Completion of EPRI Credible Dependent Failure Mechanisms (CDFM) Methodology

Eric Thornsbury[a], Jeffrey A. Julius[b], Kaydee Gunter[c], Pierre Macheret[d] and Annika MacLeod[e]

[a] EPRI, Charlotte, USA, ethornsbury@epri.com
[b] Jensen Hughes, Seattle, USA, jjulius@jensenhughes.com
[c] Jensen Hughes, Seattle, USA, kgunter@jensenhughes.com
[d] Jensen Hughes, Las Vegas, USA, pmacheret@jensenhughes.com
[e] Jensen Hughes, Saratoga Springs, NY, USA, Annika.MacLeod@jensenhughes.com

Abstract: In 2025, EPRI released the final version of a new methodology for human reliability analysis (HRA) dependency called Credible Dependent Failure Mechanisms (CDFM). This work began in 2021 with a workshop that used guided brainstorming sessions aimed at identifying novel and viable alternatives to address the challenges associated with HRA dependency analysis. Building on the results of this initial workshop, EPRI developed CDFM which is a new methodology to HRA dependency focused on identifying those realistic (that is, credible) causes (failure mechanisms) of human actions that can fail multiple (dependent) accident mitigation responses. In 2025 the final methodology was published and documented in EPRI Report 3002032023.

The CDFM process uses probabilistic risk assessment (PRA) scenarios (event tree and fault tree logic) and available information related to existing human failure events (HFEs) to identify, define and quantify Dependent Combination Events (DCEs).

The final methodology now includes two approaches to quantification of the DCEs. Approach 1 is the selection of the lowest cognitive failure probability (Pcog) from the individual HFEs of the DCE under consideration. In this approach it is important to ensure the individual HFEs quantifications are capturing the same common failure mechanism. This approach is only applicable if all HFEs within the DCE are homogenous. When Approach 1 is not appropriate, Approach 2 will be required. Approach 2 uses the same HRA methodology used to quantify individual HFEs in the DCE to evaluate the DCE probability. Expanded examples and guidance for these approaches can be found within the 2025 Report. This paper will focus on the new quantification approaches and provide an example of DCE grouping and quantification.

1. INTRODUCTION

In 2025, EPRI released the final version of a new methodology for human reliability analysis (HRA) dependency called Credible Dependent Failure Mechanisms (CDFM) and is documented in EPRI Report 3002032023 [1]. This work began in 2021 as an effort to improve upon existing HRA Dependency Methods, specifically the EPRI HRA Calculator approach [6]. CDFM focuses on identifying those realistic (that is, credible) causes (failure mechanisms) of human actions that can fail multiple (dependent) accident mitigation responses. One of the primary research goals of CDFM was to reduce the resources and time required for dependency analysis. Traditional methods are often time-consuming. The approaches rely on mining cutsets and assume that all HFEs within a cutset are fully dependent unless otherwise justified. This approach leads to the identification of thousands to tens of thousands of potential HFE combinations, all of which must be evaluated and potentially incorporated into the PRA model. The insights gained from that analysis are often conservative and disproportionate to the resources required to perform the analysis. Additionally, traditional methods are typically performed at the end of the probabilistic risk assessment (PRA) development process.

CDFM addresses these challenges by:

- Focusing on credible dependent failure mechanisms that can be identified through a review of accident sequences and model logic.
- Avoiding reliance on cutset mining, allowing the analysis to be conducted earlier in the PRA process.
- Reducing the number of dependency groupings, which minimizes the need for repeated updates when the PRA model changes.

In April 2026, the CDFM methodology underwent a Newly Developed Method (NDM) Peer Review. The key insights resulting from this review were:

- The NDM review did not find any fundamental flaws in the CDFM method.
- Identification of the dependent combination events is the key feature, and because of its novelty the technical basis requires more documentation.
- CDFM is applicable to PRAs modeling all plant operating modes and all hazard groups, but additional testing and guidance was suggested for application to external hazards such as seismic PRA that use multipliers to develop the human error probabilities (HEPs) of individual HFEs.

EPRI has committed to developing supporting CDFM documentation to address the facts and observations (F&Os) and expects to complete an F&O Closure Review of the NDM comments.

2. OVERVIEW OF CDFM PROCESS

The CDFM process uses PRA scenarios modeled with event tree and fault tree logic and uses available information related to the existing, individual HFEs to identify, define and quantify Dependent Combination Events (DCEs). A DCE is an event in the PRA that represents the probability that all operator actions within a group of operator actions fail as a result of the occurrence of one or more common failure mechanisms that have been determined to be shared by all events within the group. An important aspect of DCEs is that they are developed to be functionally independent not only from other DCEs, but also from individual HFEs.

2.1. Identification and Definition of DCEs

To identify DCEs, the process is as follows:

1 Identify event tree functions (ETFs) and assign individual HFEs to each function.
2 Identify all individual HFEs which support the same support system.
3 Define DCEs, categorized based on the above as ETF DCEs or support system DCEs.

2.1.1. Event tree function DCEs

An ETF DCE is a group operator actions that work together to satisfy a specific goal in a given event tree, which is typically a safety function of the nuclear power plant. An event tree function is typically one or more front-line systems. To develop ETF DCEs, the analyst can either apply a top down approach, a bottom up approach, or a combination of both. The top down approach starts with a review of the PRA event trees to identify ETFs, and from there identify associated HFEs which then becomes the initial list of HFEs within a DCE. The bottom-up approach starts by identifying all HFEs in the PRA model and then grouping them together functionally, based on the definition and summary context of each individual HFE.

The most efficient approach to identifying DCEs will depend on any or all of the following:

- The PRA model structure,
- The PRA documentation,
- Analysts familiarity with different portions of the PRA.

The top-down approach could be less straightforward than the bottom-up approach for PRA models that have a large number of event trees, each event tree representing a variation on a type of initiating event (e.g., transients divided into turbine trip event, main feedwater loss event, loss of an electrical bus). This is in contrast to PRAs where only a small number of event trees are developed, each event tree representing a main event type (e.g., transients, small LOCA, medium LOCA, etc.). The abundance of event trees may hinder the identification of HFEs within the logic.

2.1.2. Support system DCEs

Support system DCEs are identified by reviewing individual HFEs involved in the operation of support systems after an initiating event. For example, the service water system provides cooling water that will support the operation of front-line systems ensuring inventory control and decay heat removal, as well as other support systems (e.g., diesel generators). The associated HFEs are therefore different in their consequences rather than individual HFEs supporting ETF DCEs. The common dependency mechanism underlying support system HFEs is found first in shared procedures or a set of procedures governing that support system.

2.1.3. Develop the DCE Definition

The initial list of individual HFEs underlying each ETF DCE and support system DCE likely needs to undergo some further refinements to ensure that two fundamental principles of the CDFM methodology are achieved:

1. DCEs should be independent from each other. This first principle is to ensure that, when the PRA model is quantified, two DCEs that end up in the same cutsets do not need further post-processing in order to evaluate their level of dependence. The DCEs must be structured in such a way that this independence is inherently maintained throughout their incorporation into the model. Examples of factors that promote independence include:
    a. HFEs performed in different response phases
    b. Crew/shift change between the HFEs
    c. Different high level goals/functions
    d. HFEs separated by an intervening success
2. Within a DCE, there should be a common thread, typically cognitive, shared by all its constituent HFEs. Expressed in an equivalent way, the analyst should be able to develop a “narrative” for the common failure mechanism that would affect all HFEs within the DCE. The narrative tells the story of what the DCE represents. It accomplishes several purposes:
    a. A narrative provides a good understanding of DCEs and therefore ensuring independence between them. Comparing the narrative of DCEs may reveal a dependency factor that, for example, can be removed by an adjustment to the narrative themselves, which in turn would lead to an adjustment to the partitioning of HFEs into DCEs. An example of adjustment could be the merging of DCEs together. For a given plant, the initial grouping of HFEs under individual HFEs can undergo some changes as the narratives of DCEs are developed and finalized, leading to a potential repartitioning of HFEs into groups that will eventually be plant-specific
    b. A narrative sheds light on the context associated with the DCE and, as such, helps in its quantification. For example, a narrative will help understand whether disparities between the cognitive failure probabilities (Pcogs) of underlying HFEs are significant enough to warrant not considering quantification Approach 1 (see Section 2.2.1 for that quantification approach).
    c. A narrative for the DCE provides insights that are actionable, i.e., susceptible to plant actions such as enhanced operator training, changes in procedures, which in turn provide a basis for further refinement of the DCE if that DCE is found to be risk-significant in the cutsets.

2.2. Quantification of DCE Probability

CDFM provides two detailed approaches for quantification:

1. Select the lowest cognitive failure probability (Pcog) within the HFEs assigned to the DCE. This quantification approach is recommended if the set of Pcogs is homogeneous.
2. Explicitly develop a failure probability for the DCE. This approach can be used in all cases and is therefore recommended if quantification approach 1 is not applicable.

2.2.1. Quantification Approach 1

Approach 1 consists of selecting the lowest cognitive probability (Pcog) associated with the individual HFEs in a DCE under consideration. The underlying motivation for this approach is the observation that the DCE represents a common failure mechanism or a common cognitive failure path among all the HFEs it represents, therefore pointing to the lowest "common denominator" within their probability range.

Approach 1 relies on the premise that the HFEs underlying the DCE are relatively homogeneous. That homogeneity condition has two aspects:

1. The narrative associated with the lowest human error probability modeling cognition (termed Pcog) should include the cognitive failure paths found in the narrative of the DCE. If this condition is met, the lowest Pcog carries the core of the DCE failure probability.
2. The HFEs within the DCE should have been developed to the same level of detail with regard to their cognitive failure contribution. That is, the higher Pcogs should not carry excessive conservatism compared to the lowest Pcog. Similarly, the lowest Pcog should not be refined to a level not commensurate with the other Pcogs. This condition, if met, will guarantee some epistemic homogeneity across Pcogs.

As a first approximation, the homogeneity condition is considered met if the Pcogs within the DCE differ by one order of magnitude or less.

2.2.2. Quantification approach 2

Approach 2 should be used when the homogeneity premise of Approach 1 is not applicable. It can also be used as an alternative method where the development of a narrative substantiates the DCE basis. Approach 2 consists of quantifying the DCE following the same approach as was used for the individual HFEs. The quantification should explicitly account for the impact of instrumentation, procedures, and other performance shaping factors (PSFs) based on the definition that was developed for the DCE and the relevant failure mechanisms of the DCE. It incorporates information from the detailed evaluations of the HFEs included in the DCE group. This approach ensures that the DCE probability accounts for the information most relevant to the cognitive failure path common to all operator actions in the DCE.

For consistency among HFEs and DCEs, the analysts should use the same quantification method for the development of both. For example, if the constituent HFEs are quantified using the EPRI HRA methods such as the maximum of cause-based decision tree method (CBDTM) and human cognitive reliability/operation reliability experiments (HCR/ORE) [2], then the DCE should follow the same approach.

CDFM has added an additional failure mode not typically considered in traditional HRA dependency approaches. The EPRI HRA CBDT [2] methodology does not capture the failure mode corresponding to mis-prioritization or incorrect goals. This failure mode represents a fundamental failure to properly assess the situation, leading the operators to focus their efforts on tasks or issues that are unrelated to

the event of interest. In both pressurized water reactors (PWRs) and boiling water reactors (BWRs), design features, operational principles, and operating experience have reduced the likelihood of this failure mode. However, in principle, no combination of actions is immune to it. Therefore, if the quantification method of the DCE leads to negligible results or all other failure modes have been determined to not be applicable, the failure mode of mis-prioritization or incorrect goals should be included. Regarding its quantification, the following considerations apply:

- For long-term DCEs (time available for recovery greater than 1 hour), the feedback from the emergency response team and/or the arrival of extra crew constitute dependency breaking factors that help the operating crew re-establish proper prioritization of tasks. For such DCEs, these dependency breaking factors support an assessment of low dependence between multiple actions, which correlates to a value as low as 1E-05 based on the guidance in EPRI 1021081 [3]. Because of the large uncertainty associated with this failure mode, a value of 5E-05 is conservatively recommended for its contribution in long-term scenarios.
- For shorter-term DCEs (time available for recovery less than 1 hour) there may not be enough time for the emergency response team and/or the arrival of extra crew to be established; therefore, they should not be considered as dependency breaking factors. Generally, the emergency response team and/or the arrival of extra crew is credited with a 0.1 recovery, which implies the short-term DCE probability should be a factor of 10 larger than the long-term DCE probability. Consequently, a value of 5E-04 is recommended for its contribution in short-term scenarios.

For the HRA methodologies that account for the contribution of time-reliability correlations (TRC), (for example, HCR/ORE [2]) in the quantification of the DCE probability, the probability recommended above may be eliminated from consideration if its contribution is lower than the value obtained from the TRC method. The TRC represents the non-response probability, which includes the failure mode of mis-prioritization.

2.3. Model Incorporation

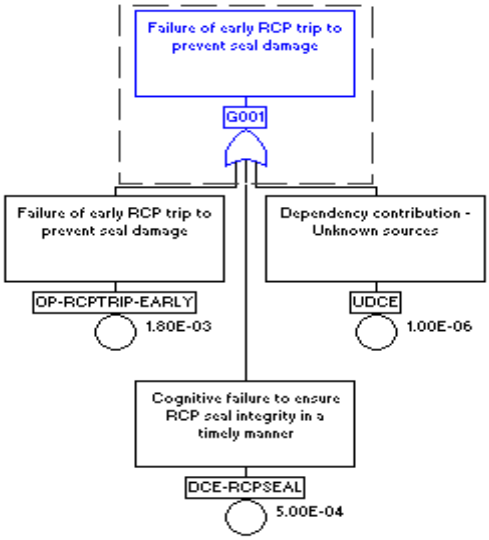
Once the DCEs have been identified and defined, the next step is to incorporate the results into the PRA. In the fault tree, the DCEs should be placed under OR gates with each individual HFE associated with the DCE. This modeling is similar to how common cause failure (CCF) events are modeled for component failures. Figure 1 provides an example of the DCE that represents the "Cognitive failure to ensure RCP seal integrity in a timely manner" discussed in the example of Section 4. This basic event is placed under an OR gate (gate ID "G001" in Figure 1), which allows the DCE to fail the logic associated with the operator action.

In addition to the DCE, an Unanalyzed Dependencies Contribution Event (UDCE) should also be incorporated into the fault tree logic. This event represents the lower limit for the probability of combinations of HFEs in a PRA model, due to factors not captured by CDFM. The UDCE represents what is commonly referred to as the "floor value" or "minimum joint human error probability (JHEP)," which is generally used to prevent unrealistically low probabilities, and for which a value must be defined per Supporting Requirement HR-G7 of Ref. [4].

The UDCE should be incorporated into the PRA fault tree in the same manner as the DCEs, but in this case, it should be included with almost all the post-initiator HFEs in the model. Figure 1 provides an example of the placement of the UDCE.

After the dependency results have been incorporated into the PRA logic model, the HRA analyst should review the quantification results to ensure that the HRA dependency results are as expected and reasonable. Because DCEs are identified based on an inductive approach, there may be unexpected or missed dependency groups following implementation, thus requiring some iteration of the CDFM process.

Figure 1: Example placement of a DCE and a UDCE in a fault tree



Supporting Requirement HR-G6 of the PRA Standard (Ref. [4], Ref. [5]) identifies the need for consistency of human error probability (HEP) quantifications and calls for reviewing HFEs against each other for reasonableness. HR-G6 also applies to DCEs. That is, the DCE probabilities obtained by application of the CDFM methodology should be reviewed to ensure that they make sense when compared against each other, and against HEPs of the PRA. The narrative developed for each DCE will help ascertain the appropriateness of the DCE probabilities.

If DCE values have high uncertainty or competing values are available for a DCE probability, as is the case for the example developed in Section 4, an evaluation of these DCE probabilities against those obtained for other DCEs, and to some extent, to the values of individual HEPs, will help ascertain the appropriate DCE probability.

4. EXAMPLE OF DCE DEVELOPMENT

This section provides an example of identification and definition of a DCE and quantification of the DCE probability using Approach 1 and Approach, this example does not cover a reasonableness check or model incorporation of the DCE into the PRA. The DCE being developed in this example is an ETF DCE for Reactor Coolant Pump (RCP) Seal Integrity in a PWR.

4.1 DCE Development using bottom-up approach

For this example, a bottom-up approach is taken. The full listing of all post-initiator HFEs in the PRA model were reviewed and individual HFEs are categorized based on their detailed HRA definition and qualitative analysis. Table 1 summarizes the categories identified based on a preliminary grouping. Table 1 was then reviewed in conjunction with the PRA logic model to define the specific DCE related to RCP seal integrity.

- As seen in the Table 1, one of the categories is RCP seal integrity, showing that this function is readily identifiable from the HRA documentation.
- Table 1 also shows other categories that clearly have no bearing on maintaining RCP seal integrity (e.g., the "Reactor trip" category, or the "Recirculation" category). These HFEs do not require further review for potential inclusion in the DCE modeling the ETF for RCP seal integrity.
- There are also other categories, shaded in the table, that could conceivably help maintain RCP seal integrity. For example, because an SBO causes loss of all RCP seal cooling, there might be actions intended to mitigate that loss (e.g. start of a dedicated pump for RCP seal cooling). In

another example, loss of a safety-related power train (under "AC power" category) may include HFEs whose timing is tailored for quick re-alignment of that power before RCP seal integrity is challenged. The HFEs in the shaded parts of the table are therefore reviewed in further detail to see if any of them should be added to the RCP seal integrity DCE. The right column in Table 1 shows a summary of the determinations made in that review.

Table 1: Review of HFEs by Category for Inclusion or Not in RCP Seal Integrity DCE

HFE Category	HFE(s) in category assigned to RCP seal integrity?
Auxiliary Feedwater	No. Category not related to RCP seal integrity.
Boration	No. Category not related to RCP seal integrity.
Charging	Maybe Upon further review this category includes one action, whose timing is focused on preserving RCP seal integrity.
Containment Isolation Phase A	No. Category not related to RCP seal integrity.
Cooling Support System	Maybe Upon further review, there are 6 HFEs in this categories. 3 of them have a time window incompatible with the timing of RCP seal cooling and are eliminated from further consideration. In the 3 remaining ones, one contributes to the calculation of an initiating frequency and can be excluded from further consideration because the subsequent reactor trip will reset the operator mindset and break dependencies. In the 2 remaining HFEs, one has a time window specifically selected with loss of RCP seal integrity as undesired outcome and accordingly is assigned to the RCP seal integrity DCE. The time window of the last action is compatible with maintaining seal integrity, but just by coincidence. The HFE is really about preserving adequate temperature in the service water system and its relationship with RCP seal cooling is indirect. Nevertheless, since, in the PRA model, there are no other HFEs with which that HFE would have a more obvious connection, this HFE is included in the RCP seal integrity DCE.
DC power	Maybe Upon further review, actions either support load shedding or have a time window incompatible with the timing of RCP seal cooling. None of these HFEs support the ETF of RCP seal integrity
Depressurization/Cooldown	No. Category not related to RCP seal integrity.
Decay heat removal via secondary side	No. Category not related to RCP seal integrity.
Engineered Safety Feature (ESF) start	Maybe Upon further review, the HFEs associated with ESF start already assume a LOCA. RCP seal integrity is irrelevant at that point. None of these HFEs support the ETF of RCP seal integrity
Feed and Bleed	No. Category not related to RCP seal integrity.
FLEX	No. Category not related to RCP seal integrity.
HVAC	No. Category not related to RCP seal integrity.
Interfacing-System LOCA	No. Category not related to RCP seal integrity.
Main Feedwater	No. Category not related to RCP seal integrity.

HFE Category	HFE(s) in category assigned to RCP seal integrity?
Main Steam Line Break	No. Category not related to RCP seal integrity.
PORV Block valve	No. Category not related to RCP seal integrity.
Power	Maybe Upon further review, the HFEs support electrical power recovery alignments with timings independent from RCP seal integrity. None of these HFEs support the ETF of RCP seal integrity
RCP seal cooling	Yes. This category contains 3 HFEs that directly relate to RCP seal integrity.
Reactor trip	No. Category not related to RCP seal integrity.
Recirculation	No. Category not related to RCP seal integrity.
Recirculation switch Hog leg/Cold leg	No. Category not related to RCP seal integrity.
Residual Heat Removal system	No. Category not related to RCP seal integrity.
RWST line break	No. Category not related to RCP seal integrity.
SBO	Maybe Upon further review, this category is focused is on FLEX actions independent from RCP seal integrity. None of these HFEs support the ETF of RCP seal integrity
Steam Generator Tube Rupture	No. Category not related to RCP seal integrity.
Safety Injection Termination	No. Category not related to RCP seal integrity.
Charging suction from VCT/RWST	Maybe Upon further review this category includes only one action, whose timing is focused on preserving RCP seal integrity.

The process above shows that for one of the Categories ("Cooling Support System"), there is an HFE assigned to the RCP seal integrity DCE, but that, under different circumstances, could conceivably be assigned to a different DCE. In the example treated here, the top-down approach (event tree review) is found to be not needed for the identification of the HFEs, except for the HFE in the Cooling Support System category. The assignment of this HFE was confirmed based on review of the event tree and fault tree, which help understand how the HFE is related to the others HFEs.

Table 2 shows the list of seven HFEs that, following the bottom-up process described above, resulted in being assigned to the RCP seal integrity DCE. These HFEs have a cognitive unity (i.e., a common narrative) in that their occurrence jeopardizes that integrity, and, in combination, can lead to RCP seal failure. The DCE can be described as: "Cognitive failure to ensure RCP seal integrity. This constitutes a basic narrative that needs to be further developed as part of the quantification process.

Table 2: Individual HFEs Associated with the RCP Seal Integrity DCE

HFE Name And Description	Time window (min)	Pcog	HEP total prob	Summary of HFE Context
RCPTRIP-LATE Operators fail to trip of RCP to prevent seal damage (late)	30	1.4E-04	5.7E-04	Late RCP trip avoiding significant seal leakage after RCP seal cooling loss.
SWFANSTRT Operators fail to start of service water cooling tower fan	30	4.4E-04	9.3E-04	Increased heat loads require the start of a cooling tower fan to ensure service water maintains appropriate cooling capability. Loss of service water eventually leads to loss of component cooling water (CCW) and of cooling to the charging pumps, leading to the loss of RCP seal injection and thermal barrier cooling.
RCPTRIP-EARLY Operators fail to trip of RCP to prevent seal damage (early)	16	1.4E-03	1.8E-03	Early RCP trip allowing minimum seal leakage after RCP seal cooling loss.
CCWPMPSTRT Operators fail to start of alternative CCW pump given failure of running pump	13	2.0E-03	3.7E-03	Upon loss of the normally operating CCW pump, the standby pump automatically starts. The action here models the manual start of that pump should auto-start fail. Loss of CCW causes loss of thermal barrier cooling and charging pump injection, thereby challenging RCP seal integrity.
ALTCCWPUMPSTRT Operators fail to start of alternative charging pump given failure of thermal barrier cooling	10	2.7E-02	3.5E-02	The CCW system which cools the thermal barrier also cools the normal charging pump. The loss of the CCW system requires starting another charging pump, cooled by a different system. In absence of both thermal barrier cooling and charging, RCP seal integrity is lost.
RWSTALIGN Operators fail to transfer charging pump suction from VCT to RWST	10	2.7E-02	3.5E-02	During normal operation, a charging pump takes suction from the volume control tank (VCT). Upon low VCT level, suction is transferred to the refueling water storage tank (RWST). The action here ensures that transfer. If failed, charging would be lost, challenging the RCP seal integrity function.
CHGALIGN Operators fail to align safety grade charging	10	2.7E-02	3.5E-02	Loss of instrument air causes loss of the normal charging path. Safety grade alignment provides an alternative charging path that does not rely on instrument air. Failure of that alignment leads to the loss of charging, challenging the RCP seal integrity function.

Note: To facilitate DCE quantification, the HFEs in Table 2 are sorted in terms of increasing cognitive failure probability.

4.2. DCE Quantification

Based on review of the HEPs in Table 2, the Pcog values of the HFEs in the group differ by more than one order of magnitude and would not meet the criterion for homogeneity given in Section 2.2.1 for the use of quantification Approach 1. Therefore, in this example quantification Approach 2 will be used. A comparison with quantification Approach 1 will be done afterwards.

4.2.1. Application of quantification Approach 2

Quantification Approach 2 consists of evaluating the mechanisms by which the DCE can occur. As recommended in Appendix C of Ref. [1], CBDTM (Ref. [2]) provides an appropriate framework for this task, keeping in mind that the decision trees of that method should be evaluated through the lens of whether a failure mechanism common to the DCE HFEs exists. The following determinations are made:

- **Decision trees Pca (data not available) and Pcd (information misleading)**: These decision trees should only be considered when the DCE identifies a common set of instrumentation as a common failure mechanism. If there is no common set of instrumentation, or if there is sufficient instrumentation redundancy and diversity that this failure mechanism is not credible, then these decision trees should not be evaluated for the DCE. This is the case here.
- **Decision tree Pcb (failure of attention):** This decision tree is evaluated in the context of failing to attend to/collect information that all actions in the DCE group require for successful diagnosis. In the context of the RCP seal integrity DCE, the underlying indications are multiple, alarmed, and clearly visible. Plus, operators, by training, are keen on maintaining RCP seal integrity. All these performance shaping factors combine to yield a negligible probability for the failure to notice challenges to RCP seal integrity, even in the worst-case scenario of a high workload.
- **Decision trees Pcc (misread/miscommunicate data) Pch (deliberate violation):** These failure mechanisms denote insufficiencies in communication protocols or in the general adequacy of procedures. For operating PWRs and BWRs, whose licensing environment has reached a significant maturity level, these failure mechanisms are unlikely to be present. Both trees are not applicable in this example since the plant under consideration here is a PWR that has been operated for over 30 years, using well-designed human-machine interface, and under well-controlled communication protocols.
- **Decision tree Pce (skip a step in procedure):** This decision tree is not applicable because there is no common procedural step that, if missed, would lead to a failure in diagnosis. That is, there are multiple alarms and procedural paths available to the operators, allowing for a proper diagnosis.
- **Decision trees Pcf (misinterpret instruction) and Pcg (misinterpret decision logic):** Because there is no common step to the diagnosis (see Pce above), these decision trees do not apply (they would apply only as a possible way by which a misinterpreted common procedural step would affect decision making).

Based on the above, the DCE failure probability using CBDTM is negligible. In such a situation, as discussed in Section 2.2.2, it is recommended to incorporate the contribution of a failure mode representing misprioritization/incorrect goals, which cannot be excluded as a common failure mechanism in a DCE. For shorter-term DCEs (i.e., those DCE with a time available for recovery less than 1 hr, which is the case of the RCP seal integrity DCE), a value of 5E-04 is recommended.

In this example, the individual HFEs are quantified using the maximum value of the CBDTM and HCR/ORE methods. The HCR/ORE method, described in Ref. [2], is a time-reliability correlation method whose evaluated failure probability becomes significant only for those actions whose cognition time (i.e., time dedicated to decision-making) is comparable to the time available. The time spent on cognition in the evaluation of RCP seal integrity is only a couple of minutes (based on a review of the cognition time used in the HFEs of Table 2) and small compared to the time available (the average time

window of the actions in Table 2 is 17 minutes, a good surrogate for the average time available for recovery). On that basis, it is concluded that the contribution from the HCR/ORE method is insignificant.

Based on the above discussion, quantification Approach 2 yields a DCE failure probability of 5E−04.

4.2.2 Application of quantification Approach 1

Using Approach 1, the lowest Pcog in Table 2 is equal to 1.4E-04 and corresponds to HFE RCPTRIP-LATE, representing the failure of operators to trip the RCPs in time, before a significant seal leakage can be avoided. That Pcog is less than the highest Pcogs in the group (2.7E-02) by more than one of order of magnitude. Per Section 2.2.1, Pcogs differing by more than one order of magnitude suggest that quantification Approach 2 is preferable, but this is by first approximation. What really matters in determining whether quantification Approach 1 is applicable is whether there is homogeneity between the Pcogs of the underlying HFEs. The homogeneity criterion has two aspects that need to be evaluated:

1. The narrative associated with the lowest Pcog should include the cognitive failure paths found in the narrative of the DCE. If this condition is met, the lowest Pcog carries the core of the DCE failure probability. As evaluated in Section 4.2.1, the DCE cognitive path by which the operators would fail to ensure RCP seal integrity most likely entails a misprioritization of tasks, a mindset where they focus on an item other than preserving RCP seal integrity. The narrative of OP-RCPTRIP-LATE is similar. Although that HFE was modeled using the CBDTM method, where misprioritization of tasks is not considered, skipping a procedural step (decision tree Pce) would be the closest representation, mimicking a situation where the operator, in focusing on another part of the procedure, fails to perform the key step that directs RCP trip to preserve RCP seal integrity. A review of RCPTRIP-LATE shows that Pce is in fact the unique cognitive failure mechanism identified for that action. In essence, the cognitive failure path of the DCE narrative is akin to that of RCPTRIP-LATE.
2. The HFEs within the DCE should be developed to the same level of detail with regard to their cognitive failure contribution. To evaluate this aspect, the HFEs of Table 2 are reviewed, and in particular the last four ones in the table, i.e., those whose Pcog is greater than the least Pcog in the table by more than one order of magnitude. None of these HFEs is found to embed excessive conservatism compared to OP-RCPTRIP-LATE. The last three HFEs in Table 2 share the same template, expressing that they have been grouped together because their severe time window of 10 min drives their relatively high HEP. That time window is the limit beyond which a first line of defense against RCP seal integrity is gone, i.e., loss of RCP seal injection via charging water flow through the seals. This kind of failure indicates that RCP seal integrity is challenged but not yet lost. There are still opportunities to maintain it, which is what the other actions in Table 2 are about. The high HEPs in Table 2 are therefore explained based on realistically modeled severe conditions. Conversely, the Pcog of RCPTRIP-LATE does not carry refinements in modeling that would make it incommensurate with the Pcog of other HFEs in that table. This leads to the determination that the lowest and highest HFEs in the DCEs are developed to the same level of detail.

It is therefore concluded that Pcog of RCPTRIP-LATE, despite being more than one order of magnitude less than the Pcog of some HFEs in Table 2, could be an acceptable surrogate value for the probability of the RCP seal integrity DCE.

4.2.3. Summary of the two quantification approaches

Approach 1 and Approach 2 provide DCE probabilities on the same order of magnitude.

- Approach 1 - DCE Probability 1.4E-04
- Approach 2 – DCE Probability 5E-04

Approach 1 does not meet the homogeneity test, however, on closer examination, Approach 1 reveals similarities with Approach 2 in the narrative including the insight that within this HFE there is essentially an "early set' and a "last chance" set of actions. That would suggest a lower DCEP. But given the short time window overall (30 minutes) during the initial part of the event (more susceptible to mis-prioritization) a higher DCEP could be warranted.

Which value to use will be decided from a comparison with the probabilities of other DCEs and from a reasonableness evaluation conforming to Supporting Requirement HR-G6 of the PRA Standard (Ref. [4], Ref. [5]). Part of the reasonableness evaluation could come from review of plant experience. In the example of RCP seal integrity, the HB Robinson event could be cited as an example where RCP seal cooling was ignored due to the context of the fire scenario. This determination is beyond the scope of this example and is not performed here.

5. CONCLUSION

The CDFM methodology, using a narrative-based approach for the analysis of dependencies, facilitates their quantification, comparison, and reasonableness evaluation, and provides actionable elements for continued operator-response improvements. It improves on the previous dependency analysis approach by allowing for an earlier integration of the HRA into PRA models and a more efficient identification of insights.

6. REFERENCES

[1] EPRI Credible Dependent Failure Mechanisms: HRA Dependency Methodology and Guidance. EPRI, Palo Alto, CA: 2025. 3002032023.

[2] An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment. EPRI, Palo Alto, CA: 1992. 100259.

[3] Establishing Minimum Acceptable Values for Probabilities of Human Failure Events: Practical Guidance for Probabilistic Risk Assessment. EPRI, Palo Alto, CA. 2010. 1021081.

[4] American Society of Mechanical Engineers. "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME/ANS RA-S-1.1-2024, May 9, 2024.

[5] American Society of Mechanical Engineers. ASME/ANS RA-Sa-2009, "Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," February 2, 2009.

[6] A Process for HRA Dependency Analysis and Considerations on Use of Minimum Values for Joint Human Error Probabilities, EPRI, Charlotte, NC: 2016. 3002003150.