STETKAR & ASSOCIATES

203 WHISPERING HILLS STREET
HOT SPRINGS, AR USA 71901
TELEPHONE: (501) 627-0500 • E-MAIL: jwstetkar@aol.com

November 18, 2020

Dr. Michael Cheok
Director, Division of Risk Analysis
Office of Nuclear Regulatory Research
Mail Stop T10-A12
U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852

Dear Dr. Cheok:

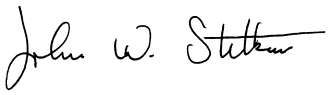
Comments on FLEX HRA Using IDHEAS-ECA

Attached are my comments on the version of the Research Information Letter report, "Draft – Flexible Coping Strategies (FLEX) HRA Using IDHEAS-ECA, Volume 2", that was discussed during the September 23, 2020 meeting of the ACRS Subcommittee on Reliability and Probabilistic Risk Assessment.

I do not request, or expect, formal responses to any of these comments and questions. They are provided only for your consideration as you finalize this important project.

Please contact me if you have any questions, or if you need any additional information.

Very truly yours,



John W. Stetkar

Attachment

**Comments and Questions on**
**Research Information Letter Report**
**Draft - Flexible Coping Strategies (FLEX) HRA Using IDHEAS-ECA, Volume 2**
**September 2020**
**John W. Stetkar**

***JWS Note:*** These comments are based on the version of this report that was discussed during the September 23, 2020 meeting of the ACRS Subcommittee on Reliability and Probabilistic Risk Assessment (ADAMS accession number ML20245E459).

- Some comments refer to the "current version of NUREG-2198". That report is: NUREG-2198, "The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G)", Draft, June 2020 (ADAMS accession number ML20238B988).

- Some comments refer to the "IDHEAS-ECA report". That report is: RIL-2020-02, "Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA)", February 2020 (ADAMS accession number ML20016A481).

## 1. General Comment

I read the draft Preface to the combined Volume 1 and Volume 2 of this report (ADAMS accession number ML20245E457). The Preface provides useful context and background information for a general understanding of how these two efforts are related, and how they differ. Please also refer to my November 8, 2020 comments on Volume 1 of the report.

However, after I finished reading both reports, it is not apparent to me how, or whether, the study that is documented in this report used the qualitative or quantitative results that are developed in Volume 1 (i.e., the FLEX expert elicitation). In particular, based on the information in Section 6 of this report, it does not seem that any of the estimated human error probabilities (HEPs) in this study are informed by or derived from that earlier effort.

If that is the case, it is not evident why these reports are characterized as Volume 1 and Volume 2 of an integrated study. To avoid confusion about the intent of each study and how its respective results should be interpreted and used, it seems that the reports should be issued separately, to clearly distinguish the fact that they are not functionally or technically related.

Why are these reports characterized as Volume 1 and Volume 2 of an integrated study?

## 2. General Comment

This draft report summarizes an application of the IDHEAS-ECA guidance to perform human reliability analyses (HRAs) for three scenarios that involve the use of FLEX equipment. The analyses were completed in late 2019. Therefore, it is evident that any comments on this report cannot alter that effort, the analysts' evaluations, or their results. However, some of these comments may be useful for characterizing the overall results from this study, or for developing improved guidance to structure similar future exercises.

### 3. General Comment

***JWS Note:*** I read Appendix B in parallel with Section 3.4 of the main report. This example is the first clear evidence that I found for this comment. Section C.5 of Appendix C and Section D.6 of Appendix D contain the same discussion.

Section B.5.2 of Appendix B notes that:

> "The following performance influencing factors are considered by IDHEAS-ECA (see Reference Z, ***Table 2-1***, page 2-3) under the high-level headings of 'Environment and situation,' 'System,' 'Personnel,' and 'Task':" [emphasis added]

Section B.5.2 lists a total of 14 performance-influencing factors (PIFs). Table 2-1 in the current IDHEAS-ECA report lists the 20 PIFs that are described in the IDHEAS general methodology in NUREG-2198. The current IDHEAS-ECA guidance simplifies the PIF evaluations by combining some PIFs from the general methodology into a set of 15 PIFs.

This is not a simple editorial discrepancy. Most of the 14 PIFs that are listed in Section B.5.2 seem to correspond directly to PIFs in the current version of the IDHEAS-ECA report. However, in addition to the different totals (i.e., 14 vs. 15), it is evident that there are some functional differences in the definitions, scope, and attributes of a few PIFs. Those differences may affect how the analysts interpreted and applied specific PIFs for the evaluations in this study.

Based on these differences, it seems apparent that the analyses which were performed and documented in this study did not use the current version of the IDHEAS-ECA guidance. Furthermore, the IDHEAS-ECA software tool contains embedded numerical values for specific human error probabilities (HEPs) and PIF attribute weights. I do not know whether, or how, the current version of the software may differ from that used in this study.

A public version of the current IDHEAS-ECA report and guidance was published in February 2020. This FLEX HRA report will apparently be published in late 2020 or some time in 2021.

It is very important that this report must clearly document the fact that the analyses in this study and their documentation are not based on the current version of the IDHEAS-ECA guidance. The report should also describe how specific elements of the analyses or their documentation might differ if the current version of the guidance were used. That comparison should also address differences that may be related to interim changes in the software tool or its numerical values for specific HEPs and PIF attribute weights.

***JWS Note:*** The discussion in Section 4.2 refers to the "6-step IDHEAS-ECA process". The current IDHEAS-ECA guidance describes an 8-step analysis process. I do not know if the different number of steps is due to differences in the guidance used for this study, or whether it is an editorial oversight in this report.

***JWS Note:*** In retrospect, Footnote 3 in the Executive Summary and Footnote 46 in Section 5.5 provide a hint that there might be differences. However, those footnotes can be easily overlooked, and they do not draw readers' attention to important differences that may affect the use or interpretation of this report and how it relates to the current IDHEAS-ECA guidance.

## 4. General Comment

The IDHEAS methodology described in NUREG-2198 and the IDHEAS-ECA application of that methodology explicitly evaluate and quantify two contributions to the overall human error probability (HEP) for each modeled action. The cognitive contribution ($P_c$) accounts for scenario-specific conditions that affect human cognitive performance, as represented by the combined effects from several performance-influencing factors (PIFs). The scenario timing contribution ($P_t$) accounts for the probability that the action cannot be completed within the scenario-specific time constraints, as determined by uncertainties in the amount of time that is available to perform the action ($T_{avail}$) and the amount of time that is needed to complete that action ($T_{reqd}$).

This study evaluates and quantifies only the cognitive contribution ($P_c$) to each HEP. It does not discuss, evaluate, or quantify the scenario timing contribution ($P_t$) to the HEP for any modeled action. Therefore, this study is an incomplete demonstration of how the IDHEAS methodology and the IDHEAS-ECA application are used to perform an analysis of the actions to deploy and use FLEX equipment.

In particular, for the "base case FLEX scenario", the project team apparently assumed that the nominal FLEX validation exercises are adequate to fully justify a conclusion that $P_t = 0$ for each evaluated action. The report contains discussions about how the validation exercises demonstrate that the actions are feasible. The scenario description provides nominal times at which each action is completed. However, the analysis does not document the time when the batteries will be functionally depleted ($T_{avail}$) or the uncertainty in that time. It also does not document the uncertainties in the times that are needed ($T_{reqd}$) to shed the additional FLEX DC loads, clear the debris, transport the diesel generator and its cables, connect the generator, get it running, and re-energize the necessary loads. Thus, based on the available information, it is not possible to quantify the scenario timing contribution ($P_t$) to the overall HEP for the actions to provide alternative power from the FLEX diesel generator. It is also not possible to understand why that contribution is necessarily negligibly small, especially for a scenario which involves a "relatively short battery life" and an analysis that does not evaluate the efforts that are needed to clear the debris. Furthermore, the documentation for that analysis does not discuss how the project team or the individual analysts considered this element of the IDHEAS methodology.

The "non-FLEX scenarios" are clearly different from the FLEX validation exercises. The documentation for those scenarios similarly does not address how the project team or the analysts considered how uncertainties in the scenario timing might affect the quantified HEPs. For example, for the loss of all feedwater scenario, several timing assumptions affect both $T_{avail}$ and $T_{reqd}$ for the modeled action. However, no uncertainties for any of the assumed times are discussed or quantified. Thus, it is not apparent how, or whether, the analysts considered the scenario timing contribution ($P_t$) to the HEP for that action. Similar comments apply for the "non-FLEX" station blackout scenario.

Section 6.2 briefly notes that:

> "Timing data, Pt, was discussed during the workshop, but was not consistently used when applying IDHEAS-ECA (in part, because there was expansive time available for the operator actions being addressed). Also, in some cases, timing parameters were not clearly defined or known for the scenarios. Overall, HEP contributions from timing concerns were not considered to be a major contributing factor to the overall HEP."

In practice, there is no evidence that the project team systematically developed, documented, or examined the information about scenario timing and its uncertainty that is needed to objectively evaluate $P_t$ for any of the actions, either quantitatively or qualitatively. Therefore, despite the assertion in Section 6.2, this report contains no clear technical justification for the conclusion that "timing concerns were not considered to be a major contributing factor to the overall HEP".

It is essential that the final study report must clearly document this fundamental deficiency and explain why the analyses do not address or quantify the HEP contribution from event scenario timing constraints (i.e., $P_t$). If the project team simply focused only on an evaluation of the HEP contribution from cognitive performance (i.e., $P_c$), then the report should clearly document that fact. The report should also acknowledge this limitation and explicitly note that this study does not demonstrate how the IDHEAS methodology and the IDHEAS-ECA guidance are used to evaluate the effects from scenario timing.

Subsequent comments address specific issues regarding the treatment of scenario timing information in this study.

Why does this study not address or quantify the HEP contribution from $P_t$?

How does this study demonstrate a complete analysis of the actions to deploy and use FLEX equipment according to the IDHEAS methodology and the guidance in the IDHEAS-ECA application?

Why does the report not clearly acknowledge and document this fundamental omission from the analyses?

**5. Section 1.3.2, HRA Analysts; Section 1.3.3, FLEX and Operational Experts**

Section 1.3.2 very briefly summarizes the backgrounds and responsibilities of the three NRC analysts and three industry analysts who performed the human reliability analyses (HRAs). Section 1.3.3 briefly summarizes the responsibilities of the operational experts who supported this study.

One sub-bullet item in Section 1.3.3 notes that operational experts participated:

> "in support of HRA analyst understanding of scenarios – before and during FLEX HRA Workshop"

From this introductory material, I understand that the operational experts had extensive involvement with compilation and interpretation of technical information about the plants, procedures, and training, including detailed discussions during the site visits. I also understand that they were involved integrally with the development and descriptions of the three scenarios. Section 5 indicates that "FLEX experts" were available to provide additional supporting information during the HRA workshop.

***JWS Note:*** A footnote in the introduction to Section 5 indicates that two HRA analysts did not attend the workshop in person and participated only by phone.

Contemporary guidance emphasizes the fact that it is very important that at least one member of the HRA team should have actual operating experience, preferably at the specific plant that is being analyzed, or one that is very similar. That experience is very important. For example,

regardless of the amount of detail that is provided in a written operational narrative and other qualitative information about a particular scenario, it is often very difficult for analysts who have no actual operating experience to fully understand and appreciate all of the challenges that are faced by the plant operating crew. Without that perspective, analysts may overlook relevant questions about the entire scenario context, and they may not ask the "operational experts" about that information.

Did any of the HRA analysts have actual nuclear power plant operating experience?

If not, why was that not a consideration for selection of the analysts for this study?

**6. Section 2, Plant Site Visits, General Comment**

This is a very good summary of the site visits. The preparatory information in Section 2.2 through Section 2.5 is thorough and well-organized. Those sections contain useful experience and guidance for considerations that apply for any site visit to collect information to support a human reliability analysis (HRA).

**7. Section 2.5.2, Attendees for BWR Plant Site Visit; Section 2.5.3, Attendees for PWR Plant Site Visit; Section 3.4.1, Development of the FLEX Scenario**

The introduction to Section 2.5.2 notes that:

> "Consequently, it was important that the attendees of the plant site visits include ***some of the HRA analysts*** who would later perform HRA quantification." [emphasis added]

The introduction to Section 2.5.3 notes that:

> "As for the BWR plant site visit, the participation of ***HRA analysts*** and FLEX experts in the PWR plant site visit was ***critically important*** to later project tasks." [emphasis added]

Section 3.4.1 notes that:

> "Because the NRC project team, FLEX experts, and ***most of the HRA analysts*** attended the plant site visits, recollections of these visits (e.g., observations of a seismic event response in the plant-specific simulator) aided in scenario discussions." [emphasis added]

The preceding sections of the report emphasize the importance of technical and operational information that is obtained during the site visits to provide a realistic basis for the human reliability analyses (HRAs). Very importantly, site visits also provide analysts with valuable personal experience and insights about plant-specific features, operators' perspectives, and expected personnel actions in the context of each scenario. That personal experience cannot be gained by reading reports and site visit notes, or by listening to others' observations and opinions. Therefore, to achieve a well-founded common understanding of the plant, the scenarios, and numerous factors that influence personnel response, it is very important for the entire HRA team (i.e., all analysts) to participate in the site visits.

The BWR site visit attendees seem to include only two of the six analysts. The PWR site visit attendees seem to include only three analysts, one of whom also visited the BWR. Thus, it seems that only one analyst attended both site visits, three analysts each attended one site visit, and two analysts did not attend either site visit.

Is that correct?

Why did all six analysts not attend both site visits?

How did the lack of consistent personal experience from the site visits affect the overall HRA efficiency (e.g., due to specific analyst needs for more information, etc.)?

How did the lack of consistent personal experience from the site visits affect the overall HRA technical quality (e.g., due to inconsistent analyst understanding of the plant, how the scenarios evolve in that plant, etc.)?

**8. Section 2.6.3.1, PRA Modeling for FLEX Strategies; Section 3.1, General Process of Developing Scenarios**

Section 2.6.3.1 notes that:

> "Preliminarily, there appears to be a mismatch between the success criteria used for FLEX and that ***typical for PRAs***. Namely, the event tree headings and end states for FLEX strategies ***do not correspond with core damage***. For example, failure to deploy the FLEX DG before DC batteries fail does not equate to core damage." [emphasis added]

Section 2.6.3.1 also notes that:

> "Further investigation and discussions are needed to clarify ***this potential conservatism***. Although this potential conservatism is not within the scope of the FLEX HRA Project, some discussion of this issue will be pursued." [emphasis added]

Section 3.1 notes that one of the important considerations for developing the scenarios for this study is that:

> "FLEX strategies have been developed with different 'end states' than that for a ***typical PRA*** (e.g., ***FLEX 'success criteria' do not correlate with PRA system or plant functional success criteria so a FLEX 'failure' is not a failure in PRA space***)" [emphasis added]

I am very confused about the purpose and the intended implications of these discussions. I do not understand the technical basis for the assertions about "typical" PRA success criteria, or why these discussions are relevant to an integrated PRA model that accounts for the deployment and use of FLEX equipment. Furthermore, I do not understand what "this potential conservatism" is in the context of these discussions.

Many models for system responses and personnel actions in essentially every modern PRA do not use the onset of core damage as the undesired condition that determines their functional success criteria. Examples include actions to locally start equipment or re-position valves after failures of their automatic signals; evaluations of various time windows to restore offsite power, depending on the capacities of non-safety-related and safety-related batteries; restoration of thermal barrier cooling or seal injection flow before reactor coolant pump seals begin to fail; restoration of a feedwater supply before plant conditions require initiation of feed and bleed cooling; performing an active secondary cooldown and reducing primary pressure to stop the loss of inventory during a steam generator tube rupture event; cooling down and establishing closed-loop residual heat removal cooling to avoid the need for high pressure or low pressure

recirculation flow from the containment sump; suppressing a fire before additional cables or equipment are damaged; selectively de-energizing AC and DC circuits to preclude or mitigate effects from fire-induced spurious actuations; opening selected drainage pathways to prevent flooding inundation of specific plant locations; venting to extend the available time to restore suppression pool cooling; and many, many other actions, none of which are related directly to core damage or containment failure.

The functional success criteria and associated models for personnel actions to provide alternative power from a FLEX generator or alternative makeup from a FLEX pump are not fundamentally or conceptually different from these typically modeled actions. As for every human action in every PRA, the success criteria and the amount of time that is available to complete each action are determined by the specific function that the action is intended to provide and how the lack of that function affects the continued progression of the event scenario.

***JWS Note:*** This comment also applies to the discussion of FLEX success criteria in the first bullet item in Section 7.2.

What is the technical basis for the implication that "typical" PRA models do not address personnel actions that are not related directly to preventing core damage?

In other words, what is the technical basis for the implication that core damage is always the direct consequence from failure of every action that is modeled in a "typical" PRA?

In particular, what is the technical basis for the assertion that "FLEX 'success criteria' do not correlate with PRA system or plant functional success criteria so a FLEX 'failure' is not a failure in PRA space"?

What is a specific example that illustrates this distinction?

Why is it implied that a conceptually different type of event tree or fault tree logic is needed to integrate FLEX actions into the PRA models?

Why is it implied that a different type of description is needed for scenarios that involve the use of FLEX equipment?

What is "this potential conservatism" in the context of this discussion?

**9. Section 2.6.3.2, HRA Feasibility Assessment for FLEX Strategies**

This section notes that:

> "The ***concept of feasibility was formally defined*** for HRA / PRA in the 'Joint EPRI/NRC-RES Fire HRA Guidelines,' NUREG-1921 (July 2012) [ref]. This reliability-based definition is based on the deterministic definition provided in NUREG-1852, 'Operator Manual Actions' [ref], which also addressed ***fire events***. The definition of HRA feasibility was later expanded for main control room abandonment (MCRA) scenarios in ***fire events*** with Supplements 1 (August 2017) [ref] and 2 (June 2019) [ref] to NUREG-1921." [emphasis added]

This discussion seems to imply that the concept of a feasibility assessment was developed in the referenced NUREGs and that it is somehow related uniquely to certain types of event

scenarios. It also seems to imply that the need for a feasibility assessment is not included in the IDHEAS methodology, which should be the primary reference for this report.

The notion of a feasibility assessment has always been an integral part of the human reliability analysis (HRA) process, regardless of the methodology that is used to estimate human error probabilities (HEPs). Simply put, all HRA methods state that PRA models should include only those actions which the analysts determine can actually be performed in the context of the evolving scenario and the amount of time that is available. Section 3.5 of NUREG-1921 describes initial feasibility considerations that are made in every HRA. Section 4.3 of NUREG-1921 contains more detailed guidance for evaluating feasibility in the specific context of event scenarios that involve fire damage. However, the basic considerations that are described in that guidance apply to any type of event scenario and the associated personnel actions.

***JWS Note:*** Please refer to my September 20, 2019 comments and my September 24, 2020 comments on NUREG-2198. To avoid confusion about the possible relevance of a feasibility assessment to only certain types of event scenarios, I recommended that NUREG-2198 should explicitly contain guidance for the performance of a feasibility assessment. Section 7.3 of the current version of NUREG-2198 simply refers analysts to the feasibility assessment guidance in NUREG-1921. On the other hand, I also think that it might be argued rather convincingly that the detailed scenario-specific evaluation of performance-influencing factors (PIFs) that affect cognitive response (i.e., $P_c$) and explicit evaluation of the effects from time uncertainties (i.e., $P_t$) in the IDHEAS methodology reduce the need for a separate feasibility assessment. If either of those effects make a proposed action truly infeasible, the analysis should result in an estimated HEP of 1.0.

***JWS Note:*** I know that the intent of this section is to summarize the general considerations that apply for a feasibility assessment. Those considerations are discussed very well in NUREG-1921, and it is worthwhile to summarize them as is done in the bullet points. My concern is that readers will interpret the introductory paragraph to imply that feasibility assessment is a rather new concept, and that it has been developed primarily for special types of event scenarios.

Why does this discussion imply that the concept of a feasibility assessment is somehow related uniquely to the guidance in NUREG-1921, or that it might apply only for specific types of actions or event scenarios?

If NUREG-2198 is not revised, can the introduction to this section simply note that the IDHEAS general methodology recommends that a feasibility assessment should be performed according to the guidance in NUREG-1921 (and then list the bullet items)?

**10. Section 2.6.3.2, HRA Feasibility Assessment for FLEX Strategies**

This section notes that:

> "Based on preliminary reviews of two ***plant-specific validations*** of FLEX strategies, it appears that the approach for the development and validation of FLEX strategies ***generally addresses*** the above feasibility assessment criteria. Consequently, it is ***assumed that operator actions addressed in the FLEX HRA project are feasible*** from the perspective of HRA. However, as in any HRA, the issue of HRA feasibility will be considered as a continuous step throughout the analysis." [emphasis added]

It also notes that:

> "Also, while HRA ***feasibility may have been adequately addressed for FLEX scenarios***, the use of FLEX strategies, procedures, and equipment in non-FLEX scenarios may not be satisfied (especially, because the timing constraints for PRA success criteria may be significantly shorter)." [emphasis added]

I disagree very strongly with the implications of these paragraphs. In particular, despite the rather mild caveats, I am very concerned about how analysts will interpret this "NRC-recommended" guidance.

It is not appropriate to use FLEX strategy validations that were performed for regulatory-focused purposes within very well-defined scenario criteria to infer that desired actions are feasible in the context of very different event scenarios, regardless of whether those scenarios are "FLEX" or "non-FLEX". A plant-specific and scenario-specific evaluation must always be conducted to determine whether a proposed action is actually feasible.

Of course, it is perfectly fine for the project team to assume that all of the actions which are evaluated in this particular study are feasible. That just means that the scope of these particular human reliability analyses (HRAs) has been simplified for the purposes of this exercise by omitting an evaluation of the action feasibilities. However, I do not think that it is appropriate to refer to two regulatory-oriented validations for specific scenarios at specific plants as an implied technical justification for concluding that all of the modeled actions are actually feasible in the context of the scenarios in this study. I am concerned that analysts will simply refer to this decision as tacit endorsement of similar "generic" inferences without performing an objective plant-specific and scenario-specific feasibility assessment.

Why does this section imply that these types of regulatory-oriented validations can be used as a basis for conclusions that proposed actions are feasible in the context of very different event scenarios?

Why does this section not just state that a formal feasibility assessment was not performed for this exercise (e.g., because it is not plant-specific), and that the effort needed for these HRAs was reduced by simply assuming that each of the actions is feasible?

**11. Section 2.6.3.3, Procedures for Implementing FLEX Strategies, Editorial Comment**

The discussion in this section is very good. However, it notes that:

> "while almost all NPPs have a severe weather procedure that addresses many hazards, some NPPs may have other hazard-specific procedures (e.g., procedure for a ***seismic event***) which may be entered even ***before*** a reactor trip and entry in the EOPs and which may have transfers to FSGs" [emphasis added]

Citation of a specific procedure for seismic events is not a good example of procedures which may be used in an anticipatory context before a reactor trip occurs.

Do any plants actually have these types of anticipatory procedures which contain specific links to the FSGs (i.e., outside the context of the EOPs)?

**12. Section 2.6.3.4, Skill-Sets, Training, and Task Analysis**

This section notes that:

> "As noted elsewhere in this report, the type of portable equipment selected industry-wide is ***more robust and simpler to operate*** than equipment typically operated in NPPs and modeled in PRA." [emphasis added]

I do not understand why the "robustness" of portable FLEX equipment is relevant to a discussion about its ease of use.

It is also not apparent why this equipment is universally "simpler to operate" than installed plant equipment for which local actions are often evaluated in a "traditional" PRA. Startup and operation of a portable generator may, or may not, be easier than local startup and operation of an installed diesel generator. For example, some of the experts' discussions in their Justifications for the estimated human error probabilities (HEPs) in Section 3.1.3 of Volume 1 of this study indicate that it may be more difficult to control the initial and subsequent loading of a small generator and prevent it from tripping, compared to a large generator that has more reserve capacity. Startup and operation of a portable diesel-driven pump may, or may not, be easier than local startup and operation of an installed turbine-driven pump. However, it is not apparent why startup and operation of a diesel-driven pump is easier than local startup and operation of an installed motor-driven pump.

I am concerned that this "generic" characterization of FLEX equipment will inappropriately bias analysts' assessments of how easy, or difficult, it is to use plant-specific FLEX equipment during a particular event scenario, in the context of the available plant-specific hands-on training.

***JWS Note:*** This comment also applies to the next bullet item in this section, which characterizes debris removal equipment as universally "robust and simple to operate". It is not likely that many nuclear power plant operators, security personnel, or whoever else is tasked to clear debris actually own and regularly operate large tractors, plows, front-end loaders, graders, bulldozers, or similar equipment that is provided at a particular plant. Most people in the U.S. do not even know how to drive an automobile with a manual transmission.

Why is the "robustness" of portable FLEX equipment relevant to a discussion about its ease of use?

Why does this "NRC-approved" guidance imply that portable FLEX equipment is universally "simpler to operate" than equipment that is installed in the plant?

**13. Section 2.6.3.5, Important Aspects Related to Timing Validations and Timelines, Editorial Comment**

This section notes that:

> "For example, inputs for the time available and time required for operator actions are important in the determination of the feasibility[20] of operator actions in HRA and are used as direct inputs in ***certain HRA quantification methods***." [emphasis added]

This study demonstrates how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. The IDHEAS methodology

explicitly accounts for uncertainties in the amount of time that is available to perform an action (i.e., $T_{avail}$) and the amount of time that needed to perform that action (i.e., $T_{reqd}$) as a direct contribution (i.e., $P_t$) to the total human error probability (HEP). This report should explicitly note that the IDHEAS methodology includes this quantitative evaluation. It may be appropriate to mention that other methodologies also include timing evaluations as an input to their quantification models, but the emphasis in this report should remain focused on IDHEAS.

**14. Section 2.6.3.5, Important Aspects Related to Timing Validations and Timelines, Editorial Comment**

This section notes that:

> "NUREG-1921 Supplements 1 and 2 [refs x and y] provide examples of such timelines and describe how they are useful to HRA / PRA."

This study demonstrates how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. Therefore, the emphasis in this report should remain focused on the IDHEAS methodology. Section 5.3 in the current version of NUREG-2198 contains an improved discussion of a timeline, and it defines the time intervals that are used in the IDHEAS methodology. Therefore, I think that this introduction to the concept of a timeline should first refer analysts to the guidance in NUREG-2198.

That being said, Figure 6-2 in NUREG-1921 provides a good general depiction of a timeline for two coincident actions. Several figures in Section 7 of NUREG-1921 Supplement 1 provide very good depictions of complex timelines. The examples in NUREG-1921 Supplement 2 do not add many more insights about how to develop a complex timeline.

Thus, I think that this section should first cite NUREG-2198 as the basic conceptual reference for a timeline that is used in analyses performed according to the IDHEAS methodology. It could then mention NUREG-1921 Supplement 1 for examples of how timelines are used to depict complex relationships among multiple sequential and coincident actions.

**15. Section 2.6.3.5, Important Aspects Related to Timing Validations and Timelines, General Comment**

A preceding comment on Section 2.6.3.2 addresses the assertion that the results from two plant-specific validations can be used to justify the assumption that every action is feasible in the context of the specific "FLEX scenario" that is evaluated in this study.

This section contains a good high-level summary of the NEI guidance for the validation process, its assumptions, acceptance criteria, etc. The last paragraph provides an appropriate characterization of how the results from a plant-specific validation might be used to inform the timing information for sufficiently similar PRA scenarios at that plant.

**16. Section 2.6.3.6.1, Debris Removal**

This section notes that:

> "Debris removal is only required for FLEX scenarios (i.e., is not needed for non-FLEX scenarios)."

Suppose that a hurricane, tornado, derecho, ice storm, or blizzard causes extensive damage to the site's transmission lines or switchyard. Suppose also that the storm distributes substantial amounts of debris throughout the site, or it buries the site under a few feet of snow. Suppose further that the plant has two emergency diesel generators (EDGs). Neither of the EDGs or their cooling water supplies is damaged directly by the storm. However, both EDGs experience catastrophic hardware failures shortly after they start.

***JWS Note:*** Numerous combinations of other equipment failures might also disable the onsite AC power supplies, but it is easiest to use EDG starting failures for the purpose of this comment. If someone raises concerns that I ignored the plant's installed station blackout (SBO) diesel generator, it is located outdoors, and the storm damages its shelter, the diesel generator, or its connections to the plant.

These storms are certainly not "beyond-design-basis" external events. Nevertheless, it seems evident that personnel would need to clear the transportation pathways before the FLEX generator and pumps could be deployed.

The point of this comment is that arbitrary designations such as "FLEX scenarios" and "non-FLEX scenarios" might facilitate some administrative practices and regulatory discussions, but they are completely irrelevant to what plant personnel need to do during a wide variety of real-world scenarios that are evaluated in a full-scope PRA.

Are these examples of a "FLEX scenario" or a "non-FLEX scenario?

**17. Section 3.1, General Process for Developing Scenarios**

This section notes that:

> "Even though initial efforts were on understanding operational experience (e.g., the ***only SBO in the U.S.*** – a ***site-wide***, shutdown event at Vogtle [ref NUREG]), the next steps taken were aimed at collecting information to populate typical HRA documentation formats (e.g., SPAR analyses)." [emphasis added]

The station blackout (SBO) event at Vogtle occurred on March 20, 1990. I think that only Unit 1 lost all AC power. Other single-unit SBO events have occurred in the U.S. My earliest examples are a May 17, 1983 event at Fort St. Vrain and a July 26, 1984 event at Susquehanna Unit 2. I think that other SBO events may have occurred more recently. However, I do not keep organized records of these events, and I did not perform an exhaustive search for this comment, so I am not sure whether more recent events have actually occurred.

Did both Vogtle units lose all AC power during the March 20, 1990 event?

Why does this section state that the Vogtle event is the only SBO that has ever occurred in the U.S.?

Have any single-unit SBO events occurred in the U.S. since the Vogtle event (i.e., during any plant operating mode and due to any cause)?

**18. Section 3.1, General Process for Developing Scenarios**

This section notes that:

> "Even though initial efforts were on understanding operational experience (e.g., the only SBO in the U.S. – a site-wide, shutdown event at Vogtle [ref NUREG]), the next steps taken were aimed at collecting information to populate ***typical HRA documentation*** formats (e.g., ***SPAR analyses***)." [emphasis added]

I do not understand why "typical HRA documentation" that is provided for analyses that use the SPAR-H methodology is relevant to this study. I do not think that this reference is appropriate.

This study demonstrates how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. Therefore, the emphasis in this report should remain focused on the IDHEAS methodology. Section 4.2 of NUREG-2198 describes the information that is needed to understand the event scenario context for the required human actions. In particular, it contains guidance for the development of an operational narrative of the scenario. That narrative should describe the progression of the scenario from the time when the initiating event occurs until the time when each modeled action is needed. To establish the functional success criteria for those actions and the time that is available to perform them, the narrative should also describe how the scenario will continue if the actions are not taken. The narrative should summarize the plant-wide effects from the initiating event and any equipment failures that have occurred during the scenario (i.e., not just the failures that are explicitly included in the PRA model). That information is important for analysts to understand possible distractions, conflicting priorities, or demands for personnel to cope with other competing issues when the modeled actions are needed. The IDHEAS guidance also addresses how the documentation should establish the environment and situation context, system context, personnel context, and task context for each needed action.

These elements of the qualitative analysis are fundamental to the IDHEAS methodology. This report should emphasize them and clearly demonstrate how they were implemented during this study.

***JWS Note:*** Section 3.1 of the IDHEAS-ECA report summarizes the guidance for this element of the analyses. Worksheet A for each example analysis in Appendix C of that report documents the information developed for each scenario. Please refer to my October 11, 2020 comments on the IDHEAS-ECA report for comments on Section 3.1 and the worksheets.

Why does this section emphasize "typical HRA documentation" that is developed to support an application of the SPAR-H methodology?

Why does this section not specifically refer to the guidance that is described in the IDHEAS methodology (i.e., in Section 4.2 of NUREG-2198 or Section 3.1 of the IDHEAS-ECA report)?

**19. Section 3.2.1, Selection of the FLEX Scenario, General Comment**

This section notes that:

> "In order to address these concerns, the FLEX scenario selected is for a BWR NPP such as that described in the EPRI FLEX HRA report [x]."

The EPRI FLEX HRA report is EPRI 3002013018, "Human Reliability Analysis (HRA) for Diverse and Flexible Mitigation Strategies (FLEX) and Use of Portable Equipment: Examples and Guidance", November 30, 2018. I do not have a copy of that proprietary report. Therefore,

my comments on the FLEX scenario for this study are based only on the information that is provided in this report.

**20. Section 3.3, General Assumptions**

This section summarizes general assumptions that apply for all three scenarios evaluated in this study. It lists six assumptions that are apparently consistent with those used in NEI 12-06 and EPRI 3002013018. Those assumptions are reasonable and appropriate for this study.

The last paragraph in this section notes that:

> "Note that, since the non-FLEX scenarios do not involve an external event, that the list above is not identical to that given in NEI 12-06 and EPRI's FLEX HRA report since these two documents deal with beyond-design-basis external events (BDBEE)."

I was initially confused by this paragraph. After reading it a couple of times, I think that it means that the NEI report and the EPRI report contain additional assumptions that pertain specifically to some elements of the beyond-design-basis external event (i.e., the FLEX scenario), and those assumptions are not used in this study.

Is that a correct interpretation of this paragraph?

If not, what are the differences between the assumptions in this study, compared to the NEI and EPRI reports?

Are those differences relevant to an understanding of the scenarios that are evaluated in this study (especially the FLEX scenario)?

**21. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

This section notes that:

> "For example, the ***traditional PRA scope*** that limits modeling to the first 24 hours after plant trip was adopted." [emphasis added]

"Traditional PRA" models typically use a 24-hour mission time to quantify the unavailability of equipment due to failures that occur during its operation (e.g., running failures of diesel generators or pumps, spurious opening or closure of valves, etc.). There is a long history of discussions about that applied 24-hour mission time, which I will sidestep here. For the purpose of this comment, I fully acknowledge that a 24-hour mission time is traditionally used as a nominal parameter for quantification of equipment unavailabilities.

***JWS Note:*** When I read the "24-hour mission time" assumption in Section 1.4, I assumed (perhaps naively) that it pertained to this issue.

Since this assumption addresses a 24-hour "modeling" limit, I have a broader concern.

In a "traditional PRA", it is not appropriate to truncate an event sequence and assign it to a success state, simply because core damage did not occur within 24 hours after the initiating event. For example, based on a realistic analysis of the plant thermal-hydraulic response, suppose that a tank contains enough water for 28 hours of injection flow to keep the core cool.

Suppose also that core damage will occur if that tank is drained, and an alternative source of makeup is not aligned. When the tank is drained, core damage might not begin for another 3 hours, accounting for heatup and boil-off of the remaining water in the reactor vessel. In other words, core damage will begin about 31 hours after the initiating event occurred. In this case, many PRA models evaluate whether an alternative water supply can be aligned, despite the fact that the core was not damaged within the first 24 hours. The available time window for personnel actions to align the alternative supply begins when the operators receive the first cue that it is needed, and it ends when core damage begins.

Of course, there are always pragmatic considerations. In practice, analysts often use approximate criteria of 48 hours or 72 hours to justify the assumption that an appropriately "safe and stable" state has been achieved without the need for further analysis. So, in the tank example, if the inventory is sufficient to maintain injection for 48 hours or 72 hours, the analysts might not evaluate whether an alternative water supply is available. That assumption should be documented in each PRA, and it often varies from study-to-study. I am not aware of any consistent general guidance for its use. The analysis time interval also typically expands when the Level 1 PRA is extended to a Level 2 PRA, and it expands further for a Level 3 PRA.

With specific regard to the use of on-site FLEX equipment, it seems that the assumption that an appropriately "safe and stable" state has been achieved should be based on the time when additional equipment is available from the SAFER distribution center. So, for example, suppose that failure to align the onsite FLEX equipment will result in core damage before the SAFER equipment arrives and is connected. That condition should not be assigned to successful termination of the event sequence, even if core damage will not begin until considerably more than 24 hours after the initiating event. Of course, in an actual PRA, analysts would also evaluate whether offsite power can be reconnected or if undamaged onsite equipment can be restored to prevent core damage before the SAFER equipment arrives.

***JWS Note:*** This comment also applies to the specific assumption in this section that "The HRA / PRA model addresses accident progression out to 24 hours after the initiating event". It also applies to the same 24-hour assumption in Section B.3 of Appendix B, Section 3.5.1.2, and Section 3.5.2.2.

How does the applied 24-hour modeling limit affect the specific analyses in this study?

**22. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

One of the assumptions in this section is:

> "The initiating event causes a Loss of Offsite Power (LOOP) and subsequent Station Blackout (SBO)."

From other assumptions, I know that one of the two installed emergency diesel generators (EDGs) was out of service for extensive maintenance when the earthquake occurred. I do not know why power is not available from the remaining EDG.

Section B.1 of Appendix B contains more information about this scenario. It notes that the second EDG failed to start. That is very important information. In particular, the EDG apparently did not sustain direct damage from the earthquake. Thus, it is likely that substantial attention and personnel will be allocated to efforts to troubleshoot the problem, make any needed repairs, start the EDG, and restore power. If the EDG had sustained extensive seismic

damage, it is likely that personnel would conclude rather quickly that it could not be used. Thus, in this particular scenario, supervisors may be more reluctant to at least partially abandon attempts to restore the EDG, declare that an extended loss of AC power (ELAP) condition exists, and turn their attention to shedding DC loads and deploying the FLEX equipment.

***JWS Note:*** The scenario summary in Section B.1 notes that "within the first hour", "the equipment operator attempts to restart the EDG but determines that major repairs are needed".

Why does this section not describe why power is not available from the second EDG, so readers do not need to search for that important information in Appendix B?

**23. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

One of the assumptions in this section is:

> "FLEX validation exercises and integrated timeline use the same starting point for the 'start time' (or time delay) and the 'success criteria' (or time available).[29] This starting point is ***assumed to be t=0 (or reactor trip and time of the initiating event)***." [emphasis added]

The simple explanation for this assumption is not conceptually consistent with the timeline and the functional definitions of the time intervals in the IDHEAS methodology. In particular, it may be misleading for some analysts and readers.

In the context of the IDHEAS methodology, the system time window ($T_{SW}$) begins when the relevant damage occurs. That time often coincides with the initiating event, but that is not necessarily always the case for every action. The time window for a particular desired action begins when the first salient cue for that action occurs (i.e., after $T_{delay}$). That is the starting point for measuring the amount of time that is available for the action ($T_{avail}$) and the amount of time that is needed to complete the action ($T_{reqd}$).

The first salient cue for the action to declare an extended loss of AC power (ELAP) condition occurs when all AC power fails. Since the available emergency diesel generator (EDG) failed to start in this scenario, that functional condition and cue happen to occur at time t = 0. In this particular scenario, $T_{delay}$ = 0. In a different scenario, if the EDG had started and failed after running for 1 hour, the first cue for the action to declare the ELAP condition would have occurred at time t = 1 hour, regardless of the assumptions that are made in the FLEX validation exercises.

Please refer to my October 11, 2020 comments on the treatment of $T_{delay}$ in the IDHEAS-ECA report. Considering those comments, I think that it is very important to describe the functional conditions that determine when the first salient cue occurs. The assumptions for this scenario should not imply that those conditions always simply coincide with the initiating event.

***JWS Note:*** This comment also applies to this assumption in Section B.3 of Appendix B.

Why does this assumption not explain the functional conditions (i.e., loss of all AC power) that determine the first salient cue for the action to declare an ELAP condition and note that those conditions occur at time t = 0 in this particular scenario (i.e., because the EDG failed to start at that time)?

**24. Section 3.4.2, Specific Assumptions for the FLEX Scenario, Editorial Comment**

Footnote 29 in this section notes that:

> "Definitions for FLEX timing terms are different than that for HRA / PRA. Using the timing parameter definitions in ***NUREG-1921 (i.e., EPRI/NRC-RES Fire HRA Guidelines)***, 'start time' in FLEX is the time when a cue or procedure step occurs to start an operator action. In ***NUREG-1921***, this time is called 'time delay' (e.g., the time from t=0 that a cue occurs). Also, FLEX defines the 'success criteria' as the time by which an operator action should be performed to be successful. In HRA / PRA, this definition is associated with the term 'time available'." [emphasis added]

This study demonstrates how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. Therefore, the emphasis in this report should remain focused on the IDHEAS methodology. Section 5.3 in the current version of NUREG-2198 contains an improved discussion of a timeline, and it defines the time intervals that are used in the IDHEAS methodology. Therefore, this footnote should refer analysts to the guidance in NUREG-2198, rather than NUREG-1921.

***JWS Note:*** The timeline and definitions in Section 5.3 of the current version of NUREG-2198 are the same as those in Section 4.6.2 of NUREG-1921.

***JWS Note:*** This comment also applies to similar references to the NUREG-1921 timelines in Footnote 34 in Section 3.5.1.2 and Footnote 62 in Section B.4 of Appendix B.

Why does this footnote refer to NUREG-1921, rather than NUREG-2198?

**25. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

One of the assumptions in this section is:

> "FLEX validation times for operator actions are used as-is, even if they appear to apply to both units on site. (In some cases, it might be possible to separate Unit 1 and Unit 2 timing information. In other cases, it appears that a single operator will perform actions for both units.)"

I do not understand what this assumption means in the context of the analyses in this study, or how it affects those analyses.

***JWS Note:*** This comment also applies to this assumption in Section B.3 and the discussion of the validation times in Section B.4.3 of Appendix B.

Does this assumption mean that some of the personnel response times that were measured during the FLEX validation exercises may be longer than the times which might apply if only a single unit were affected?

If so, which specific times are affected by this assumption (i.e., which specific actions)?

If this is not a correct inference from this assumption, what are the actual purpose and practical effects from the assumption?

**26. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

One of the assumptions in this section is:

> "Even if there is ***some warning*** prior to the initiating event, there is inadequate time to prestage FLEX equipment that requires transportation." [emphasis added]

This scenario is initiated by a severe earthquake. Unless this assumption is intended to address the possible occurrence of pre-shocks before the main earthquake, it is not apparent why it is relevant to this scenario. If it is simply a "generic" assumption, I think that it adds confusion, rather than clarity, to an understanding of the scenario.

***JWS Note:*** This comment also applies to this assumption in Section B.3 of Appendix B.

Is this assumption specifically intended to address the possible occurrence of pre-shocks before the main earthquake?

**27. Section 3.4.2, Specific Assumptions for the FLEX Scenario; Appendix B, Section B.5.1, Mapping Relevant HRA Information on FLEX to IDHEAS-ECA "Context"**

One of the assumptions in Section 3.4.2 is:

> "Operator actions in the MCR are not directly affected by environmental conditions."

The introduction to Section B.5 in Appendix B notes that:

> "The NRC technical team provided the HRA analysts with examples of how to interpret the site visit notes (Section 2) into the terminology used in IDHEAS-ECA [ref]."

The discussion of "Environmental context" in Section B.5.1 of Appendix B notes that:

> "Operator actions performed in the MCR are not directly affected by environmental conditions."

Thus, it is apparent that the project team for this study made this conclusion and provided it to the analysts as a common assumption for their analyses.

The loss of all AC power disables normal Main Control Room (MCR) lighting, and it disables all ventilation and room cooling.

I do not know if this is simply an assumption that was made by the project team for the purposes of this study, or if it is a conclusion that is justified by supporting analyses, measured lighting levels, measurements of MCR temperature and humidity as a function of time, etc. Regardless of its technical basis, I think that the report should explicitly identify these effects on the MCR environment to document the fact that the project team considered them. It can then be noted that the project team assumed that they do not affect personnel performance for the purpose of this study.

***JWS Note:*** The summary of this scenario in Section 3.4.4 and Section B.1 of Appendix B notes that "After 1 hour, plant conditions begin to degrade" and specifically "Building heat up occurs due to loss of ventilation". It is also interesting to note that the event tree shown in Figure B-1 in

Appendix B contains Top Event ALTHVAC for "Alternate HVAC Alignment". However, that event tree is shown only to illustrate the logic model that was used for the analysis of this scenario in EPRI 3002013018, and I do not know what specific alternate ventilation it evaluates.

***JWS Note:*** The detailed scenario script in Table B-1 in Appendix B notes that actions to provide alternative MCR ventilation start at time t = 5.5 hours.

What is the technical basis for this assumption?

Why does this assumption not acknowledge the loss of normal lighting and loss of all MCR ventilation and cooling?

**28. Section 3.4.2, Specific Assumptions for the FLEX Scenario**

One of the assumptions in this section for the base case scenario is:

> "The modeled NPP has a ***relatively short*** battery life such that an Extended Loss of AC Power (ELAP) must be recognized at one hour after event initiation." [emphasis added]

The discussion of scenario Variation #1 notes that:

> "The modeled NPP has a longer battery life (e.g., ***approximately 4 hours; more than 1 hour but less than 12 hours***)." [emphasis added]

The IDHEAS methodology emphasizes the importance of a systematic evaluation of scenario timing. Uncertainties in the amount of time that is available to perform a desired action ($T_{avail}$) and the amount of time that is needed to complete that action ($T_{reqd}$) are explicitly evaluated as a contribution ($P_t$) to the overall human error probability (HEP). The battery life is one of the most important functional constraints that determine $T_{avail}$ during each scenario. Therefore, unless the analyses assign very large uncertainties for that time, vague discussions about the battery life are not consistent with the scenario-specific technical information that is needed to support an application of the IDHEAS methodology or the IDHEAS-ECA guidance.

***JWS Note:*** The scenario summary in Section B.1 and the assumptions in Section B.3 of Appendix B do not document the battery life.

The assumptions indicate that the decision to declare an extended loss of AC power (ELAP) condition must be made by time t = 1 hour during the base case scenario. The scenario summary in Section B.1 of Appendix B notes that "within the first hour", "the equipment operator attempts to restart the EDG but determines that major repairs are needed". After the ELAP decision is made, supervisors begin to use the FLEX Support Guidelines (FSGs) and to mobilize personnel responses according to that guidance. Subsequent actions to shed DC loads, clear debris, and deploy (transport, connect, and start) the FLEX generator must be completed before the batteries are depleted. Thus, the battery life is clearly a key constraint in the evaluation of $P_t$ for each of those actions.

What is the battery life for the base case scenario?

What is the battery life for scenario Variation #1?

How are these vague discussions about the battery life consistent with a scenario-specific

analysis that is performed according to the IDHEAS methodology?

**29. Section 3.4.2, Specific Assumptions for the FLEX Scenario; Section 3.4.4, Summary Description of the Base Case FLEX Scenario; Appendix B, Section B.5.1, Mapping Relevant HRA Information on FLEX to IDHEAS-ECA "Context"**

The discussion of "System context" in Section B.5.1 of Appendix B notes that:

> "Initially, there will several calls to the MCR from field operators to report what work was stopped by the seismic event and associated loss of all AC power. After those calls, the MCR environment will be ***less busy than usual*** since, without AC power, most systems will not be running." [emphasis added]

According to the introduction to Section B.5, this assessment was developed by the project team, and it was provided to the analysts as a common basis for their evaluations.

This does not seem to be a realistic depiction of the actual plant conditions shortly after the occurrence of a beyond-design-basis earthquake.

The assumptions in Section 3.4.2, the scenario summary in Section 3.4.4, and the information in Appendix B describe only conditions that are directly relevant to the specific actions that are evaluated in this analysis. In particular, they do not adequately describe the entire site-wide earthquake damage and the full context of this scenario from a plant-level operational perspective, as emphasized in the IDHEAS methodology and guidance. That information is essential for analysts to understand possible distractions, conflicting priorities, or demands for personnel to cope with other competing issues when the modeled actions are needed. Thus, this limited and focused scenario information may inappropriately bias analysts to disregard potentially important influences on personnel performance for the desired actions, especially during the first hour or two after the earthquake occurs and while aftershocks continue.

What site-wide structures, systems, and components are damaged by the earthquake (regardless of whether those items are explicitly included in the PRA model)?

Did the earthquake damage cause any consequential steam releases, flooding, or fires?

Did the earthquake damage cause any consequential releases of radioactive liquids or gases (e.g., from damaged waste processing or storage systems, with releases inside the plant or to the external environment)?

Are any onsite personnel injured (anyone, anywhere, who needs rescue efforts or medical attention)?

Considering the IDHEAS guidance for describing the "system context", why does the operational narrative for this scenario not include this information?

**30. Section 3.4.3, HFEs for the FLEX Scenarios; Appendix E, Section E.3, Table E-1 HRA for FLEX Project: Organizing Variations within Scenarios**

Section 3.4.3 identifies the four human failure events (HFEs) that are analyzed for this scenario. It notes that actions to clear debris, actions to deploy and use the portable FLEX pumps, and actions to refuel the diesel generator and pumps are not evaluated. It also notes that a

complete evaluation of the actions to initiate containment venting was not performed. It is certainly reasonable to limit the scope of this study by not quantifying the human error probabilities (HEPs) for these actions.

Section 3.4.3 notes specifically that:

> "Regarding actions associated with debris removal, it was agreed that this task, requiring only the skill set of a 'journeyman,' was ***not suited for HRA modeling***." [emphasis added]

An implication that "journeymen" do not make errors is certainly not supported by actual experience. More importantly, the implication that the IDHEAS methodology is not suitable for an evaluation of those activities is neither appropriate nor technically justified.

Table E-1 in Appendix E summarizes the project team's considerations of possible general categories of "FLEX scenarios" and "Non-FLEX scenarios", based on discussions that were held during the site visits and the workshop. Footnote 78 in that table applies for the actions to remove debris. It notes that:

> "Note that the HRA is ***not expected to model this activity***." [emphasis added]

I disagree very strongly with that conclusion and its implications in a report that contains "NRC-approved" guidance for the use of the IDHEAS-ECA methodology. However, since Table E-1 simply summarizes the team's preliminary discussions, I will only note here that an analysis which is performed according to the IDHEAS methodology ***must*** account for all relevant personnel actions, how they are integrated into the scenario evolution, and the time that is needed to perform those actions.

What is the technical basis for the project team's assertion that the IDHEAS methodology cannot be used to evaluate activities that are performed by a "journeyman" and to quantify an HEP for those activities?

**31. Section 3.4.3, HFEs for the FLEX Scenarios; Appendix B, FLEX Scenario for a BWR**

***JWS Note:*** This is a continuation of the immediately preceding comment. However, it addresses a different issue, so I separated them. It also addresses an issue that applies more broadly to the entire study. The discussion about uncertainty in the amount of time that is needed to clear the debris provided the first convenient opportunity to raise this broader concern.

This section notes that:

> "Also, there is ***significant uncertainty*** in what effort (e.g., amount of debris, affected plant areas, ***time required*** for removal) would be needed for the task of debris removal." [emphasis added]

The total amount of time that is needed to clear the debris, move the FLEX diesel generator to its operating location, connect the generator, and get it running affect the overall human error probability (HEP) for failure to provide alternative FLEX power before the plant batteries are depleted.

In particular, according to the IDHEAS methodology and the guidance in the IDHEAS-ECA

application, uncertainties in the amount of time that is available to perform a desired action ($T_{avail}$) and the amount of time that is needed to complete that action ($T_{reqd}$) are explicitly evaluated as a contribution ($P_t$) to the overall HEP. The battery life is one of the most important functional constraints that determine $T_{avail}$ for the actions to declare the extended loss of AC power (ELAP) condition, shed DC loads, and restore power from the FLEX generator.

The assumptions for this scenario indicate that the decision to declare an ELAP condition must be made by time t = 1 hour. After the ELAP decision is made, supervisors begin to use the FLEX Support Guidelines (FSGs) and to mobilize personnel responses according to that guidance. Subsequent actions to shed DC loads, clear debris, and deploy (transport, connect, and start) the FLEX generator must be completed before the batteries are depleted. Thus, the battery life is clearly a key constraint in the evaluation of $P_t$ for each of those actions.

The FLEX diesel generator cannot be moved to its operating location until its transportation pathway is cleared. Summaries of the information that was obtained during the site visits also indicate that the same equipment (e.g., trucks or tractors) may be used to clear the debris and to transport the generator. Thus, it is evident that the total elapsed time before the diesel generator is supplying power must account for the amount of time that is needed to clear the debris. For example, if more time is needed to clear the debris, less time remains available for the actions to transport, connect, and start the diesel generator. Thus, the HEP for those actions would have a correspondingly higher contribution from $P_t$.

The scenario summary in Section 3.4.4 and the detailed information in Table B-1 in Appendix B provide nominal estimates for the amount of time that is needed to shed the additional FLEX DC loads (30 minutes); clear the debris (1 hour); and transport the diesel generator and its cables, connect the generator, and get it running (2.5 hours).

The analysis does not document the time when the batteries will be functionally depleted after the load shed is performed, or the uncertainty in that time. In practice, that time would be determined by the first functional impact that changes the scenario progression or the information that is available for personnel to understand the plant status (e.g., failure of RCIC control, re-positioning of DC-powered valves, loss of Main Control Room indications and displays, etc.). Furthermore, the analysis does not document the uncertainties in the times that are needed to perform each of the actions that are discussed in this comment.

Thus, based on the available information, it is not possible to quantify the scenario timing contribution (i.e., $P_t$) to the overall HEP for the actions to provide alternative power from the FLEX diesel generator, or to justify a conclusion why that contribution is necessarily negligibly small.

***JWS Note:*** For reference, Items 9, 12, 13, 14, and 18 in the detailed scenario script in Table B-1 in Appendix B provide the following estimated times, which are also listed in the scenario summary in Section 3.4.4.

- ELAP is declared at time t = 1 hour
- FLEX DC load shed is completed at time t = 1.5 hours (30 minutes after ELAP is declared)
- Debris removal is completed at time t = 2 hours (1 hour after ELAP is declared)

- Deployment of the diesel generator begins at time t = 3 hours (1 hour after the debris is cleared, 2 hours after ELAP is declared)

- The diesel generator is connected and operating at time t = 5.5 hours (2.5 hours after it's deployment began, 4.5 hours after ELAP is declared)

***JWS Note:*** Section B.4.3 of Appendix B discusses the criteria and assumptions that are used in the FLEX validation exercises. Those evaluations are the basis for the action times that are listed in Table B-1. Section B.4.3 provides nominal estimates for the amount of time that is needed to perform each action, except debris removal. It does not discuss uncertainties in those times. All times are characterized as "about xx minutes".

What is the amount of time until the batteries will be functionally depleted after the FLEX DC load shed is performed, and what is the uncertainty in that time?

What are the uncertainties in the estimated times that are needed to shed the FLEX DC loads; clear the debris; and transport the diesel generator and its cables, connect the generator, and get it running?

How do the analyses in this study address the evaluation of $P_t$, or justify why its contribution to the overall HEP for the action to deploy the FLEX diesel generator is negligibly small?

**32. Section 3.4.4, Summary Description of the Base Case FLEX Scenario, Editorial Comment**

One item listed under the bullet for "Within the first hour after reactor trip" is:

"MCR operators initiate containment venting"

The suppression pool is an integral part of the BWR containment. Therefore, this item is certainly accurate in a strict technical sense. It is also probably consistent with terminology that is used in the BWR procedures. However, many readers of this report may not be very familiar with BWR design details and terminology. They might be more apt to associate the drywell with a BWR "containment". They might also be familiar with initiatives to require venting capability for BWR drywells and large PWR containments. So they might be confused about why the operators would vent the "containment" at this point in the scenario. Thus, despite the technical accuracy of this item, I think that it would be better understood by a broader audience if it indicated that the operators initiate "suppression pool" venting.

***JWS Note:*** Footnote 30 helps to make the conceptual link with the suppression pool, but I think that explicit reference to the suppression pool vent avoids any confusion.

***JWS Note:*** This comment also applies to the same item in Section B.1 of Appendix B. The detailed scenario script in Table B-1 directly associates the start of containment venting with conditions in the suppression pool, so the relationship seems clear in that table.

Should this item indicate that the operators initiate "suppression pool" venting (rather than "containment" venting)?

**33. Section 3.4.4, Summary Description of the Base Case FLEX Scenario**

One item listed under the bullet for "After 1 hour, plant conditions begin to degrade" is:

> "Long-term RCIC operation (i.e., use of turbine-driven pump) is needed to maintain adequate core cooling."

This is the first mention of the reactor core isolation cooling (RCIC) system in the scenario summary. Beginning at time t = 0, RCIC is the only available system to maintain reactor vessel water inventory and core heat removal. Therefore, it is a bit surprising that it is not mentioned at the start of the scenario. I think that the intent of this particular item is to document the need to control reactor vessel pressure and suppression pool temperature, so that RCIC can remain operating for an extended period of time (i.e., with adequate steam pressure, without cavitation, and avoiding challenges to the suppression pool heat capacity limits).

***JWS Note:*** The detailed scenario script in Table B-1 in Appendix B notes that RCIC starts at time t = 0, and it discusses RCIC operation.

Is my understanding of the intent of this item correct?

Why does the scenario summary not explicitly document the fact that RCIC is providing reactor vessel makeup and core heat removal, beginning at time t = 0+?

**34. Section 3.5.1.1, Development of the Non-FLEX Scenario: "Sunny Day" Loss of All Feedwater, Editorial Comment**

This section indicates that Appendix B contains a more complete description of this scenario. It is described in Appendix C.

**35. Section 3.5.1.2, Specific Assumptions for the Non-FLEX Scenario – Loss of All Feedwater**

One of the assumptions in this section is:

> "FLEX validation exercises and the integrated timeline use the same starting point for the 'start time' (or time delay) and the 'success criteria' (or time available).[34] This starting point is ***assumed to be t=0 (or reactor trip and time of the initiating event)***." [emphasis added]

This assumption is not appropriate for this scenario. It is not consistent with the guidance in the IDHEAS methodology or the IDHEAS-ECA application.

Section 5.3 in the current version of NUREG-2198 contains an improved discussion of a timeline, and it defines the time intervals that are used in the IDHEAS methodology. In the context of the IDHEAS methodology, the system time window ($T_{SW}$) begins when the relevant damage occurs. That time often coincides with the initiating event, but that is not necessarily always the case for every action. The time window for a particular desired action begins when the first salient cue for that action occurs (i.e., after $T_{delay}$). That is the starting point for measuring the amount of time that is available for the action ($T_{avail}$) and the amount of time that is needed to complete the action ($T_{reqd}$).

According to the summary in this section and the more detailed information in Appendix C, this scenario evolves as follows:

- The unit is operating at power.
- Auxiliary feedwater (AFW) pump 1A is out of service for maintenance.
- A complete loss of all condensate flow occurs (all four condensate pumps fail).
- The reactor trip occurs at time t = 0.
- AFW pump 1B starts automatically at time t = 0, and it feeds at least one steam generator.
- AFW pump 1B fails at time t = 1 hour.
- Personnel must deploy a FLEX pump and align alternative makeup to at least one steam generator before the criteria for initiation of feed and bleed cooling occur.

***JWS Note:*** The scenario summary does not indicate how many steam generators are supplied by AFW pump 1B. While I was reading the detailed procedure summaries in Section C.6.1 and Section C.6.2 of Appendix C, I discovered that the plant apparently has four steam generators (e.g., criteria in Step 14 of FR-H.1). Since there are only two AFW pumps, I strongly suspect that pump 1B supplies two steam generators. However, I might be wrong. The number of steam generators that are fed during the first hour of this scenario is important, because the steam generator levels at time t = 1 hour determine the amount of time that is available until the feed and bleed criteria occur (i.e., $T_{avail}$).

The initiating event occurs at time t = 0. That time is important for this scenario, because it defines when the reactor trip occurs and when core decay heat production starts. Therefore, it is appropriate to indicate that the starting point for measurement of $T_{SW}$ is time t = 0.

The first salient cue for the actions to deploy the FLEX pump occurs when AFW pump 1B fails at time t = 1 hour. In other words, in this particular scenario, $T_{delay}$ = 1 hour. Thus, regardless of any assumptions that are made in the FLEX validation exercises, the starting point for measurement of $T_{avail}$ and $T_{reqd}$ in this scenario is time t = 1 hour, not time t = 0. In particular, in this scenario, $T_{avail}$ is determined by boil-off of the available steam generator water inventory from time t = 1 hour until the time when the feed and bleed criteria occur.

Why does this assumption indicate that the starting point for measurement of $T_{avail}$ and $T_{reqd}$ in this scenario is time t = 0?

**36. Section 3.5.1.2, Specific Assumptions for the Non-FLEX Scenario – Loss of All Feedwater**

A preceding general comment addresses the observation that this study does not provide a complete evaluation of the human error probabilities (HEPs) for the actions to deploy and use FLEX equipment, according to the IDHEAS methodology and the IDHEAS-ECA guidance. In particular, the analyses do not characterize or quantify the uncertainties in any time estimates, and they do not evaluate the scenario timing contribution ($P_t$) to the overall HEP for any action.

This section summarizes several assumptions that are made about the scenario timing. Some are very specific (e.g., 1 to 2 minutes, or less, to execute a step in a procedure). Others are much more approximate, but are much more important to the integrated analysis of personnel performance. For example, it is noted that:

> "It is assumed that it takes 20 minutes to satisfy that the red path criteria heat sink is met (in the Critical Safety Function Status Tree (CSFST)) after the 1B AFW pump fails to run (i.e., 80 minutes after reactor trip)."

It is also noted that:

> "It is assumed that the decay heat removed while 1B AFW pump runs in the 1st hour after reactor trip is such that feed-and-bleed criteria are not reached until after the time needed to deploy the FLEX pump (including time needed to get to relevant steps in FRH1.
> - Specifically, the criteria for F&B conditions are reached later than 78 minutes after FR-H1 is entered (i.e., more than 158 minutes after reactor trip)."

It is finally noted that:

> "It is assumed that deploying a FLEX pump for feeding a SG from the RWST takes one hour to perform from the time of dispatch."

According to these assumptions, after including the times to step through the procedures, just enough time is available for personnel to align alternative makeup from the FLEX pump. If there is reason to believe that any of these estimates are plausibly accurate, it seems apparent that quantification of the contribution from $P_t$ may be very important to the overall HEP for this action.

***JWS Note:*** Section C.3 in Appendix C does not contain a discussion of the technical bases for these timing assumptions.

What is the technical basis for each assumed time?

How are these assumptions and the analysis of this action consistent with the IDHEAS guidance for evaluating scenario timing uncertainties and their contribution ($P_t$) to the overall HEP?

**37. Section 3.5.1.2, Specific Assumptions for the Non-FLEX Scenario – Loss of All Feedwater; Appendix C, Section C.2.2, HRA Modeling; Section C.6.1, Non-FLEX Scenario – Procedure Path for Case #1; Section C.6.2 - Non-FLEX Scenario – Procedure Path for Case #2**

***JWS Note:*** After reading a lot of detailed material, I finally found the answer to my question in the summary of Step 13 of FR-H.1 in Section C.6.1 and Section C.6.2 of Appendix C. By that time, I had written most of this comment. The first part of it remains relevant for background information and my perspective on this scenario.

I could not find an important piece of information in Section 3.5.1.2 or Appendix C.

In many plants, the FLEX pumps are low pressure pumps, with a shutoff head of approximately 150 psig to 300 psig. The opening pressure setpoints for steam generator safety valves are typically in the range of approximately 1,000 psig to 1,200 psig. Thus, if the FLEX pump that is

used in this scenario is a low pressure pump, personnel must actively depressurize (i.e., blow down) a steam generator before the pump can deliver makeup flow.

The amount of time that is needed to reduce steam generator pressure below the FLEX pump shutoff head depends on the relief capacity of the available steam generator atmospheric relief valves and procedural limitations on the maximum allowed primary system cooldown rate (if any limit applies during these conditions).

This requirement may also cause supervisors to be rather reluctant to implement alternative steam generator makeup from the FLEX pump. In particular, active blowdown of the steam generator will rapidly exhaust much of the remaining water inventory, which provides additional time for efforts to restore main feedwater or auxiliary feedwater.

The scenario summary in Section 3.5.1.4 and the information in Appendix C do not mention actions to actively depressurize a steam generator. Similarly, the fault tree in Figure C-2 of Appendix C does not include that task.

Section C.2.2 of Appendix C contains a discussion of the Critical Task for "Operators fail to initiate use of FLEX pump (cognitive contribution)". That discussion notes that Item c under Step 5 of FR-H.1 is:

> "Dispatch field operator to 'align AF crosstie per 1FSG-3, Alternate ***Low Pressure*** Feedwater" [emphasis added]

Section C.5 of Appendix C contains discussions of the performance-influencing factors (PIFs) for "Key Cues and Indications" and "Procedures". Those summaries indicate that procedure 1FSG-3 pertains to "Alternate Low Pressure Feedwater". The detailed summaries of the procedures in Section C.6.1 and Section C.6.2 of Appendix C refer to "1BFSG-3, Alternate low pressure feedwater for AF crosstie".

Thus, the title of procedure 1FSG-3 (or 1BFSG-3) seems to clearly imply that the FLEX pump is a low pressure pump, and a steam generator must be depressurized for its use.

Section C.6.1 and Section C.6.2 of Appendix C contain detailed summaries of the procedures that apply during the two versions of this scenario. Step 13 of FR-H.1 notes that:

> "Step 13: Try to establish feed flow from any available ***low pressure source*** to at least one SG" [emphasis added]

A NOTE under Step 13 indicates that:

> "Bleed and feed should not be initiated due to low level in ***SGs being depressurized***, unless core exit temperatures are above 557 °F and rising." [emphasis added]

Item c in the summary of Step 13 of FR-H.1 notes that:

> "Check ***low pressure feedwater source*** – READY TO PROVIDE FLOW" [emphasis added]

It is unfortunate that these summaries do not reproduce the relevant steps after Item c. However, it seems evident that personnel must actively depressurize a steam generator before

the FLEX pump can deliver makeup flow. This is an integral task in the deployment, connection, and use of the FLEX pump to achieve the desired functional success criteria. Therefore, the PRA model for these actions and the associated human reliability analysis (HRA) must explicitly include the action to actively depressurize a steam generator. The PRA model must also include the equipment that is needed for that task (e.g., steam generator atmospheric relief valves and their support systems).

Section 3.5.1.3 indicates that the analysis of this scenario evaluates only the decision to initiate alternative makeup from the FLEX pump (i.e., to initiate deployment of the pump). The possible reluctance that is discussed in this comment could affect either the timing of that decision or several PIFs which are relevant to the estimated human error probability (HEP).

However, more importantly, this example should demonstrate how the IDHEAS methodology is used to systematically evaluate integrated personnel performance in the context of this scenario. The example should not selectively exclude actions that are essential to achieve the functional success criteria, simply because those actions are not labeled "FLEX-related". That omission is completely inappropriate for an example of "NRC-approved" guidance for the use of the IDHEAS methodology.

The HRA for this FLEX function is not complete without these essential analyses.

What is the shutoff head of the FLEX pump that is used in this scenario?

In particular, is it necessary to actively depressurize a steam generator before that pump will deliver makeup flow?

If it is necessary, are the operators instructed to depressurize one or two steam generators?

How much time is needed to reduce steam generator pressure below the shutoff head of the FLEX pump?

If it is necessary to depressurize one or more steam generators, why is that action not included in the summary of this scenario, the functional description of the actions that are needed to achieve successful alternative makeup from the FLEX pump, and the analyses of the HEPs for those actions?

**38. Section 3.5.1.3, HFEs for Non-FLEX Scenario – Loss of All Feedwater; Appendix C, Section C.2.2, HRA Modeling**

Section 3.5.1.3 notes that:

> "Although there are some differences between deploying a FLEX pump for a FLEX scenario and this loss of all feedwater scenario, the HRA analysts agreed that the HRA assessment would be similar in both cases. Consequently, the execution portion of the larger HFE was not addressed in this effort."

Section C.2.2 of Appendix C contains a discussion of the Critical Task for "Operators fail to initiate use of FLEX pump (contribution from execution)". It is noted that:

> "The execution contribution to this HFE is not developed; the critical tasks and associated performance influencing factors (PIFs) should be similar to that developed for the 'classic

FLEX scenario.' If time allows, HRA assessment of this HFE contribution could be performed as a variation on that for the 'classic FLEX scenario' since different NPPs underlie the two different scenarios."

This study does not evaluate the actions to deploy, connect, and operate the portable FLEX pumps during the "FLEX scenario". Section 3.4.3 simply notes that:

"For example, it was agreed that the operator actions associated with using the FLEX pump were similar to that for the FLEX DG."

This seems to be a rather nebulous extension of a rationale that has little technical justification or relevance to the actual event scenarios. For example, it seems very likely that evaluations of the time uncertainty contribution ($P_t$) to the overall human error probability (HEP) for these actions could be much different for each scenario. Furthermore, achievement of the functional success criteria in each scenario is not necessarily limited to moving the pump, connecting it, and starting it. As noted in the immediately preceding comment, if it is necessary to actively depressurize a steam generator, the integrated actions to achieve makeup flow from the FLEX pump during this scenario are significantly different from those which might apply during the FLEX scenario.

***JWS Note:*** This comment also applies to the discussion of the scope of this human failure event (HFE) in Section 6.4.

Rather than trying to provide rationales that may have poor technical justification, why does the report not simply state that the actions to deploy, connect, and operate the portable FLEX pumps were not analyzed during any of the scenarios evaluated in this study, due to project resource constraints?

**39. Section 3.5.2.2, Specific Assumptions for the Non-FLEX Scenario – SBO with One EDG Out for Maintenance, Editorial Comments**

The first paragraph in this section notes that:

"Such assumptions would include general training for use of FLEX equipment, FLEX human-machine interface (HMI), procedure support for deploying a FLEX ***pump***, etc." [emphasis added]

This scenario involves the use of FLEX diesel generators. It does not involve the use of a FLEX pump.

One of the assumptions in this section is:

"The initiating event (i.e., ***loss of all AC power***) and reactor trip occur at t=0." [emphasis added]

The initiating event for this scenario is not a "loss of all AC power". The initiating event is a "loss of all offsite power".

The assumptions indicate that emergency diesel generator (EDG) A fails to start during this scenario. As a consequence of that EDG failure, all onsite AC power is lost very shortly after the offsite power failure occurs (i.e., at essentially time t = 0). It is important to consistently

document these basic concepts. For example, if the EDG had started and failed after running for 10 minutes, the initiating event would still be the loss of offsite power at time t = 0. However, the station blackout would occur at time t = 10 minutes, and that would be the first salient cue for the modeled actions.

***JWS Note:*** Section D.3 of Appendix D indicates that the initiating event is a grid-related loss of offsite power (LOOP).

**40. Section 3.5.2.2, Specific Assumptions for the Non-FLEX Scenario – SBO with One EDG Out for Maintenance; Section 3.5.2.3, HFEs for Non-FLEX Scenario – SBO with One EDG Out for Maintenance**

One of the assumptions in Section 3.5.2.2 is:

> "This NPP has a ***very long*** battery life." [emphasis added]

Another assumption is:

> "The total time elapsed from reactor trip until when connections between the FLEX DGs and 4160 V bus are completed and the FLEX DGs started and synched is ***less than 1 hour***[37] (when ELAP would need to be declared)."

Footnote 37 indicates that:

> "Information is provided by plant-specific AOs."

Another assumption notes that:

> "The designated RO will dispatch the designated AO to perform the actions described in the contingency plan,[42] which include ***several breaker manipulations and electrical connections***, in addition to start of the FLEX DGs." [emphasis added]

Footnote 42 provides a reference to the plant-specific contingency plan.

The last assumption in Section 3.5.2.2 notes that:

> "Starting from when dispatched, the time needed for the AO to perform tasks associated with putting the pre-staged FLEX DGs into service is ***assumed to be 30 minutes***, including required travel time to performance locations after dispatch." [emphasis added]

Footnote 43 in Section 3.5.2.3 indicates that:

> "We decided to ***eliminate 'adding loads'*** to our discussions because we had inadequate information on the procedure guidance for this and how this would be implemented (including what steps would be taken by the AO and what the MCR operators would need to do)." [emphasis added]

The IDHEAS methodology emphasizes the importance of a systematic evaluation of scenario timing. Uncertainties in the amount of time that is available to perform a desired action ($T_{avail}$) and the amount of time that is needed to complete that action ($T_{reqd}$) are explicitly evaluated as a contribution ($P_t$) to the overall human error probability (HEP). The following discussion

summarizes my understanding of information that supports estimates of $T_{avail}$ and $T_{reqd}$ for the actions that are evaluated in this scenario.

***JWS Note:*** This comment includes the tasks for "adding loads" as part of the actions which must be completed to achieve the functional success criteria for use of the FLEX diesel generators. The next comment addresses completeness of this analysis as an example of the IDHEAS methodology and guidance.

**Estimation of $T_{avail}$**

The assumptions indicate that emergency diesel generator (EDG) A fails to start during this scenario. Thus, the first salient cue to align alternative power from the FLEX diesel generators occurs at time t = 0. The assumptions indicate that the turbine-driven auxiliary feedwater (AFW) pump starts successfully, the pressurizer power-operated relief valves (PORVs) reclose, and the reactor coolant pump (RCP) seals remain intact (at least for some time). Thus, unless another plant-specific consideration is important, it seems that the battery life or behavior of the RCP seals may be the functional condition that determines the system time window ($T_{SW}$) for this scenario.

Section 3.5.2.3 indicates that the success criteria for this analysis require that personnel must start the pre-connected FLEX diesel generators, synchronize them, and re-energize the necessary loads before the need to declare an extended loss of AC power (ELAP) condition occurs. The assumptions indicate that the ELAP declaration should be made at time t = 1 hour. Thus, for this analysis, regardless of the actual battery life or other conditions that may affect the functional time window, it is apparent that $T_{avail}$ = 1 hour.

Provided that no other plant responses impose a shorter functional constraint, the ELAP declaration time seems reasonable as the basis for $T_{avail}$. Declaration of the ELAP condition will probably initiate the shedding of several DC loads. Those loads may affect subsequent progression of the scenario or information that is available to plant personnel. Furthermore, the FLEX Support Guidelines (FSGs) that are implemented after the ELAP condition is declared may align the FLEX diesel generators differently from the configuration in this scenario.

**Estimation of $T_{reqd}$**

The assumptions indicate that a designated reactor operator (RO) is responsible for implementing the contingency plan to use the FLEX diesel generators. The designated RO is supposed to implement the plan in parallel with the other Main Control Room (MCR) operators' actions that are specified in the emergency operating procedures (EOPs).

It is noted that the RO dispatches an auxiliary operator (AO) to perform the needed actions. However, it is not evident whether that decision and command are made prior to consultation with supervisory personnel. The assumptions note that the shift manager (SM) arrives in the MCR at time t = 5 minutes, and the shift technical advisor (STA) arrives at time t = 10 minutes. The scenario timeline in Section 3.5.2.4 indicates that the AO is dispatched at time t = 5-8 minutes.

From the available information, it is apparent that all of the actions to start the FLEX diesel generators, synchronize them, and re-energize the needed plant loads (i.e., the implementation part of $T_{reqd}$) are performed by a single AO. The analysis assumes that these actions are completed within 30 minutes after the AO is dispatched, without any estimate of the uncertainty

in that time. The scenario timeline in Section 3.5.2.4 indicates that the actions are completed at time t = 38-40 minutes.

Based on the available information, it is not possible to quantify the scenario timing contribution ($P_t$) to the overall HEP for the actions to provide alternative power from the FLEX diesel generators, or to justify a conclusion why that contribution is necessarily negligibly small. Furthermore, the analysis documentation does not discuss how the project team or the individual analysts considered this element of the IDHEAS methodology.

***JWS Note:*** Section D.3 of Appendix D does not provide any additional information about the time needed to perform these actions.

Is the decision to implement the contingency plan made by the SM, or is it made by the RO without consultation with supervisory personnel?

What is the uncertainty in the estimated time for the decision to implement the contingency plan?

Are all of the actions to start the FLEX diesel generators, synchronize them, and re-energize the necessary loads performed by a single AO?

What is the sequence of electrical breaker operations, startup, and loading of the FLEX diesel generators?

In particular, are some breaker manipulations needed both before and after the diesel generators are started and synchronized?

Where are the relevant circuit breakers located (i.e., with respect to the FLEX diesel generator pad)?

What is the technical basis for the assumption that all of these actions (i.e., startup of the diesel generators, synchronization, and all necessary circuit breaker manipulations) can be completed within 30 minutes after the AO is dispatched?

What is the uncertainty in that estimated time?

How does the analysis of this scenario account for the HEP contribution from $P_t$?

What is the technical justification for a conclusion that $P_t$ is negligibly small?

**41. Section 3.5.2.3, HFEs for Non-FLEX Scenario – SBO with One EDG Out for Maintenance; Appendix D, Section D.7, Additional Notes Made During the Workshop**

Section 3.5.2.3 notes that:

> "The success criteria for this HFE for operators to put the FLEX Plus DGs into successful operation before ELAP would need to be declared."

Footnote 43 in Section 3.5.2.3 indicates that:

> "We decided to ***eliminate 'adding loads'*** to our discussions because we had inadequate information on the procedure guidance for this and how this would be implemented (including what steps would be taken by the AO and what the MCR operators would need to do)." [emphasis added]

Section D.7 of Appendix D indicates that the project team's decision to omit the task of "adding loads" was made during the workshop, and that it was prompted by questions from the analysts.

The functional success criteria for the human failure event (HFE) that is evaluated in this scenario require that personnel must start the pre-staged FLEX diesel generators, synchronize them, and re-energize the necessary plant loads before the extended loss of AC power (ELAP) condition is declared at time t = 1 hour. An assumption in Section 3.5.2.2 indicates that the actions to implement the contingency plan "include several breaker manipulations and electrical connections, in addition to start of the FLEX DGs".

The immediately preceding comment addresses evaluation of the scenario timing and associated uncertainties.

It is evident that the actions to connect the necessary loads, and perhaps additional preparatory electrical alignments, are integral tasks for the use of the FLEX diesel generators to achieve the desired functional success criteria for this scenario. Therefore, a complete human reliability analysis (HRA) must quantify the contribution from those tasks to the overall human error probability (HEP) for this HFE. The highlighted assumption clearly documents the fact that this analysis is not complete.

However, more importantly, this study is intended to demonstrate how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. Therefore, this example should demonstrate how the IDHEAS methodology is used to systematically evaluate integrated personnel performance in the context of this scenario. The example should not selectively exclude actions that are essential to achieve the functional success criteria, simply because not enough information is available to evaluate those actions. In this situation, analysts should: (1) find the relevant plant-specific information, (2) use whatever information is available to make appropriate assumptions, clearly document those assumptions, and document the associated uncertainties, or (3) assign an HEP of 1.0, pending availability of the needed information.

***JWS Note:*** Footnote 42 in Section 3.5.2.2 and Footnote 68 in Section D.1.3 of Appendix D seem to indicate that information about specific steps to implement the contingency plan is available for the reference plant.

***JWS Note:*** Section D.2.2 of Appendix D indicates that one critical task for the HFE "Operator fails to properly align and manually start FLEX DGs" is "Designated AO fails to properly align breakers and make other electrical connections".

***JWS Note:*** The summary of results in Table 6-5b and the discussion of that analysis in Section 6.3.3 also indicate that the analysts evaluated only the actions to connect and start the diesel generator (i.e., unloaded) during the FLEX scenario. Footnote 47 in Section 6.3.3 notes that "Two HRA analysts also addressed FLEX DG 'load' but those results are not reported here".

Omission of the analysis of critical tasks that are needed to achieve the functional success criteria is contrary to the IDHEAS methodology and the guidance in the IDHEAS-ECA

application. The implication that these tasks are not an integral part of the HFE and that they can be excluded from the analysis is completely inappropriate for an example of "NRC-approved" guidance for the use of the IDHEAS methodology.

The HRA for this FLEX function is not complete without the analysis of these essential actions.

What is the intended use and interpretation of the results from this analysis?

Why is this incomplete analysis used to illustrate an example of how the IDHEAS methodology and guidance supports a systematic, integrated assessment of personnel performance?

**42. Section 5.4, Summary of Workshop, Editorial Comment**

The last bullet item in this section repeats the fourth bullet item about the FLEX experts' input.

**43. Section 6.1, High-Level Description of IDHEAS-ECA Guidance and Software Tool, Editorial Comments**

This section notes that:

> "The IDHEAS-ECA HRA method [1] represents human actions in a PRA (i.e., human failure events (HFE)) using five ***macro cognitive*** functions: *detection, understanding, decisionmaking,* ***action*** *and* ***inter team*** *coordination.*" [non-bold italics in original, emphasis added]

The IDHEAS general methodology and the guidance in the IDHEAS-ECA report use "action execution" as the label for the fourth macrocognitive function. There is also no space in "macrocognitive" or in the label for "interteam coordination". This report should use the same terminology.

Table 6-1 should use the actual titles for each macrocognitive function (or cognitive failure mode), not truncated or approximate names.

The last paragraph uses the terms "cognitive failure mechanism" and "macro cognitive mechanism". The title for Table 6-1 also contains the term "macro cognitive mechanisms". Those terms are not used in the IDHEAS vernacular. In the context of this discussion and Table 6-1, I think that the applicable term is "cognitive failure mode".

This section also notes that:

> "***Within IDHEAS-ECA***, the PIFs and attributes are provided in a drop-down list with associated boxes for the user to select." [emphasis added]

I think that it is extremely important to clearly distinguish between the IDHEAS-ECA methodology and guidance, and the IDHEAS-ECA software tool. The software tool is not the methodology, and this report should not imply that it is. The drop-down list and boxes are elements of the IDHEAS-ECA software tool, not the methodology.

**44. Section 6.1, High-Level Description of IDHEAS-ECA Guidance and Software Tool**

This summary mentions the notion of critical tasks only in the following sentence.

"The attributes describe the way the PIFs represent a challenge to macro cognitive functions for a critical task, thereby increasing the likelihood of error in the affected macro cognitive function(s)."

I think that the summary should briefly, but explicitly, address the concept of critical tasks and how they fit into the hierarchy of the IDHEAS methodology. That concept is important for a high-level understanding of the process that analysts use to decompose and evaluate each human failure event (HFE). It is a fundamental element of the IDHEAS general methodology, the IDHEAS-ECA guidance, and the IDHEAS-ECA software tool as described in the current IDHEAS-ECA report.

In practice, analysts first identify the critical tasks that are needed to accomplish each modeled action. A particular HFE may involve one or more critical tasks. The analysts next select the applicable cognitive failure modes (CFMs) for each task. They then assess the relevant scenario-specific performance-influencing factor (PIF) attributes for each CFM.

***JWS Note:*** Appendix D in the current IDHEAS-ECA report seems to indicate that the software tool has a limit of three critical tasks per HFE.

Why does this high-level summary not discuss the notion of critical tasks?

**45. Section 6.2, High-Level Description of IDHEAS-ECA Results, Editorial Comment**

This section notes that:

"In contrast, ***the only HFE was quantified*** for each of the two non-FLEX scenarios." [emphasis added]

The intent of this sentence is to note that only one human failure event (HFE) was quantified for each of the non-FLEX scenarios.

**46. Section 6.2, High-Level Description of IDHEAS-ECA Results**

This section notes that:

"Within each table, results are shown for each of the HRA analysts who participated in the NRC's FLEX HRA project. The HRA analysts are identified as 'Subject A,' 'Subject B,' and so on, consistently throughout the results tables."

Section 1.3.2 indicates that six human reliability analysis (HRA) analysts participated in this study (i.e., three NRC analysts, and three industry analysts). Section 6.3, Section 6.4, and Section 6.5 summarize the results from only five analysts.

***JWS Note:*** Slide 8 in the NRC staff's September 23, 2020 presentation to the ACRS Subcommittee on Reliability and Probabilistic Risk Assessment lists six analysts, and it provides their names.

How many HRA analysts actually participated in this study?

If six analysts participated in the study, why are only five analysts' results reported?

**47. Section 6.2, Table 6-2, Roadmap for FLEX Scenario HFE Quantification Results, Editorial Comment**

The FLEX scenario entry in Table 6-2 for the human failure event (HFE) "Fail to deploy FLEX DG" lists what seems to be a single critical task for "Transport DG connect, start, and load DG". The table indicates that the analysis is documented in Table 6-5.

Section 6.3.3 confirms that separate analyses were performed for two critical tasks for this HFE. Critical Task 1 is "Fail to transport". The results for that task are summarized in Table 6-5a. Critical Task 2 is "Fail to connect and start FLEX DG". The results for that task are summarized in Table 6-5b.

I think that Table 6-2 should more clearly indicate that two separate critical tasks were analyzed, and it should list the specific results table for each task (i.e., Table 6-5a and Table 6-5b).

**48. Sections 6.3, 6.4, and 6.5, FLEX HRA Results Using IDHEAS-ECA, General Comments**

Section 6.3, Section 6.4, and Section 6.5 summarize the analysis results for each scenario. The results depend on each analyst's understanding of the scenario, interpretation of each modeled action, identification of the critical tasks that are needed to accomplish that action, selection of the applicable cognitive failure modes (CFMs) for each task, and assessment of the relevant performance-influencing factor (PIF) attributes. I read the tables carefully to understand each analyst's assessments and their justifications. However, I intentionally did not comment or ask any questions about specific elements of any analysis.

An important objective of the IDHEAS methodology is to reduce variability in the human reliability analysis (HRA) results due to differences in how individual analysts understand and interpret the scenario-specific context of each action, and how they use the analysis guidance. In cases where there is substantial analyst-to-analyst variability, the systematic documentation of each analysis is intended to identify the source and reasons for that variability. Despite the fact that there are clear differences in some analysts' assessments in this study, the presentation format in this report provides an excellent demonstration of that key strength of the IDHEAS methodology. For example, in Table 6-3, it is rather easy to understand why the results from Subject B are much different from the other analysts. Similarly, in Table 6-6, each analyst's considerations and the reasons for their different results are readily apparent.

**49. Section 6.3.2, Table 6-3a. Variation #1 on Base Case HFE – Operators Fail to Declare ELAP in FLEX Scenario, Editorial Comment**

The entries in Table 6-3a for Subjects A, B, and C list only the cognitive failure mode (CFM) for Decision Making. The entry for Subject D lists Detection and Decision Making. The entry for Subject E lists Decision Making and Understanding.

Table 6-3 indicates that analysts A, B, C, and E evaluated other CFMs for the base case scenario (e.g., Detection and Understanding, depending on the analyst). The entries in Table 6-3 also indicate that Subject B had special considerations for the performance-influencing factor (PIF) for Task Complexity, and Subject E evaluated effects from the PIF for Multitasking, Interruption, and Distraction.

Based on the results shown in Table 6-3a, it is not apparent how the analysts evaluated the

other CFMs and PIFs for Variation #1. For example, it seems apparent that Subject C and Subject E each evaluated Detection with a "No Impact" condition for this scenario. However, it is not apparent how, or whether, Subject C evaluated the CFM for Understanding, and it is not apparent how, or whether, Subject E evaluated the PIF for Multitasking, Interruption, and Distraction for this scenario.

Table 6-3a should list all CFMs that were evaluated by each analyst for Variation #1 and their associated PIF attribute assessments, so that readers can understand the basis for each revised human error probability (HEP) and can more easily compare the individual analysts' evaluations with those for the base case scenario.

***JWS Note:*** This comment also applies for Table 6-3b.

**50. Section 6.3.2, Table 6-3b. Variation #2 on Base Case HFE – Operators Fail to Declare ELAP in FLEX Scenario**

***JWS Note:*** I am fairly confident that this is an editorial comment. However, I first noticed the difference that is discussed below when I compared the individual analysts' assessments and results. So I kept the technical discussion, in case this is not simply an editorial oversight.

I think that the human error probability (HEP) that is listed in Table 6-3b for Subject D should be 1.6E-2, rather than 1.6E-3. For example, it seems that Subject C and Subject D made the same assessments for Variation #2.

Furthermore, it seems that the HEP shown in Table 6-3b for Subject D should be higher than that shown in Table 6-3a.

For scenario Variation #1, Table 6-3a indicates that Subject D made the following assessments:

- Detection No Impact
- Decision Making Procedures and Guidance (PG2)

The listed HEP for Variation #1 is 1.73E-3.

For scenario Variation #2, Table 6-3b indicates that Subject D made the following assessments:

- Detection No Impact
- Decision Making Procedures and Guidance (PG2), Task Complexity (C32)

The listed HEP for Variation #2 is 1.6E-3. Subject D assessed an additional detrimental performance-influencing factor (PIF) attribute for Variation #2, compared to Variation #1 (i.e., additional Task Complexity). However, the HEP for Variation #2 is slightly lower than the HEP for Variation #1. That does not seem reasonable.

Should the HEP for Subject D for scenario Variation #2 be 1.6E-2, rather than 1.6E-3?

**51. Section 6.3.3, Results for FLEX Scenario: HFE2, HFE3, and HFE4, Editorial Comment**

This section notes that:

> "***Table 7-2*** shows the results for the second human failure event performed per the plant-specific FLEX procedure for FLEX DC load shed." [emphasis added]

These results are shown in Table 6-4.

**52. Section 6.3.3, Table 6-5a. HFE3: Operators Fail to Deploy FLEX DG in FLEX Scenario / Critical Task 1: Fail to Transport**

I do not understand the human error probability (HEP) results for Subject B in Table 6-5a.

Subject A and Subject C made the following assessments:

- Action Scenario Familiarity (**SF3; level 1)

The listed HEP for Subject A and Subject C is 1.0E-3.

Subject B made the following assessments:

- Action Scenario Familiarity (**SF3; level 1), Training and Experience (**TE1; level 1)

The listed HEP for Subject B is 1.0E-3.

Subject B assessed an additional detrimental performance-influencing factor (PIF) attribute (i.e., inadequate training frequency or refreshment). However, the HEP for Subject B is the same as the HEP for Subject A and Subject C. That does not seem reasonable.

Why is the HEP for Subject B in Table 6-5a the same as that for Subject A and Subject C?

**53. Section 6.5, Table 6-8, HFE / Critical Task: Operators Fail to Connect Pre-Staged, FLEX Plus DGs to Energize Plant Safety Bus in Non-FLEX, SBO Scenario, Editorial Comments**

The entries in Table 6-8 contain the analysts' initials. They should be removed.

The human error probability (HEP) listed for Subject A should be 3.13E-3, rather than 3.13E03.

The Justification notes for Subject B indicate that:

> "Removing PG3, HEP ***increases*** to 1.36E-2. This was a variation captured from Subject B." [emphasis added]

I think that should be "decreases".

**54. Section 6.6, Conclusions**

This section notes that:

"Based on the influencing factors and attributes selected, there were only ***slight differences*** in the overall HEP values for ***most HFEs***." [emphasis added]

The following table lists the minimum and maximum human error probabilities (HEPs) for each human failure event (HFE).

| Table | Minimum HEP | Maximum HEP | Ratio |
|---|---|---|---|
| 6-3 | 1.1E-03 | 2.69E-03 * | 2.4 |
| 6-3a | 1.1E-03 | 3.0E-02 | 27.3 |
| 6-3b | 1.6E-02 ** | 1.02E-01 | 6.4 |
| 6-4 | 2.0E-03 | 6.0E-03 | 3.0 |
| 6-5a | 1.0E-03 | 3.0E-03 | 3.0 |
| 6-5b | 1.0E-03 | 1.2E-02 | 12.0 |
| 6-6 | 2.1E-03 | 2.72E-02 | 13.0 |
| 6-7 | 1.69E-03 | 1.59E-02 | 9.4 |
| 6-8 | 1.1E-03 | 2.5E-02 | 22.7 |

* I did not include the estimate from Subject B, which may account for a different intended effect. If that estimate is included, the ratio for this HFE would be approximately 128.

** I assumed that the correct estimate from Subject D is 1.6E-02.

The range in results for three of the nine analyses is less than a factor of 5, and the range for two others is less than a factor of 10. That is generally considered to be rather "good agreement" for about half of the analyses. However, it is not apparent that these results show "only slight differences" for "most HFEs".

***JWS Note:*** This comment also applies to the bullet item in Section 7.1 which notes that "Generally, the HEPs developed by the participating industry and NRC HRA analysts were consistent (within an order of magnitude)".

What is the basis for the assertion that the results from this study show "only slight differences in the overall HEP values for most HFEs"?

**55. Section 6.6, Conclusions, General Comment**

Despite the fact that there are clear differences in some analysts' assessments, I think that the results demonstrate an important strength of the IDHEAS methodology, its structured analysis process, and its systematic documentation. In particular, even at the rather high level of the summaries in this section, it is possible to identify distinct differences in the individual analysts' selections of the applicable cognitive failure modes (CFMs) for each task, and their assessments of the relevant performance-influencing factor (PIF) attributes. In an actual human reliability analysis (HRA), the analysts would need to provide more comprehensive documentation of their assessments and the reasons for their decisions. For example, that documentation would include the reasons why they excluded specific CFMs, and the reasons why they concluded that specific PIFs were either not applicable or were "nominal" for the

scenario conditions. That forensic information would provide additional insights about the breadth and depth of their assessments and the applicability of their estimates.

***JWS Note:*** Experience has also shown that the need to provide those justifications forces the analysts to clarify their thought process, which may further reduce a source of variability in these rather hasty analyses.

Why does this section not discuss this perspective of the results?

**56. Section 7.2, Insights for HRA and PRA Modeling**

The first major insight in this section notes that:

> "However, it is ***likely*** that HRA / PRA analysts would need to confirm that FLEX implementation for another NPP is similar to the two NPPs visited in this project." [emphasis added]

It is absolutely essential that analysts must confirm all elements of the plant-specific FLEX strategies, including equipment, personnel, guidance, and training.

**57. Section 7.2, Insights for HRA and PRA Modeling**

The second major insight in this section notes that:

> "The level of detail in the developed scenarios was ***likely greater than that typical*** of an HRA / PRA. However, this detail was important for the HRA analysts to consider the scenarios as credible." [emphasis added]

All scenarios that are evaluated in a PRA are, or should be, "credible".

The IDHEAS methodology emphasizes the importance of a scenario-focused evaluation of human performance. That focus relies on a description of the evolving scenario that provides analysts with a comprehensive understanding of all factors that affect personnel performance, including the plant-wide damage, scenario timing, possible competing or conflicting priorities, etc. A vital element of that understanding is derived from the scenario narrative, which provides an integrated operational perspective of what has happened, and is happening, in the plant when the desired actions are needed.

This scenario-focused perspective and the need for a more comprehensive evaluation of the scenario context was one of the most important reasons for developing the IDHEAS methodology to rectify identified shortcomings of "typical HRA / PRA" methods.

Several of my comments address details that are either missing or are not fully explained in the three example scenario narratives that were developed for this study. Therefore, it is not apparent that the amount of detail in these narratives is "likely greater" than that which is recommended by the IDHEAS guidance.

What is the basis for this assertion?

How is this assertion consistent with the fundamental scenario-focused perspective of the IDHEAS methodology?

Does the project team for this study believe that an abbreviated scenario narrative is adequate to support a realistic human reliability analysis that is consistent with the IDHEAS methodology?

What is the intended interpretation of this insight for other applications of the IDHEAS methodology?

**58. Section 7.2, Insights for HRA and PRA Modeling**

The second bullet item under the discussion of insights for modeling FLEX scenarios notes that:

> "The timing validations for FLEX implementation may be conservative as compared to the timing information typically used in PRA."

That may certainly be true for specific scenarios that are evaluated in a full-scope PRA. However, depending on the plant-specific assumptions, applied constraints, and defined success criteria for the validation exercises, the timing information from those exercises may also be optimistic for a realistic analysis of many other scenarios.

This comment also applies to the implied universal conservatism of timing information from the multi-unit FLEX validation exercises that are discussed in the third bullet item. In particular, although the project team for this study often states that the PRA analyses are "typically" performed for a single unit, a realistic analysis must account for everything that is happening at the site and how all units and all personnel are affected. Experience has shown that a myopic focus on a single unit can often provide very misleading and optimistic assessments.

**59. Section 7.2, Insights for HRA and PRA Modeling, General Comment**

The discussion of insights for non-FLEX scenarios is very good.

**60. Appendix A, Summary Notes from the Plant Site Visits, General Comment**

I understand that the material in this appendix compiles and summarizes the project team's notes from each site visit. I read this material carefully to understand the technical details, plant operational information, and various perspectives. However, I intentionally did not comment or ask any questions about specific items.

**61. Appendix B, Section B.2.1, PRA Modeling, Editorial Comment**

This section indicates that the event tree is shown in Figure A-1. It is Figure B-1.

**62. Appendix B, Section B.2.2, HRA Modeling**

The discussion of "Operators fail to deploy FLEX diesel generator" notes that:

> "Deploying the FLEX DG involves: 1) transport of the DG from the FLEX Building to the appropriate laydown area via FSG-10, 2) AC electrical alignment via FSG-13, and 3) installation, starting, and ***adding of loads***....In all cases, field operators are responsible for doing electrical alignment, then installing, starting and ***loading***. Electrical connections are standardized for FLEX and the FLEX DG is ***supposed to be easy to operate (e.g., push button)***, by design." [emphasis added]

It may be rather easy to connect the generator cables to the electrical panel and start the diesel engine. However, the timing and sequence of actions that are needed to correctly add loads and to avoid overloading the generator, tripping, or damaging the unit may not be as easy or well-trained. I do not know how the generator loading sequence is accomplished in practice, who controls the loading, or what specific guidance is available for that process. Some of the experts' discussions in their Justifications for the estimated human error probabilities (HEPs) in Section 3.1.3 of Volume 1 of this study indicate that it may be more difficult to control the initial and subsequent loading of a small generator and prevent it from tripping, compared to a large generator that has more reserve capacity.

***JWS Note:*** The summary of results for the FLEX scenario in Table 6-5b and the discussion of that analysis in Section 6.3.3 indicate that the analysts evaluated only the actions to connect and start the diesel generator (i.e., unloaded). Footnote 47 in Section 6.3.3 notes that "Two HRA analysts also addressed FLEX DG 'load' but those results are not reported here". Thus, it is apparent that the study results do not account for the actions to load the generator. I did not re-write this comment or questions after I read Section 6.3.3, because it is important that the report should clearly document what was evaluated and what was not evaluated, and it should document the reasons why relevant tasks were omitted from the scope of this study.

Did the human failure event (HFE) description that was used by the analysts explicitly indicate that the tasks for this HFE include controlled loading of the generator?

If not, why not?

If so, is there evidence that the analysts' evaluations accounted for that task?

**63. Appendix B, Section B.4.2, FLEX Scenario Script, General Comment**

The scenario script in Table B-1 provides very useful information about the scenario evolution, the primary issues that are related directly to the actions that are evaluated in this study, the timing of specific actions, personnel who perform the actions, and relevant procedural guidance. However, as noted in a preceding comment, it does not describe other coincident activities that may be needed to cope with the site-wide damage from the earthquake.

**64. Appendix B, Section B.4.3, HFE Timing Information and Plant-Specific FLEX Final Integrated Plan, Editorial Comment**

The introduction to this section notes that:

> "Standard HRA terminology for timing parameters (see, for example, ***Section 4.6.2 in NUREG-1921*** [ref]) is used here, e.g.," [emphasis added]

This study demonstrates how the guidance in the IDHEAS-ECA application is used to evaluate personnel actions to deploy, connect, and operate FLEX equipment. Therefore, the emphasis in this report should remain focused on the IDHEAS methodology. Section 5.3 in the current version of NUREG-2198 contains an improved discussion of a timeline, and it defines the time intervals that are used in the IDHEAS methodology. This introduction to the timeline terminology should refer analysts to the guidance in NUREG-2198.

***JWS Note:*** The timeline and definitions in Section 5.3 of the current version of NUREG-2198

are the same as those in Section 4.6.2 of NUREG-1921.

**65. Appendix B, Section B.4.3, HFE Timing Information and Plant-Specific FLEX Final Integrated Plan, General Comment**

The discussion of "Perform debris removal" notes that:

> "The plant's validation plan does not identify this action as time sensitive. In addition, the event timeline in the plant's validation plan shows that this is action is not time constrained."

The discussion of "Deploy FLEX diesel generators" notes that:

> "This action is identified as a Level A TSA in the plant's validation plan. For Level A TSAs, a simulator or timed walkthrough is performed to develop results."

***JWS Note:*** TSA = Time-Sensitive Action

This dichotomy seems extremely odd, considering the fact that the debris must be cleared before the diesel generator can be moved to its connection location. However, since this is apparently a summary of the plant's actual FLEX validation plan and assumptions, I will only make this observation without asking about its rationale or implications.

**66. Appendix C, Section C.4.1, Non-FLEX Scenario Timeline for Case #1: AFW Pump Trips at t=0, General Comment**

The Note in this section indicates that:

> "Per the event tree shown in Figure C-1, this case is typically not addressed (i.e., if F&B is successful, the subsequent event tree headings and end states do not address restoration of FW). Consequently, it is not immediately apparent what PRA credit could be obtained by using the FLEX pump if typical PRA modeling is used."

If secondary heat removal is restored before the RSWT is drained, it is not necessary to align high pressure recirculation flow from the containment sump (i.e., Top Event HPR in Figure C-1). Thus, restoration of steam generator makeup from the FLEX pump after initiation of feed and bleed cooling would have a measureable effect on the core damage frequency.

**67. Appendix C, Section C.4.2, Non-FLEX Scenario Timeline for Case #2: AFW Fails to Run after 1 Hour of Operation, General Comments**

The Note in this section indicates that:

> "This case can be addressed in PRA by using modified fault trees (FTs) such as that shown in Figures 2 and 3."

***Editorial Comment:*** The modified fault tree is shown in Figure C-2.

A preceding comment on Section 3.5.1.2 addresses whether it is necessary to actively depressurize a steam generator to achieve makeup flow from the FLEX pump. If that task is needed, the operator action and the associated hardware (e.g., steam generator atmospheric relief valves, including their support system dependencies) should also be shown as separate

basic events under Gate AFW-FLEX in Figure C-2.

**68. Appendix C, Section C.4.3, Non-FLEX Scenario – Potential Variations, General Comment**

The discussion of Variation #1 in this section notes that if the FLEX pump is pre-staged:

> "This potentially changes the task complexity (see discussion below) to ***NOT complex*** because SM / operators would be trained that there is ***no consequence*** to starting the process of deploying the FLEX pump. If normal AFW is restored before the FLEX pump is operated, there are no irreversible steps to overcome." [emphasis added]

A preceding comment on Section 3.5.1.2 addresses whether it is necessary to actively depressurize a steam generator to achieve makeup flow from the FLEX pump. If that task is necessary, it should be noted in this discussion. It seems that the need to actively depressurize a steam generator would also affect the analysts' assessment of the overall complexity of the tasks that are needed to establish makeup flow from the FLEX pump during this scenario variant.

**69. Appendix C, Section C.5, Non-FLEX Scenario and HRA Influencing Factors, General Comment**

This section summarizes the project team's assessments of the attributes for each relevant performance-influencing factor (PIF) during this scenario. Although I might disagree with some specific assessments, my judgment is neither more relevant nor necessarily better justified technically than the analysts'. Therefore, my comments address situations that involve analyst judgment only when I could not understand the rationale for a particular decision, or when the judgment does not seem to be consistent with the general IDHEAS guidance.

**70. Appendix C, Section C.5, Non-FLEX Scenario and HRA Influencing Factors**

The first paragraph under "HFE: Operators fail to deploy FLEX pump (cognitive contribution)" notes that:

> "Similarly, ***MCR design features*** important to this action are the same as those considered in ***typical HRAs*** (and there are no concerns with respect to human-machine interface, no requirements for equipment, no fitness concerns)." [emphasis added]

This paragraph also notes that:

> "Communications and command and control are unchanged from that ***typically addressed*** by HRA / PRA (i.e., there is no need to explicitly model these PIFs)." [emphasis added]

It is not appropriate for "NRC-approved" guidance to imply that conclusions about the effects from the performance-influencing factors (PIFs) for Human-Machine Interface, Communications, and Teamwork and Command and Control are "nominal" for this scenario, simply because this action is performed in the Main Control Room (MCR) and these PIFs are "typically addressed" in human reliability analyses (HRAs). These "generic" inferences are not consistent with a systematic, objective, scenario-specific evaluation, according to the IDHEAS methodology.

For example, the first excerpt seems to imply that the analysts concluded that the PIF for

Human-Machine Interface is "nominal" during this scenario, because that situation applies for "typical HRAs". A similar inference applies for the second excerpt.

Of course, it is perfectly appropriate for the project team to conclude that the effects from these PIFs are "nominal" in the context of this specific scenario, based on their examinations of the information that is needed to support this decision, how the human-machine interface displays that information, and how the decision is affected by communications among the control room crew, its command structure, and teamwork. That would demonstrate a plant-specific and scenario-specific assessment, rather than a generic inference.

***JWS Note:*** Section 3.1.1 in Volume 1 of this study report defines four general attribute states for each PIF: "nominal", "low impact", "moderate impact", and "high impact". My use of "nominal" in this comment is intended to be consistent with that taxonomy.

***JWS Note:*** This comment also applies to a similar discussion and references to "typical" assumptions in the first paragraph under "Post-initiator: Operator fails to dispatch AO to perform steps for starting FLEX DGs[2]" in Section D.6.

Why does this "NRC-approved" guidance imply that these assessments are based on a conclusion that the effects from these PIFs are usually "nominal" for every MCR action that is evaluated in "typical HRAs"?

**71. Appendix C, Section C.5, Non-FLEX Scenario and HRA Influencing Factors, Scenario Familiarity**

The assessment of the performance-influencing factor (PIF) for Scenario Familiarity is focused entirely on the scope and frequency of training. The discussion is primarily relevant to the PIF for Training and Experience, and it is essentially repeated in the assessment of that PIF. This assessment does not address the intended considerations for the PIF for Scenario Familiarity, as that PIF is defined and used in the IDHEAS methodology.

***JWS Note:*** For reference, the basic elements and attributes of the PIF for Scenario Familiarity are summarized in Table 3-15 in the current version of NUREG-2198.

Training on similar scenarios is an important consideration that affects human performance. However, the PIF for Scenario Familiarity is intended to measure how scenario-specific differences affect the operators' understanding of the scenario evolution (i.e., their mental model of expected plant behavior and the most appropriate response strategy). For example, in this particular scenario, the simultaneous loss of all four condensate pumps may be quite unusual, and it may not be consistent with the operators' expectations for the most common conditions that cause a loss of all main feedwater. Thus, they may spend more effort and time to diagnose the cause of the problem and to adapt their responses to this particular situation.

From the perspective of the operators' familiarity with this scenario, if the condensate pumps are permanently damaged, it is pointless to try to restore high pressure main feedwater flow, and it is pointless to depressurize the steam generators in an effort to supply alternative makeup flow from the condensate system. The PRA model "knows" those options cannot work. However, the operators do not have that benefit. Thus, in practice, they may spend more time and effort to understand why those options will not work during this scenario, compared to a more familiar scenario when the main feedwater pumps tripped.

Why does the assessment of this PIF focus exclusively on the scope and frequency of training, rather than attributes of the PIF for Scenario Familiarity, as that PIF is defined and used in the IDHEAS methodology?

**72. Appendix C, Section C.5, Non-FLEX Scenario and HRA Influencing Factors, Time Availability / Urgency**

The immediately preceding comment addresses the focus on training in the assessment of the performance-influencing factor (PIF) for Scenario Familiarity. The assessment of this PIF similarly focuses on training and procedures.

The title for this PIF does not match any of the 20 PIFs that are described in the IDHEAS general methodology in NUREG-2198 or the 15 PIFs that are used in the current version of the IDHEAS-ECA guidance. Furthermore, the PIF list in this section contains the IDHEAS PIF for Time Pressure and Stress, so this PIF certainly does not account for those effects. Thus, without more information about this PIF, it is not appropriate to speculate about how the analysts interpreted its intent and used it in this study.

What is the functional definition of this PIF, as it is used in this study?

How is this PIF related to the 20 PIFs that are described in the IDHEAS methodology?

Why does the assessment of this PIF focus primarily on training and procedures?

**73. Appendix C, Section C.5, Non-FLEX Scenario and HRA Influencing Factors, Time Pressure and Stress**

The general assessments in the first paragraph under "HFE: Operators fail to deploy FLEX pump (cognitive contribution)" and the more detailed assessments of individual performance-influencing factors (PIFs) do not address the analysts' consideration of the PIF for Time Pressure and Stress.

Why does this section not document the analysts' assessment the PIF for Time Pressure and Stress, as that PIF is defined and used in the IDHEAS methodology?

**74. Appendix C, Section C.6.2 - Non-FLEX Scenario – Procedure Path for Case #2, General Comments**

At the end of this section, there is a brief discussion of "Execution Contribution – Operators fails to deploy FLEX pump".

Preceding comments address the assertion that the actions needed to achieve successful alternative steam generator makeup from the FLEX pump during this scenario (i.e., deployment of the pump, connection of the pump, active reduction of steam generator pressure, and operation of the pump) are "identical to that for implementing FLEX strategies in response to an external event". They are not.

A preceding comment on Section 2.6.3.4 addresses the assertion that "FLEX equipment is simpler to operator than other (e.g., nuclear-grade) equipment".

The third bullet item in this discussion notes that:

"FLEX connections have been standardized, US NPP industry-wide. Also, color-coding is used for FLEX DG connections to ensure that correct connections are made."

Color-coding of the FLEX diesel generator electrical connections is completely irrelevant to the use of a FLEX pump in this scenario.

**75. Appendix D, Section D.1.1, Background**

This section notes that:

"Details of the pre-staging and associated contingency plan are given below (***after the References section***)." [emphasis added]

There is no section after Section D.8, References. Unless additional pertinent details are available, I think that Section D.1.3 contains this information.

Is this simply an editorial oversight?

Is more detailed pertinent information available about the diesel generator pre-staging and contingency plan?

If so, why is it not included in this appendix?

**76. Appendix D, Section D.1.3, FLEX Equipment Pre-Staging and Contingency Plan, Editorial Comment**

The summary in this section indicates that the contingency plan is implemented by a reactor operator (RO) and an auxiliary operator (AO). Footnote 66 indicates that there is apparently an important distinction between "designated" and "dedicated" personnel. The discussion and the bullet items in this section do not seem to use the "designated" and "dedicated" labels consistently for either the RO or the AO.

Based on a quick word search, it seems that most of Appendix D refers to both the RO and the AO as "designated" operators. Section D.5 uses the "dedicated" label for the RO. Section D.6 uses the "dedicated" label for the RO and the AO. The "dedicated" RO also appears in Section E.1.1 of Appendix E. I do not know if I missed any others.

***JWS Note:*** The summary in Section 3.5.2.2 and the scenario timeline in Section 3.5.2.4 consistently label both the RO and the AO as "designated" operators.

***JWS Note:*** I would not normally make this type of comment, but the footnote indicates that the labels must be important to someone in some administrative or regulatory context.

**77. Appendix D, Section D.2.1, PRA Modeling, Editorial Comment**

The last sentence in this section notes that:

"However, for this specific NPP, the FLEX DGs are not the same FLEX DGs used in a FLEX event."

I think that I understand the intent of this sentence, but it contains too many "FLEX DGs".

The summary of this scenario often refers to the pre-staged 4.16 kV diesel generators as "FLEX Plus" diesel generators (e.g., as distinguished by Footnote 35 in Section 3.5.2.2). Until I read this section, I thought that this plant might have only "FLEX Plus" diesel generators. However, this sentence seems to imply that the plant also has some other "normal FLEX" diesel generators, which are apparently used differently from the 4.16 kV "FLEX Plus" diesel generators. For example, the "normal FLEX" diesel generators might be lower voltage units.

That seems odd, but I am certainly not familiar with the complement of FLEX equipment at every plant, or how specific components are used according to the plant-specific FLEX Support Guidelines (FSGs). In any event, if this plant actually has different portable diesel generators for different purposes, this summary should at least clearly distinguish between the pre-staged "FLEX Plus" diesel generators and the other FLEX diesel generators, so readers better understand the intent of this discussion.

***JWS Note:*** Section D.7 confirms that this plant has both "SAFER-like" and "typical FLEX" portable diesel generators.

Can this discussion be clarified to avoid confusion about the "FLEX DGs"?

**78. Appendix D, Section D.2.2, Operator Actions and Human Failure Events; Section D.3, Key Modeling Assumptions**

The first sentence in Section D.2.2 notes that:

> "The following additional basic events are needed to credit the FLEX DGs (***and parallel events for the FLEX pump***):" [emphasis added]

The last bullet item in Section D.3 notes that:

> "Operator training is on a 4-year cycle for FLEX. ***Starting pumps and noting flow*** is part of training. Also, AOs tour FLEX buildings and talk through all of the FLEX equipment, including associated cables and ***hoses***." [emphasis added]

The summary of this scenario does not mention the need for a FLEX pump.

Is it actually necessary to use a FLEX pump to achieve the functional success criteria for this scenario (e.g., to maintain long-term operation of the diesel generators)?

If so, why does the scenario summary not clearly identify that functional need for a FLEX pump?

Why does Section D.2.2 mention the need for basic events for actions to deploy, connect, and operate a FLEX pump?

Why does the summary of training in Section D.3 mention the pumps and hoses?

**79. Appendix D, Section D.2.2, Operator Actions and Human Failure Events; Section D.3, Key Modeling Assumptions; Section D.6, Preliminary Assessment of HRA Influencing Factors**

Three items in Section D.2.2 seem to refer to Footnote 2 (e.g., Item 3 in the first list, Item 2 and Item 3 in the second list). The third-from-last bullet item in Section D.3 contains an explicit reference to "(See Footnote 2)". The subheadings for the two post-initiator actions and three bullet items under the discussion of the second post-initiator action in Section D.6 seem to refer to Footnote 2.

Footnote 2 in the Executive Summary clearly does not apply for this appendix.

What is the missing Footnote 2?

**80. Appendix D, Section D.2.2, Operator Actions and Human Failure Events**

Item 4 and Item 5 in the list of basic events identify hardware failures of the diesel generators. Of course, the actual PRA model should contain basic events for all three diesel generators.

An assumption in Section 3.5.2.2 indicates that the actions to implement the contingency plan "include several breaker manipulations and electrical connections, in addition to start of the FLEX DGs". Footnote 69 in this section also mentions that the contingency plan instructions include "breaker manipulations" and "electrical connections".

Why does this summary not identify the need for basic events to account for hardware failures of the circuit breakers that are operated for this alignment?

**81. Appendix D, Section D.3, Key Modeling Assumptions**

The introduction to Section D.2 provides a high-level overview of the plant status before the initiating event occurs and during the early progression of this scenario. In particular, it notes that the turbine-driven auxiliary feedwater (AFW) pump starts successfully, the pressurizer power-operated relief valves (PORVs) reclose, and the reactor coolant pump (RCP) seals remain intact (at least for some time). This information is important for analysts to understand the system context of this scenario.

An assumption in Section 3.5.2.2 indicates that:

> "This NPP has a ***very long*** battery life." [emphasis added]

Section D.3 does not mention this assumption, and it does not provide any information about the battery life. The battery life is an important part of the system context for this scenario. It is very likely the reason why the extended loss of AC power (ELAP) condition must be declared by time t = 1 hour.

Why does this section not discuss the project team's assumptions about the battery life?

What is the battery life for this plant?

**82. Appendix D, Section D.6, Preliminary Assessment of HRA Influencing Factors, General Comment**

This section summarizes the project team's assessments of the attributes for each relevant performance-influencing factor (PIF) during this scenario. Although I might disagree with some specific assessments, my judgment is neither more relevant nor necessarily better justified technically than the analysts'. Therefore, my comments address situations that involve analyst judgment only when I could not understand the rationale for a particular decision, or when the judgment does not seem to be consistent with the general IDHEAS guidance.

**83. Appendix D, Section D.6, Preliminary Assessment of HRA Influencing Factors**

Section B.5.1 of Appendix B summarizes the project team's initial assessments of the environmental context, system context, personnel context, and task context for the FLEX scenario, in accordance with the IDHEAS-ECA guidance. Section C.5 of Appendix C summarizes the project team's initial assessments of the 14 performance-influencing factors (PIFs) that are used in this study for the loss of feedwater scenario.

This section briefly discusses the project team's conclusions about which specific PIFs are relevant for each of the modeled actions and thus merit further evaluation. However, it does not contain an initial assessment of the attributes for those PIFs, like that provided in Section C.5 of Appendix C.

***JWS Note:*** A preceding comment on Section C.5 of Appendix C addresses the inappropriate inference that "typical" assumptions about the PIFs for actions that are performed in the Main Control Room (MCR) can be used as a basis for asserting that several of the PIF attributes for the designated reactor operator's (RO's) response are "nominal" in this scenario.

Why does this section not summarize the project team's initial assessments of the relevant PIF attributes for each action in this scenario (i.e., like those in Section C.5 of Appendix C)?

**84. Appendix E, Variations on Scenarios, General Comment**

I understand that the material in this appendix compiles and summarizes the project team's notes from discussions that were held during the site visits and the workshop. I read this material carefully to understand the technical details, plant operational information, and various perspectives. However, I intentionally did not comment or ask any questions about specific items.

**85. Appendix E, Section E.2, Discussion of FLEX Scenario Variations Between NPPs, Editorial Comment**

The third-from-last major bullet item in this section notes that:

> "All ***PWRs*** have a deviation document that identifies how that NPP has deviated from the standard FSGs." [emphasis added]

This section summarizes discussions that were held during the BWR site visit. Almost all of the bullet items seem to address generic considerations that may apply for BWRs or PWRs. The second-to-last bullet item clearly addresses a BWR issue. This is the only bullet item that explicitly mentions PWRs.

Is this reference to PWRs correct?

**86. Appendix E, Section E.3, Table E-1, HRA for FLEX Project: Organizing Variations within Scenarios, Editorial Comment**

Table E-1 contains references to Footnotes 36, 38, 39, and 41.

Those footnotes in Section 3.5.2.2 clearly do not apply for this table.

What are the missing footnotes?