Methods Guide:
Modeling Recovery and Repair

Section 6

6.0 Modeling Recovery and Repair

6.1 Objective and Scope

This section provides guidance for the treatment of recovery and repair actions of a failed or degraded structure, system, or component (SSC) that was observed in the operational event. The guidance addresses what recovery and repair actions can be credited in event and condition assessments (ECAs), and the requirements that should be met before crediting such actions. Definitions for recovery and repair action are provided. Also, guidance and considerations are provided for conducting recovery analyses and for modeling recovery/repair actions in the SPAR model. This section applies to initiating event and condition analyses in SDP, ASP, and MD 8.3 assessments.

Guidance in this section is intended for modeling recovery and repair actions in ECA. Although this guidance can be used to model recovery actions in the base case model, other guidance related to building PRA models should be reviewed for completeness.

6.2 Background

- ***Definitions: Recovery and repair.*** In PRA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems. The following definitions are from NUREG/CR-6823 and the American Society of Mechanical Engineers (ASME) PRA Standard.
  - Recovery actions involve the use of alternate equipment or means to perform a function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. The PRA Standard defines as —*. . . restoration of a function lost as a result of a failed structure, system, or component (SSC) by overcoming or compensating for its failure.”*[17]

    Examples of recovery actions include opening doors to promote room cooling when a heating, ventilation, and air conditioning system fails, recovering grid-related losses of offsite power by rerouting power or using alternate mitigating strategies (e.g. FLEX equipment), manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a hand wheel to manually open a motor-operated valve when the motor fails to operate.
  - Repair actions involve the actual repair of the mechanism which caused a component or system to fail. The PRA Standard defines repair as *“. . . restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality.*”

    Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.

- ***Overview: Modeling recovery and repair actions in PRAs.*** PRA models typically include a number of *recovery actions* of the type identified in the examples above. However, because recovery actions can involve complicated actions that are governed by procedures, most are typically evaluated using human reliability analysis (HRA) methods. A general exception is the treatment of offsite power recovery where the required recovery actions are

[17] The PRA Standard referred in this handbook includes ASME RA-Sa-2009, as endorsed by Regulatory Guide 1.200.

often not within the jurisdiction of the plant personnel. Thus, offsite power recovery data is collected and reduced for use in PRAs. Recovery of an emergency diesel generator is another action commonly modeled in PRAs based on actual data. The repair of components is generally not modeled in base PRA models because one or more of the following apply to most cut sets and sequences: (1) the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed), (2) repair is an action that is not always governed by procedures and thus difficult to justify, (3) the availability of spare parts cannot always be certain, and (4) abnormal procedures generally direct operators to use alternative equipment as a first priority. HRA techniques for estimating likelihood of successful repair should not be used because the possible repair scenarios that are affected by a variety of human actions and hardware-related issues that would not be known without knowing the specific causes of the problem.

  - *There are exceptions to these general observations.* For example, the replacement of fuses is an action identified in some fire abnormal procedures and can be accomplished rather quickly since spare fuses are available. As with a recovery action, either an HRA or data reduction approach could be utilized to generate a failure probability for a repair action. The modeling of recovery and repair actions in PRA reflects the need to accomplish the action within some time frame (e.g., before core damage occurs). Thus, the collected data must include both the time of failure and recovery to be utilized in the PRA.

- ***Overview: Modeling recovery and repair actions in ECA.*** The modeling of repair actions is limited in PRAs for the reasons stated above. The modeling of recovery actions in the PRA may be incomplete due to a new or recently proven alternate mitigating strategy. In an ECA where a failed SSC is the focus of the assessment, crediting a recovery or repair action may significantly reduce the risk significance of the unavailability. In addition, specifics are known about the ability to recover a specific failure that may lend itself to modeling, whereas the estimation of a generic recovery event in the base case PRA may not be practical.
  The consideration and process for recovery/repair modeling in event assessment generally follows the same guidance for building PRAs.

6.3 Treatment of Recovery/Repair Actions in ECA– General[18]

- ***PRA Standard requirements.*** Actions to recover/repair an observed failure of a SSC can be considered and modeled in accordance with supporting requirements of the PRA Standard. For the most part, these supporting requirements can be used to model recovery and repair actions in an event assessment.

  - The supporting requirements from the PRA Standard for crediting and modeling recovery and repair actions, including associated index numbers, are provided in Section 6.6.

  - An overview of applicable supporting requirements in Section 6.6 include the following

[18] The terms “recovery”, “repair”, “recovery event”, and “non-recovery” are often used interchangeably in risk analyses of operational events. In this handbook, the definitions from the PRA Standard are used to define recovery actions and repair actions. No standard definitions exist for the other two terms. Therefore, for the purpose of this handbook, a recovery event means human actions to restore a failed SSC or lost function, including the repair action, if any. “Non-recovery” probability means the failure probability of the recovery event. In some cases, other actions needed to restore a lost function may be modeled separately in the event tree; therefore, a recovery action may not restore a lost function in itself.

considerations:

  - ○ Demonstration that the action is plausible and feasible for the scenarios to which recovery/repair action are applied (HLR-HR-H).
  - ○ Availability of procedures, operator training, cues, and manpower (HR-H2).
  - ○ Relevant scenario-specific performance shaping factors in the HRA (HR-H2 and HR-G3).
  - ○ Dependencies between human failure events (recovery, repair, and emergency operating procedure actions) in the sequence, scenario, or cut set (HR-H3, HR-G7, and QU-C2).

- – Additional supporting requirements apply to the modeling of data-based “nominal” repair failure probabilities in the base case PRA. NUREG/CR-6823 provides guidance for allocating repair and recovery data.

- ***Using data to estimate non-recovery probabilities.*** Nominal failure probability for a *repair* action is normally based on the evaluation of industry-wide operating experience data. Examples of data-based non-recovery probabilities used in SPAR models include recovery/repair of emergency diesel generator (EDG) failures and loss of offsite power (LOOP) events.
  - – Guidance on the process for collecting and reducing recovery and repair data is provided in Section 5.3 of NUREG/CR-6823. This guidance includes a description of the type of data that is reviewed and guidelines for allocating data.
  - – A decision or procedural direction to perform deep DC load shed early in some events (e.g. SBO) may complicate recovery of AC power or emergency diesel generators, and this condition should be taken into consideration by the analyst when estimating non-recovery probabilities.
  - – Analysts specializing in parameter data collection, reduction, and statistical analysis should be consulted for estimating a non-recovery probability using operational experience data.[1]

- ***Using HRA to estimate non-recovery probabilities***. Failure probability for a recovery action is normally derived in a HRA. Good practices from NUREG-1792 for crediting post-initiator recovery actions while implementing Regulatory Guide 1.200 and the related requirements of the PRA Standard are summarized below.
  - – *Good Practice #1: Define Appropriate Recovery Actions.* Based on the failed functions, systems, or components, identify recovery actions to be credited that are not already included in the PRA (e.g., aligning another backup system not already accounted) and that are appropriate to be implemented by the crew to restore the failure. Aspects to consider are included in the questions listed in Section 6.7.
  - – *Good Practice #2: Account for Dependencies.* The good practices provided for post-initiator human failure events (HFEs) in general apply specifically to recovery actions as well.[19] Particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery actions. Considerations for accounting for dependencies are provided in Sections 6.4 and 6.8.

[1] A HFE is defined as a basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action.

  - Good Practice #3*: Quantify the Probability of Failing to Perform the Recovery.* Quantify the probability of failing to perform the recovery by (1) using representative data that exists and deemed appropriate for the recovery event, or (2) using the HRA method/tool(s) used for the other HFEs (i.e., using an analytical/modeling approach).

    If using data, ensure the data are applicable for the plant/sequence context or that the data are modified accordingly.
  - In addressing the above issues and assessing which recovery action, or actions, to credit in the PRA, for post-initiator HFEs all the good practices provided in the following sections in NUREG-1792 apply (i.e., the failure to recover is merely another HFE, like all of the other post-initiator HFEs):
    - ○ Section 5.1, "Identifying Potential Post-Initiator HFEs"
    - ○ Section 5.2, "Modeling Specific HFEs Corresponding to Human Actions"
    - ○ Section 5.3, "Quantifying the Corresponding Human Error Probabilities (HEPs) for Post-Initiator HFEs"

6.4 Treatment of Recovery/Repair Actions in ECA– Other Considerations

- ***Considerations for determining recovery/repair actions are plausible and feasible.*** A thorough recovery analysis requires careful consideration (at the cut set or scenario level) of the appropriate performance shaping factors in the HRA. Some questions to consider for crediting and modeling the recovery/repair of an observed failure are provided in Section 6.6. These questions were developed largely from the PRA Standard, NUREG-1792, and experience from SDP and ASP analyses.

- ***Exceptions to requirements and considerations.*** In general, no recovery or repair action should be credited where any of the considerations in Section 6.8 are not met (e.g., there is not sufficient time, there are no cues that there is a problem, there are not sufficient resources, and there is no procedure or training).
  - It may be possible to justify exceptions in unique situations, such as a procedure is not needed because the recovery/repair is a skill-of-the-craft, non-complex, and easily performed; or the specific failure mode of the equipment is known for the sequence (this is usually not the case at the typical level of detail in a PRA) and so repair of the failure can be credited because it can be easily and quickly diagnosed and implemented.
  - Any exceptions should be documented as to the appropriateness of the recovery/repair action.

2

- ***Consideration of observed errors, failures, and successes.*** Once an observed failure was judged recoverable or repairable given cut set-specific time constraints, the failure probability for a recovery or repair action can be estimated based on cut set-specific HRA and observations from the actual repair of the component.
  - Difficulties, error, and failures that were observed during the recovery/repair should be considered in the HRA (and in the recovery/repair plausibility and feasibility determination). This is consistent with the "Failure Memory Approach."[20]

[2] The —Failure Memory Approach‖ is used to estimate the risk significance of operational events. In the —Failure Memory Approach,‖ basic events associated with observed failures and other off-normal situations are configured to be failed or degraded, while those associated with observed successes and unchallenged components are assumed capable of failing with nominal probability.

- Similarly, recovery/repair actions that were performed successfully during the event should be addressed in cut set-specific HRAs, given that successes are treated probabilistically in the "Failure Memory Approach."

- ***Consideration of operator intervention preventing a catastrophic failure.*** For most cases, the observed end state of the SSC failure is given as the figure of merit. The recovery analysis is usually based on this observed end state. However, a catastrophic failure should be postulated probabilistically for those cases where human intervention prevented the failure to reaching a non-repairable end state. This consideration is consistent with the ―Failure Memory Approach‖ for the treatment of success (e.g., successful avoidance of a catastrophic failure). These cases could apply to a degradation found during a surveillance test or unplanned demand where the operator secured the component before catastrophic failure. The probability that the operator intervention would not occur should be considered in the recovery analysis.

  For example, a recovery analysis would consider the probability that an auxiliary operator that is typically dispatched to an operating turbine-driven auxiliary (AFW) pump following a reactor trip (per administrative procedure) would not reach the pump room in time to prevent a catastrophic failure due to a repairable lubricating oil leak.

- ***Consideration of support system availabilities.*** Ensure that support systems are available in the sequences in which recovery/repair is applied. Availability of support systems may need to be verified multiple times during events (e.g. initially upon SBO and once ELAP has been declared) to account for changes in support system availability. Additional complications from loss of support systems (e.g. additional operator actions to maintain level to avoid filling steam lines with high level trips disabled and wider level bands) should be considered under the appropriate section of this manual (e.g., section 9.0 for new human failure events).

- ***Examples of failure events and associated potential recovery actions.*** The table below provides examples of failure events and associated potential recovery actions.

Examples of Initial Failure Event(s)	Potential Recovery/Repair Action(s)
Automatic actuation fails.	Manual actuation.
Operator fails to recognize the need to take action (diagnosis failure).	Additional cues or re-visitation.
Test and maintenance unavailability.	Restore to service (if according to Technical Specifications the SSC is considered inoperable while in test/maintenance but can be returned to service quickly); or alternate mitigating strategies (e.g. FLEX, additional portable equipment).
Failure on demand (electrical, e.g. fuse or other electrical fault which can be recovered).	Replace fuse or if a control power problem, manually shut the local breaker.
Failure on demand (mechanical).	Use redundant SSC or a functionally similar component (e.g. opposite train/alternate mitigating strategies); or repair.
Failure to run.	Similar electrical / mechanical considerations as in failure on demand.
System level failure (e.g. loss of CCW system or loss of offsite power as an initiating event).	Empirical system recovery data; or alternate mitigating strategies (e.g. FLEX, additional portable equipment).

- ***Modeling recovery of test and maintenance unavailabilities.*** The recovery analysis should consider probabilistically the period of time that a SSC in a test or maintenance activity could not be restored to service given a postulated unplanned demand. This consideration is especially important for maintenance activities when the component is fully disassembled. For cases when the system is being tested during a routine surveillance activity, the restoration may be possible during the entire unavailability period.

- ***Modeling multiple recovery/repair actions.*** Considerations for crediting and modeling more than one recovery/repair actions (i.e., how many recoveries to be credited in one accident sequence/cut set) include the following:
  - Recovery/repair of failures in one system should be limited to one failed component in the system (i.e., recovery/repair limited to one train in a multiple train system).

    For example, if two EDGs failed, then plant staff would most likely focus on the less problematic diesel for recovery. Therefore, the recovery credit would be assigned to the EDG that can be restored to service earlier. Failure to recover the less problematic diesel would most likely lead plant staff to focus on alternate mitigating strategies (e.g. FLEX, deployment of additional portable equipment). These actions should be evaluated as multiple recovery/repair actions as indicated below.
  - Recovery/repair of failures in two systems may be a burden on plant staff, except when ample time and staffing exists to recover two failures or the recovery/repair of one failure is a simple reset action.

    For example, diagnosing and recovering simultaneous failures of the AFW and high-pressure injection systems may be difficult within the short time available, whereas, recovery of AFW and residual heat removal systems may be more likely. A quick recovery of one system involving trip reset from the control room may allow operators to diagnose and recover another system failure.
  - Multiple recovery/repair actions in a cut set should be checked to determine whether such credit is reasonable based on available time and staffing.

    For example, consider that one recovery may be tried (perhaps even multiple times) and then the second recovery may be tried but with even less time and resources available because of the attempts on the first recovery. Hence, the failure probability of the second and any subsequent recovery actions should be based on more pessimistic characteristics (e.g., less time available, less resources) than if such a possibility is not considered. The possibility of single point failures impacting a recovery event should also be considered (e.g., having multiple FLEX high pressure injection pumps available would not yield a credible recovery event in the event of a failure of the suction hose (with no available spare) that is common to all pumps.

- ***Consideration of alternate mitigating strategies*.** Plant licensees have implemented alternate mitigating strategies (e.g. B.5.b. measures, FLEX) in response to NRC orders. These strategies often involve the use of non-safety, portable, manual control, offsite, or non-standard system alignments. Crediting of these strategies in risk assessments should meet the guidelines outlined in NRC Regulatory Information Summary 2008-15. Considerations for incorporation of manual actions, special equipment operation, or other non-standard actions into the risk assessment include but are not limited to:
  - Operators diagnosis of the ability and need to use the alternate strategy
  - Feasibility of alternate strategy in the scenarios of interest to include engineering analysis or system testing showing the strategy to be successful throughout the accident scenario
  - Deployment (if applicable) of the equipment
  - Support systems and instrumentation availability
  - Environmental conditions
  - Reliability of associated equipment considering frequency of maintenance and testing intervals
  - Time margin for successful implementation of strategy

- Procedural direction in the scenarios of interest
- Training provided for staff responsible for actions within the strategy
- Staffing levels and availability of personnel for performing actions associated with the strategy
- Safety/Security interface considerations

  Credit for alternate mitigating strategies must be included in both the baseline risk model and the assessment of the non-conforming condition due to the performance deficiency, unless the action would only apply for the latter event. For example, if equipment is available that could reduce the risk; the analyst should consider whether the equipment could also be used for scenarios in the baseline model. Otherwise crediting the equipment in the SDP but not the base model would result in a smaller estimate of the risk increase than is realistic. For more information about where to model alternate mitigating strategies in the PRA, see section 6.5.

Nuclear Energy Institute's FRIDM (FLEX in Risk-Informed Decision Making) Task Force developed guidelines for the industry to follow when requesting credit for alternate mitigating strategies. This guidance is contained in two white papers, "Qualitative Assessment for Crediting Portable Equipment in Risk-Informed Decision Making," (ADAMS Accession No. ML16138A018), and "Streamlined Approach for Crediting Portable Equipment in Risk-Informed Decision Making," (ADAMS Accession No. ML16138A017). The NRC has not endorsed this guidance, however, a letter from the NRR Office Director was issued (ADAMS Accession No. ML16167A034), which captured NRC staff's views on the white papers. NEI subsequently submitted NEI 16-06, "Crediting Mitigating Strategies in Risk-Informed Decision Making" (Adams Accession No. ML16286A297) for information only to the NRC. This document has three sections, the first two representing the contents of the two white papers and a third section providing guidance to licensees about crediting portable equipment in a PRA. This section was reviewed by NRR staff and a publicly available memorandum (Adams Accession No. ML17031A269) was issued to capture the staff's comments. The above referenced documents should be considered information only to NRC risk analysts as background information on how licensees may credit alternate mitigating strategies in their risk assessments.

Ultimately the decision to provide credit for alternate mitigating strategies that are not explicitly modeled in the subject plant's SPAR model is up to the analyst based on, but not limited to, the factors expanded on in this section.

- ***Consideration of dependencies among multiple human actions in a cut set***. Particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery/repair actions. Considerations from NUREG-1792 include:
  - Dependencies should be assessed:
    - Among multiple recoveries in the accident sequence/cut set being evaluated
    - Between each recovery and the other HFEs in the sequence/cut set being evaluated
  - As part of this effort, the analyst should give proper consideration to the difficulties people often have in overcoming an initial mindset, despite new evidence.

    For example, consider how long the power-operated relief valve path remained open in the Three Mile Island accident, despite new cues of the problem, different personnel arriving, etc.

- The determination of whether there is dependence between HFEs and the level of dependence (if there is dependence) needs to be adequately justified and documented to ensure that credit for the recovery action(s) is appropriate. Refer to Section 9.3 for further information on dependence.

- ***Extending recovery/repair time (failure to run events).*** A component failure, after the component had operated for some of its mission time (even 10 minutes or so), can help to extend the time to core uncovery. Reduced decay heat rate, full steam generators (pressurized-water reactors), or reactor vessel (for boiling-water reactors) extends the time before core uncovery, thus allows for more recovery/repair time.

  For example, at a 4-loop Westinghouse plant, failure of the turbine-driven AFW pump after 2 hours following a SBO can result in doubling the time to core uncovery.

  Some considerations when crediting recovery/repair from a fail-to-run (FTR) event:

  - *Increase in time available for diagnosis and operator actions.* Extended time may increase the Time Available performance shaping factor (PSF) of the recovery/repair actions.

    For example, failure of the last running AFW pump at 3 hours after reactor trip would increase the available time to initiate feed and bleed actions due to lower decay heat rate and full steam generator(s).

  - *Thermal-hydraulic basis of event tree function.* The basis for changing the success criteria of a system based on extended time to core damage from a FTR event should be compatible with the appropriate thermal-hydraulic response. The timing of sequences (core damage/uncover times) used in event trees are usually based on the assumption that failure-to-start (FTS) and FTR events occur at t = 0.

  - *Reduced mission time.* A recovery/repair of a component that fails to run will reduce the mission time that the component/system has to run, after recovery/repair, to complete its 24-hour mission. However, the successful operation of the component/system before the failure must be probabilistically modeled (consistent with the “Failure Memory Approach”) in the PRA using nominal FTR probability during the first part of the mission time segment.

6.5 SPAR Model Modifications– Considerations

- ***Consult Idaho National Laboratory.*** Changes to the SPAR model should be closely coordinated with the Idaho National Laboratory staff to ensure changes are completely reflected throughout the model and changes are made in accordance with the SPAR model quality assurance program. Review checklists for SPAR model modifications are provided in Volume 3 of this handbook.

- ***Where to add the recovery event: event tree, fault tree, sequence, or cut set.*** Recovery/repair actions can be added at various levels in the SPAR model: event tree, fault tree, sequence, or cut set. The appropriate level depends on how narrow the application of the recovery/repair action is desired. All applications will require a basic event in a fault tree, either the use of an existing basic event or the creation of a new basic event. A post-processing rule can be developed or an existing rule edited to replace the recovery/repair basic event with time-dependent probabilities at the cut set, sequence, or event tree top event level.

Considerations for adding a recovery event at the various levels in the SPAR model include:[21]

- *Event tree level.* Examples when a recovery event is typically applied in the event tree top event include recovery from an initiating event (e.g., loss of instrument air, loss of service water, loss of offsite power) and recovery of another top event (e.g., loss of main feedwater, loss of primary conversion system). However, post-processing rules may be needed to apply a time-dependent recovery action (e.g., EDG non-recovery probabilities) at the sequence or cut set level.
  Fault tree level. Modeling recovery and repair actions are nominally included at the fault tree level. However, as with event tree applications, post-processing rules may be needed to apply a time-dependent recovery action at the sequence or cut set level. Further, a modified fault tree with configuration-specific structure and/or probabilities may be required for unique event-specific situations. In this case, the analyst may find it easier to copy and rename an existing fault tree, modify as desired, and apply the new fault tree in a sequence via a linking rule.[22]

  - Locate where the fault tree is used in the SPAR model. If the recovery/repair action only applies to a subset of sequences, then use linking rules to apply a modified copy of the fault tree with recovery/repair action to the sequences of interest.

- *Sequence level.* Linking rules are typically applied at the sequence level to replace an original base case fault tree with a modified copy of the fault tree (with a different name) that includes the recovery/repair action. Refer to the above for additional considerations for applying recovery/repair actions to fault trees.

- *Cut set level.* Applying recovery/repair actions at the cut set level is a common method for ensuring that the time-dependent nature of the recovery or repair action is properly modeled. Post-processing rules are used to replace or append an existing basic event in a cut set with another that includes the failure probability of the action. However, the applicable cut sets must be identified before the post-processing rules can be written. Considerations include:

  - To ensure that all important cut sets in which the recovery or repair action are identified, an initial scoping model solution should be performed with the failed event probability set to 1.0. Setting probability to 1.0, rather than a logical failure (i.e., TRUE), would ensure that the corresponding basic event appears in the minimal cut set list generated by the quantification process. However, the model solution will result in non-minimal cut sets.
  - Look for dependencies between the recovery event(s) and other events in the cut sets.
  - Write post-processing rule(s) to account for identified dependencies.
  - In the final quantification (model solution), the failed event would now be set to TRUE, in order to ensure that a correct minimal cut set equation is generated.

- ***Where to apply the recovery event: base case model or change case.*** The analyst must decide whether to add the recovery or repair action in the base case SPAR model or the

[21] In addition, see the considerations in “Using an existing recovery event in the SPAR model” in Section 6.4 when reusing existing basic events and post-processing rules.

[22] SAPHIRE Link Event Tree Rule (or linking rule) Editor creates a linking rule that replaces the original top event with a substituted top event based on the logical conditions dictated by the rule.

change case. Applying a recovery/repair basic event in the base case model may lower baseline core damage frequency (CDF), thus increasing the change in core damage frequency (ΔCDF) in select sequences. Applying the event in the change case and setting the event to FALSE in the base case model may increase baseline CDF, thus decreasing ΔCDF in select sequences. For most cases in ECA, applying a recovery or repair action to cut sets associated with the observed failure will not result in a difference in the results. Some considerations for modeling recovery and repair actions include the following:

- *Applying recovery actions of pre-planned strategies.* Recovery actions should be modeled in the base case SPAR model. These actions are usually pre-planned using installed systems with pre-staged hardware, tools, procedures, and training. Given that the intended reason to include a recovery action in the PRA model is to take credit for risk reduction in the overall plant CDF, the recovery event should be applied to the base case PRA model.
    - For a data-derived non-recovery probability already included in the base case model, the basic event parameter inputs (i.e., random failure data, uncertainty data) in the base case model may be replaced with the parameters associated with the HRA-derived estimate.
    - For a HRA-derived non-recovery probability already included in the base case model, human errors that were observed during the recovery/repair should be considered in a failure-specific HRA to re-evaluate the non-recovery probability. The basic event parameter inputs in the change case should include parameters associated with the HRA-derived estimate.
- *Applying repair actions of observed failures.* Repair actions of observed failures can be modeled in the change case. These actions are usually ad hoc; therefore, the HEP will be failure-specific. Event-specific risk reduction is usually credited in the change case.
    - If a data-derived non-recovery probability is already included in the base case model (e.g., EDG repair), then either
        - Set the recovery event in the base case model to TRUE or FALSE (no difference) and replace the basic event parameters (i.e., random failure data, uncertainty data) with the HRA-derived estimate in the change case; or
        - Change the basic event parameter inputs with the HRA-derived estimate in the base case model and make no changes in the change case.
- *Applying recovery actions associated with alternate mitigating strategies*. As a general rule, an alternate mitigating strategy, if it meets the appropriate criteria established in this section to be credited, should be modeled as a recovery action (as defined in the PRA Standard) in the base case model instead of a repair action in the change case, especially when the creditable action has been already modeled in the PRA.

- ***Using an existing recovery event in the SPAR model***. The base case SPAR model contains few recovery events that include basic events and post-processing rules with nominal failure to recover probabilities (e.g., EDG, LOOP). In addition, some SPAR models may include legacy events and rules that are not used (set to TRUE). Considerations for the use of an existing recovery event are summarized below and discussed further in the subsection.
    - Recovery/repair actions in SPAR models are noted by “XHE-XL” in the basic event name.

  - Know where the basic event (and fault tree) is used in the SPAR model.
  - Review post-processing rules used in the base case SPAR model for applicability.
  - Evaluate that the fault tree logic is correct for its intended modified use.

- ***Know where the basic event or fault tree is used in the SPAR model.*** Check that a proposed modification to an existing basic event or fault tree does not adversely impact the use of the same basic event or fault tree elsewhere in the SPAR model. The modification may not be appropriate in all sequences, especially for time-dependent recovery/repair actions.

  Some considerations include the following:

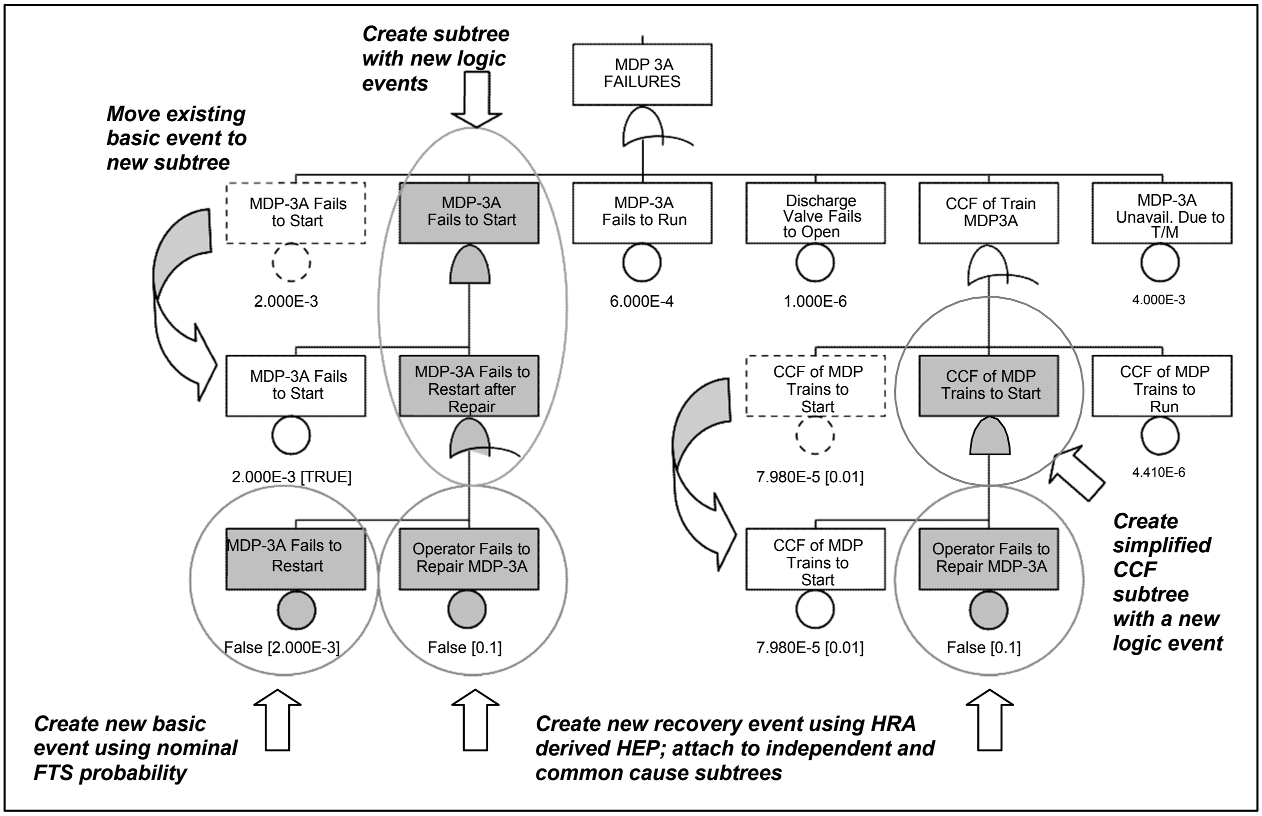
  - Examples where a modification of a basic event can affect multiple parts of the model include:
    - Basic event used in different fault trees,
    - Basic event used in a compound event [e.g., common-cause failure (CCF)],
    - Template event shared by basic events of a component group (e.g., motor-driven pump, motor-operated valve), and
    - Basic event used in post-processing rules.
  - Examples of basic event parameter variables that could impact multiple parts of the model include:
    - Failure probability/rate,
    - Mission time,
    - Calculation type, and
    - Process flag.
  - The same fault tree can be used in several event trees.
  - A new basic event or fault tree may be easier to apply in the SPAR model.

- ***Review SPAR model post-processing rules.*** Post-processing rules are free-form logic rules that allow for the alteration or deletion of fault tree or sequence cut sets in a "post-processing" fashion. Post-processing rules are used in SPAR models to apply recovery/repair events and other types of basic events in the appropriate cut sets after the change set is generated and the sequences are solved.
  - The post rules employed during the model solution should be reviewed to understand how the rules impacted dominant cut sets. Such rules may remove cut sets or significantly reduce the cut sets' probability. Confirm that any such rules are appropriate for the analysis and modify as necessary.
  - Post-processing rules may be developed for the following cases:
    - Particular fault tree (Fault Tree Rule Level)
    - All fault trees (Project Rule Level)
    - Particular sequence (Sequence Rule Level)
    - Single event tree (Event Tree Rule Level)

    - All sequences (Project Rule Level)

- A list of each type of recovery rule can be viewed in SAPHIRE.

- ***Adding a recovery event in a fault tree.*** Considerations for adding a new recovery event in an existing fault tree include the following:
  - *Include nominal failure probabilities associated with restart.* When modeling the recovery/repair of an observed failure, include nominal probability of hardware failures during and after restart attempt. Components can FTS and FTR after they are successfully recovered or repaired. This is important for failure modes with high failure probabilities (e.g., a failure mode probability that is on the same or greater than the nonrecovery probability). Since the component event is set to TRUE, a sub-tree will be needed to model the recovery and operation of the component during restart and throughout the remainder of its mission time.
  - *Example of using the correct fault tree logic.* An example of sub-tree logic for a repair model that can be added to an existing fault tree is shown in Figure 6-1. Elements of the sub-tree example are summarized below.



Create subtree with new logic events

Move existing basic event to new subtree

Create simplified CCF subtree with a new logic event

Create new basic event using nominal FTS probability

Create new recovery event using HRA derived HEP; attach to independent and common cause subtrees

Figure 6-1. An example of sub-tree logic for a repair model added to an existing fault tree. (The basic events in the figure show example base case and change set values).

    - A new recovery event (*Operator Fails to Repair MDP-3A*) is created and the failure probability is set to the HRA-derived estimate (HEP = 0.1) in the change case to represent observed failure and cut set dependences. If HEPs are cut set dependent, then post-processing rules are used to replace the —place holderǁ recovery event with the cut set-specific recovery events (not shown). Each of these recovery events will have a unique name and parameter values. This recovery event should be set to

FALSE in the base case model.

    - The original FTS basic event (*MDP-3A Fails to Start*) is moved to the sub-tree and the failure probability is set to TRUE in the change case. This basic event must remain in the model, since it is used in the CCF compound event for that failure mode (not shown). Note that the logic does not allow the propagation of the TRUE value up the tree.
    - A new basic event (*MDP-3A Fails to Restart*) is created to model the probability of failure to restart following repair. This failure probability (and other basic event parameter inputs) is normally set to the nominal value for that failure mode, i.e., same parameters used in the base case model basic event (MDP-3A Fails to Start). This recovery event should be set to FALSE in the base case model.
    - The CCF sub-tree is slightly different than the independent failure sub-tree due to simplification. The basic event that represents the nominal CCF probability to restart due to other causes is not modeled for simplicity. This simplistic approach may be slightly non-conservative; however, the CCF contribution during restart is relativity small and developing a new CCF compound event that includes restart can be problematic.
    - The recovery event in the CCF sub-tree (*Operator Fails to Repair MDP-3A*) is the same basic event used in the independent failure sub-tree. However, the analyst should consider the specifics of the failure and recovery events to determine whether this duplicative use is appropriate for the analysis.
- *Other details.* Some other details to consider in the above example are as follows:
    - The new basic event (*MDP-3A Fails to Restart*) probability can be updated to include recent operating experience as well as the observed failure as one more additional failure. The parameter update would be most important for rare or infrequent failure event. Refer to NUREG/CR-6823 for guidance in parameter estimations.
    - For cases involving repair of a FTR event, the modification of the fault tree would be much the same as in the FTS example (replace the FTS-related events to FTR). The exception is that the FTR basic event parameter for mission time should be reduced to reflect the run time required to complete the remaining sequence mission time (usually 24 hours).
- *Consideration of success terms.* When modifying a fault tree that results in a high failure probability (e.g., 0.1 to 1.0), consult Idaho National Laboratory for guidance on incorporating success terms in the model results. This is especially important for top events with a single basic event for the fault tree.
- *Update the base case SPAR model.* When adding a recovery event to a fault tree, make sure that the base case model is updated, as well as the change case model. Otherwise, a negative cut set importance may be calculated due to a lower core damage probability (CDP) or CDF of the base case SPAR model.
    - For repair actions, the recovery event in the base case model should be set to TRUE or FALSE (no difference) so that the recovery event does not show up in cut sets. Then, the recovery event should be set to the failure -specific HEP in the change case.
    - For recovery actions, the recovery event in the base case model should be set to the failure-specific HEP. No changes should be made to the recovery event in the change case.

6.6 PRA Standard Supporting Requirements– Modeling Recovery

The supporting requirements to the PRA Standard for crediting and modeling recovery and repair actions, including associated index numbers, are provided in this section for reference. For the most part, these supporting requirements apply in an ECA. Questions regarding interpretations and clarifications should be directed to an NRC representative on the ASME Committee on Nuclear Risk Management.

Deviations from or clarifications to the PRA Standard should be justified and documented in the risk analysis.[23]

- **HLR-HR-H.** Recovery actions (at the cut set or scenario level) shall be modeled only if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure shall address dependency on prior human failures in the scenario.[24]

- **HR-H1, Capability Category II.** Include operator recovery actions that can restore the functions, systems, or components on an as-needed basis to provide a more realistic evaluation of significant accident sequences.

- **HR-H2.** Credit operator recovery actions only if, on a plant-specific basis:
  - A procedure is available and operator training has included the action as part of crew's training, or justification for the omission is provided.
  - Cues (e.g., alarms) that alert the operator to the recovery action provided procedure, training, or skill of the craft exist.
  - Attention is given to the relevant plant-specific and scenario-specific performance shaping factors provided in HR-G3.
  - There is sufficient manpower to perform the action.

- **HR-H3.** Account for any dependency between the HFE for operator recovery and any other HFEs in the sequence, scenario, or cut set to which the recovery is applied (see HR-G7).

- **HR-G3.** When estimating human error probabilities, evaluate the impact of the following plant-specific and scenario-specific PSFs:
  - Quality [type (classroom or simulator) and frequency] of the operator training or experience;
  - Quality of the written procedures and administrative controls;
  - Availability of instrumentation needed to take corrective actions;
  - Degree of clarity of the cues/indications ***in supporting the detection, diagnosis, and***

[23] Clarifications to the ASME Standard in the Regulatory Guide 1.200 are emphasized in bold italics below.

[24] Recovery actions are actions taken in addition to those normally identified in the review of emergency, abnormal, and system operating procedures, which would normally be addressed in post-initiator HRA (i.e., PRA Standard designators HR-E through HR-G). They are included to allow credit for recovery from failures in cut sets or scenarios when failure to take credit would distort the insights from the risk analysis. The potential for recovery (e.g., manually opening a valve that failed to open automatically) may well differ from scenario to scenario or cut set to cut set. In this context, recovery is associated with work-arounds but does not include repair, which is addressed in SY-A22 and DA-C14.

decision-making give the plant-specific and scenario-specific context of the event;

- Human-machine interface;
- Time available and time required to complete the response;
- Complexity of ***detection, diagnosis and decision-making, and executing*** the required response;
- Environment (e.g., lighting, heat, radiation) under which the operator is working;
- Accessibility of the equipment requiring manipulation; and
- Necessity, adequacy, and availability of special tools, parts, clothing, etc.

- **HR-G7.** For multiple human actions in the same accident sequence or cut set, identified in accordance with supporting requirement QU-C1, assess the degree of dependence, and calculate a joint human error probability that reflects the dependence.[25] Account for the influence of success or failure in preceding human actions and system performance on the human event under consideration including:
  - Time required to complete all actions in relation to the time available to perform the actions;
  - Factors that could lead to dependence (e.g., common instrumentation, common procedures, increased stress, etc.); and
  - Availability of resources (e.g., personnel).

- **SY-A24.** Do not model the repair of hardware faults, unless the probability of repair is justified through an adequate analysis or examination of data ***collected in accordance with DA-C15 and estimated in accordance with DA-D9.***

- **DA-C15.** For each SSC for which repair is to be modeled (as described in SY-A22), identify instances of plant-specific ***experience and, when that is insufficient to estimate failure to repair consistent with DA-D9,*** applicable industry experience and for each repair, collect the associated repair time with the repair time being the period from identification of the component failure until the component is returned to service.

- ***DA-D9. For each SSC for which repair is to be modeled, estimate, based on the data collected in DA-C15, the probability of failure to repair the SSC in time to prevent core damage as a function of the accident sequence in which the SSC failure appears.***

- **QU-C1.** Identify cut sets with multiple HFEs that potentially impact significant accident sequences/cut sets by re-quantifying the PRA model with HEP values set to values that are sufficiently high that the cut sets are not truncated. The final quantification of these post-initiator HFEs may be done at the cut set level or saved sequence level.

[25] The state of the art in HRA is such that the assessment of dependency is largely based on the analyst's judgment.

6.7 Questions to Consider for Crediting Recovery/Repair Action

A thorough recovery analysis requires careful consideration of the appropriate performance shaping factors in an HRA. Some questions to consider for crediting and modeling the recovery/repair of an observed failure are provided below.

Observations from the actual event can provide insights into the recoverability of a failure. Some questions to consider during the event investigation include:

- How long did the recovery/repair actually take?

- Was there any time pressure for the actual recovery/repair action?

- Were there any difficulties observed during the recovery/repair activity?

- What is the basis for assuming an earlier recovery/repair time than what was actually observed?

- When did the plant staff first determine that the recovery/repair action is plausible and feasible (but decided to defer an immediate action due to operability or availability of redundant SSC)?

Did a procedure for recovery/repair exist at the time of the event?

- Could the observed failure mechanism result (probabilistically) in a worse case failure that could not be recovered/repaired?

6.8 Considerations for Defining Appropriate Recovery/Repair Actions

The following should be considered in defining appropriate recovery and repair actions:

- Can the failure be recovered/repaired given postulated extreme environmental conditions? Considerations include:
  - High temperatures due to high-energy line break,
  - Flooding from line breaks (e.g., floor drains overfill, overflow down stairways),
  - High radiation levels from sump recirculation,
  - Component accessibility,
  - Chemical hazard (e.g., transformer oil), and
  - Extreme weather (ice, high winds, lightning).

- What are the cues (e.g., alarms) that alert the operator to the need for a recovery action(s) and the failure that needs to be recovered? Will the cues be clear and provided in time for postulated sequences of interest?

- Is there sufficient time for the recovery action(s) to be diagnosed and implemented (repair failure, re-start system, and recover core cooling) to avoid the undesired outcome for postulated sequences? Time-dependent considerations include:

  - Time to core uncovery;
  - Time to recover vessel water level before pressure exceeds pump injection limits [low pressure (pump run-out), high pressure (pump shutoff head)];
  - Time to suppression pool over-pressure failure [BWR only]; and
  - Time to suppression pool temperature exceeding net positive suction head limits [BWR only].

- Can the recovery/repair action be accomplished within the required time frame? Considerations include:
  - Tools readily available,
  - Spare parts readily available,
  - Area lighting and power sources for tools available,
  - Communications with control room available, and
  - Plant staffing level with the right skills.[26]

- Would the crew know how much time is available before core uncovery or other time sensitive considerations?

- Are the crews trained on the recovery action(s) and is the quality and frequency of the training adequate?

- Is there procedural guidance to perform the recovery?

- Is the equipment needed to perform the recovery available in the context of other failures and the initiator for the sequence/cut set? Are the support systems available in sequences in which recovery is credited?

[26] Plant staffing levels during normal plant operations vary during the time of day and day of week. The full complement of the emergency response organization should be activated within 1 hour following the declaration of an emergency (Alert or higher).