters to determine, the three not discussed above include: Tsw(BUS), which is the time window to establish a power source to support injection at the RSDP, Tdelay(BUS), which is the time to cue acknowledgment that such power source is needed, and Tdelay(INV), which corresponds to the minimum time at which the action to provide inventory makeup can begin. Note that Tdelay(INV) here is not interpreted as a time to cue acknowledgement, since the operators are already aware of the need to inject as soon as possible, which is what prompted MCR abandonment.

To evaluate these three remaining parameters, advantage is taken from the fact that they are dependent on other parameters due to HFE interdependence, as further discussed in Section III.D.

III.D. Abandonment Timeline

Figure 2 outlines how the three abandonment HFEs identified previously fit into the MCR abandonment timeline.

The figure outlines how the human actions occur in a distinct order, with the decision to abandon the MCR coming first (modeled with HFE ASDCOG), followed by the actions immediately after the decision to abandon up to the time of activation of the RSDP (no HFE modeled in this example, see Section III.B), then the alignment of needed power sources (modeled with HFE ASDBUS), and finally the actions associated with re-establishing water makeup to the reactor (modeled with HFE ASDINV).

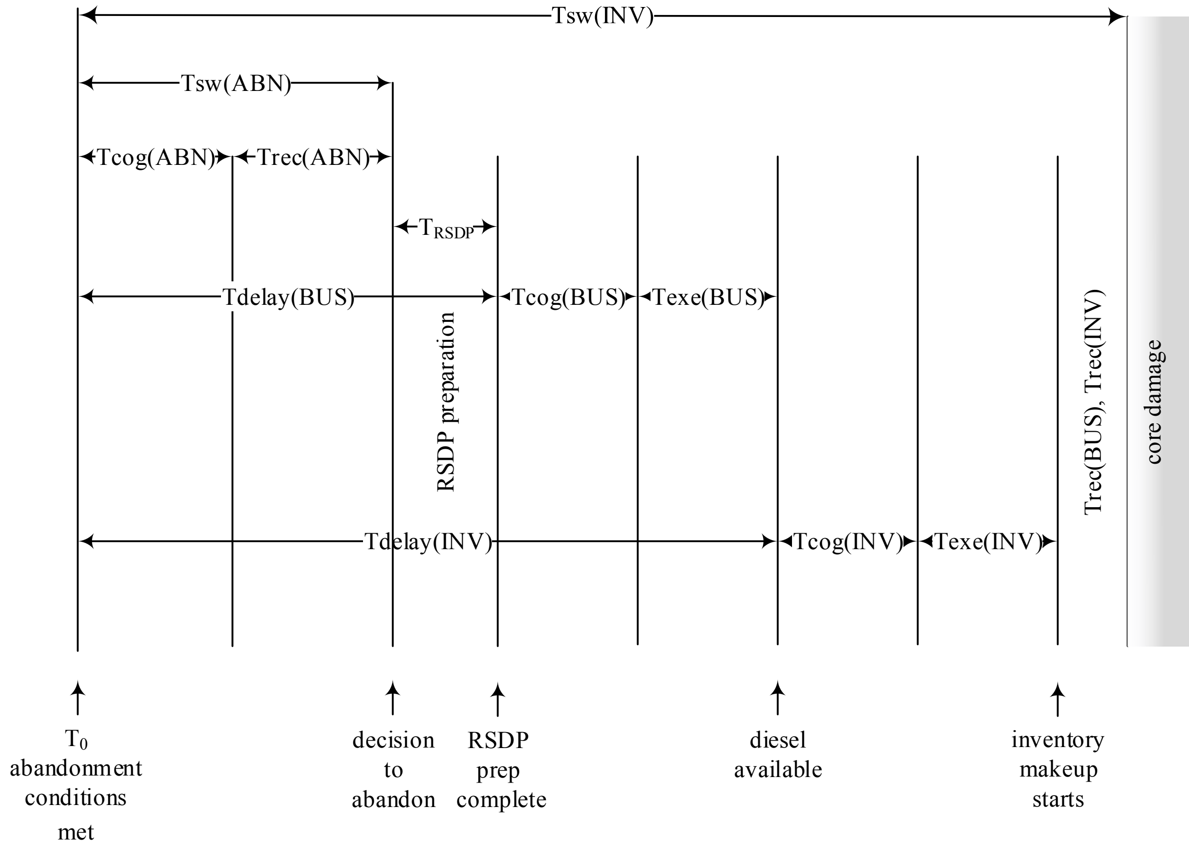

Fig. 2. MCR abandonment timeline

Figure 2 shows that the timings of the HFEs are interdependent, a result used to calculate the value of Tsw(BUS), Tdelay(BUS), and Tdelay(INV) directly from the estimates of other timing parameters. In particular:

- Tsw(BUS) = Tsw(INV) – Tcog(INV) – Texe(INV). This corresponds to the time window to establish injection, Tsw(INV), minus the time needed to perform ASDINV, i.e., Tcog(INV) + Texe(INV). The formula reflects the fact that for injection to occur, power must be established first.
- Tdelay(BUS) = Tsw(ABN) + T_{RSDP}. The time to cue acknowledgement that a power source to support injection at the RSDP is needed comes after 1) the decision to abandon the MCR has been taken and 2) the RSDP has been activated. Conceivably, a fire could cause loss of power several minutes after the RSDP activation. However, in this situation, some of the actions associated with ASDINV would have already been implemented, and the effect would be to 1) stop the actions related to ASDINV (since they would be interrupted anyway by the loss of power), 2) implement the actions related to ASDBUS, and 3) once power is re-established, continue with the remaining actions associated with ASDINV. There would be a partial re-ordering of actions, but no appreciable change in overall timing. For ease of modeling, it is appropriate to simply consider that re-establishing a power source will be the first action to take place after the RSDP is initiated.
- Tdelay(INV) = Tdelay(BUS) + Tcog(BUS) + Texe(BUS). This formula expresses the fact that the minimum time at which the action to provide inventory makeup can begin is after a power source has been established at the RSDP.

In addition, based on Figure 2, the time available to recover the failure to correctly perform ASDBUS is found to be equal to the time available to recover the failure to correctly perform ASDINV. It is equal to: Tsw(INV) – Tsw(ABN) – T_{RSDP} – Tcog(BUS) – Texe(BUS) – Tcog(INV) – Texe(INV).

The HFE timeline is also used to help ascertain a range of credible values for Trec(ABN), the time available to recover from an incorrect decision not to abandon the MCR, which in Section III.C was identified as the key parameter to estimate Tsw(ABN). In particular, Figure 2 shows that the timing parameters must follow the following inequality:

$$Tcog(ABN) + Trec(ABN) + T_{RSDP} + Tcog(BUS) + Texe(BUS) + Tcog(INV) + Texe(INV) \leq Tsw\ (INV) \qquad (1)$$

Which in turns yields the following constraint on Trec(ABN):

$$Trec(ABN) \leq Tsw\ (INV) - [Tcog(ABN) + T_{RSDP} + Tcog(BUS) + Texe(BUS) + Tcog(INV) + Texe(INV)] \qquad (2)$$

IV. RESULTS

As can be seen from Eq. (2), the constraint imposed on Trec(ABN) embeds the information gathered on all free parameters estimated in Section III.C. For that reason, Eq. (2) can be used as a timing criterion to determine the feasibility of MCR abandonment. The following possible results can be obtained:

- Trec(ABN) is at a minimum equal to 0. Therefore, if the estimates for the parameters on the right side of Eq. (2) yield the inequality Trec(ABN) < 0, there is not sufficient time to successfully perform MCR abandonment. In this situation, core damage is expected to occur. In practice, this corresponds to severe fire scenarios where 1) control of injection systems is lost from the MCR, 2) a rapid inventory loss occurs, typically caused by the spurious opening of multiple SRVs, and 3) the inventory loss happens too quickly for inventory makeup to be re-established in time from the RSDP.
- If the estimates for the parameters on the right side of Eq. (2) yield the equality Trec(ABN) = 0, the abandonment actions can be carried out just in time, but there is no extra-time available for recovery. MCR abandonment HEPs have high values, typically 5E-02 or higher.
- If the estimates for the parameters on the right side of Eq. (2) yield the inequality Trec(ABN) > 0, there is sufficient time to perform the MCR abandonment actions and there is extra time for recovery. This extra time for recovery can be applied entirely to Trec(ABN), but alternatively, Trec(ABN) could be assigned only a portion of that time, which in effect consists of assigning the unused time to Trec(BUS) and Trec(INV). Depending on their value, such recovery time assignments can contribute to a reduction of MCR abandonment HEPs by up to an order of magnitude.

For the cases where Trec(ABN) > 0, the severity of the fire scenario under consideration is used to provide insights on the fraction of the extra time available to assign to Trec(ABN).

- For severe fire scenarios, i.e., those scenarios characterized by a relatively rapid loss of inventory, an incorrect decision to not abandon is reasonably likely to be recovered (meaning that the requirement to abandon that was initially delayed has become evident) because of the clear degradation of operating conditions (reactor water level rapidly declining, for example). For such scenarios, the little extra time available for recovery can reasonably be assigned entirely to Trec(ABN).
- For milder scenarios, where inventory loss is less rapid, an incorrect judgment that evacuating the MCR is not needed is likely, and potentially reinforced by the general reluctance of the operators to abandon the MCR. Thus, for these scenarios, it would be reasonable to assign only a fraction of the extra time available for recovery to Trec(ABN) and leave the rest to Trec(BUS) and Trec(INV). Note that the abandonment procedure can also provide insights on plausible values to be used for Trec(ABN). For example, the abandonment procedure of the BWR that was evaluated prescribed MCR abandonment after confirmation that the fire had not been contained within 10 minutes of detection. This put an upper bound on the value of Trec(ABN).

The value assigned to Trec(ABN) allows for the calculation of Tsw(ABN) via the formula: Tsw(ABN) = Tcog(ABN) + Trec(ABN). With this, all 13 parameters of the timing evaluation are determined and the impact of the timing PSF can be fully evaluated.

V. CONCLUSION

Using the structured approach described above allows for an HRA of loss of control MCR abandonment fire scenarios that is both transparent and traceable, which in turn helps ensure the robustness of the results and an adequate representation of the risk of these challenging fire scenarios.

REFERENCES

1. NUREG/CR-6850 and EPRI 1011989, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology", Electrical Power Research Institute (EPRI), Palo Alto, CA, and U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Regulatory Research (RES), Washington, D.C. (2005).
2. NUREG-1921 and EPRI 1023001, "EPRI/NRC-RES Fire Human Reliability Analysis Guidelines, Final Report", EPRI, Palo Alto, CA, and NRC-RES, Washington, D.C. (2012).
3. Amico, P. and Collins, E.P., "Modeling Main Control Room Abandonment in Fire PRAs", 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA 2015), Sun Valley, ID (April 2015).