Simplified Human Reliability Analysis Process for Emergency Mitigation Equipment (EME) Deployment

Don E. MacLeod[a*], Gareth W. Parry[a], Barry D. Sloane[a], Paul Lawrence[b], Eliseo M. Chan[c], and Alexander V. Trifanov[d]

[a] ERIN Engineering and Research, Inc., Walnut Creek, USA
[b] Ontario Power Generation, Inc., Pickering, Canada
[c] Bruce Power, Toronto, Canada
[d] Kinectrics, Inc., Pickering, Canada

Abstract: For a variety of different reasons, it is becoming more common for nuclear power plants to incorporate the use of portable equipment, for example, mobile diesel pumps or power generators, in their accident mitigation strategies. In order for the Probabilistic Risk Assessment (PRA) to reflect the as-built, as-operated plant, it is necessary to include these capabilities in the model. However, current Human Reliability Analysis (HRA) methodologies that are commonly used in the nuclear power industry are not designed to accommodate the evaluation of some of the tasks associated with the use of portable equipment, such as retrieving equipment and making temporary power and pipe connections.

This paper proposes a method for estimating the component of the human error probability (HEP) associated with the deployment of portable equipment. The other components of the HEP, such as the failure to identify the need to initiate portable equipment deployment, can be addressed with existing methodologies and are not addressed by this approach. This approach is intended for application to a variety of hazard risk assessments, including internal events, internal flooding, high winds, internal fires, external flooding, and seismic events.

Keywords: HRA, Portable, Temporary, External Events.

1. INTRODUCTION

For a variety of different reasons, it is becoming more common for nuclear power plants to incorporate the use of portable equipment (referred to in this paper as Emergency Mitigation Equipment (EME)) in their accident mitigation strategies. In order for the Probabilistic Risk Assessment (PRA) to reflect the as-built, as-operated plant, it is necessary to include these capabilities in the model. Current Human Reliability Analysis (HRA) methodologies that are commonly used in the nuclear power industry are not designed to accommodate the evaluation of some of the tasks associated with the use of such portable equipment, such as retrieving equipment and making temporary power and pipe connections. Some methodologies, such as ATHEANA [1] and FLIM [2], are, in principle, capable of assessing these types of failures, but require an extensive coordination of resources, rely heavily on expert judgment, and have limited exposure in the industry.

This paper proposes a method for estimating the human failure probability associated with deploying EME. This approach is intended for application to a variety of hazard risk assessments, specifically internal events, internal flooding, high winds, internal fires, external flooding, and seismic events. Further, since the approach is intended for application to a range of methods of EME deployment, it is generic in nature and therefore tends to be conservative. While this methodology was developed to address the conditions that were anticipated to be the most relevant to EME deployment, application of the methodology has thus far been limited to work performed by Ontario Power Generation and Bruce Power to support the modeling of EME in their PRAs. As with other developing PRA techniques, it is expected that experience with the process will identify areas for further refinement and enhancement.

[*] demacleod@erineng.com

2 SCOPE

The intent of this paper is to document a methodology for evaluating the failure probability associated with the retrieval, transportation and installation of the EME, referred to in this paper as EME deployment. For this methodology, “installation” is considered to include tasks such as making temporary piping and power connections, loading a portable generator, and/or pressurizing a water system header with a portable pump, although it is expected that the specific tasks may be different for each site. The contributions associated with determining the need to initiate the EME deployment (i.e., the diagnosis and decision making) and with operating the equipment, once deployed, are not part of this methodology. The use of this methodology is only proposed for cases where there is clear guidance provided by abnormal incidents manuals (AIMs), emergency mitigating equipment guides (EMEGs), emergency operating procedures (EOPs) (or equivalent guidance) to deploy EME and that these decisions are made within the main control room or secondary control area by authorized staff (e.g., authorized nuclear operators, control room shift supervisors, shift managers). Further, the actions to initiate operation of the EME equipment, once deployed, are performed entirely within the control room or secondary control areas or using field actions required to initiate EME (e.g., opening manual valves), and these can be addressed within the scope of the hazard-specific modelling of operator response by nominal plant HRA methods. Reliability of EME hardware is also not addressed in this paper.

3. METHODOLOGY

This methodology is a simplified process that applies adjustment factors to represent the impact of performance shaping factors (PSFs) on a hazard-specific basis on a base human error probability (HEP). The impacts of each PSF are tracked in an HRA decision tree and the combined impact of all decision branches, which characterize the implementation conditions for the site being evaluated, determine the scenario-specific HEP. An example decision tree is described in Section 5.

In the event that it is necessary to evaluate EME deployment for other types of hazards, additional HRA decision trees can be developed. For consistency in a given PRA model, it is suggested that any additional HRA decision trees be developed in the same manner as those presented in this paper.

3.1. Base HEP

The base HEP is used as the starting point in the EME deployment HRA decision trees. It is considered to represent the failure probability of a deployment activity that:

- Is governed by procedures that provide all of the information required to effectively perform the task. For example,
    - It is assumed that there are step-by-step instructions for the installation tasks, such as making temporary power and piping connections, aligning valves, starting and loading a generator, and/or pressurizing water system header.
    - The level of detail associated with procedures for acquiring and transporting equipment is expected to be lower, but if the EME is loaded on a trailer that can only be towed by a specific set of trucks, the procedure should identify which vehicles are capable of supporting the task.
- The responsible plant personnel have been trained on. Determining the adequacy of training is somewhat subjective, but adequate training could be described as:
    - Having received classroom training on deployment as a prerequisite for being part of the deployment team,
    - Re-performing the training on a periodic basis has been demonstrated to be feasible under nominal conditions. For the internal events analysis, the environmental conditions in which the deployment will occur are likely similar to those

conditions in which the validation exercise was performed. It is possible that other environmental conditions may exist that were not present in the validation exercise, such as:

- Extreme cold weather
- Extreme hot weather
- Heavy rain
- Heavy snow
- Nighttime deployment

However, the base HEP is assumed to account for these factors in that it represents an average over these conditions for internal events. These are underlying random conditions that are not modeled in the PRA. These variations, such as changes in temperature from day to day could have an influence on performance, e.g., performance could degrade if the actions were being taken at very high or very low temperatures. However, since they are random with respect to when the demand could occur, and are not modeled explicitly, the HEP is characterized as being the average HEP over the spectrum of these conditions. Conditions that are correlated with the hazard being evaluated are treated explicitly in the following decision trees.

A failure probability of 1.0E-01 is assigned for this base HEP, which is consistent with a screening HEP from NUREG-1792 [3].

3.1.1 Feasibility for Specific Hazards

While the feasibility of EME deployment has been established for nominal plant conditions, it will be necessary to establish feasibility for each of the hazards in which it is credited. This includes consideration of:

Staffing: Each hazard presents different requirements on the plant and may require the performance of different activities by the available staff. For each case in which EME deployment is credited, it must be confirmed that EME deployment team personnel that are qualified to perform required duties will not be diverted to other tasks such that they would not be available to support EME deployment. Any special fitness requirements for performing deployment tasks, such as operating chainsaws (to facilitate clearing debris for example), should be considered as part of the staffing assessment.

Timing: In order to establish feasibility, it must be demonstrated that the time required to perform the deployment is less than or equal to the time available after allowing for the time to initiate the EME given successful deployment. A separate "time margin" assessment is used as part of this HRA methodology, but it is focused on determining potential credit for the recovery of errors.

Equipment and Location Accessibility: For each hazard in which the EME is credited, it must be established that the EME will not be damaged to the extent it cannot function and that it will be possible to access the equipment, transport it to the deployment area, and that it is possible to work in the deployment area. Events that could prevent this include:

- Failure of the structure(s) that house the EME, for example:
  - Building collapse that damages the EME
  - Building collapse that prevents access to the EME,
  - Partial collapse or other damage, such as door buckling, that prevents access to the EME.

- Failures of structure(s) along the access path between the EME storage location and the point where it is to be deployed, or structural failures of the access paths,
- Obstruction of path due to debris accumulation that is beyond the capability of on-site sources to remove,
- Failures of the structure(s) where the EME is deployed (if applicable).
- Fire in an area where EME deployment activity is required: No credit is taken for EME deployment in fire scenarios where part of the activity must be performed in the same (or very nearby) location as the fire.
- Flooding in an area where EME deployment activity is required: No credit is taken for EME deployment in internal or external flooding scenarios where part of the activity must be performed in a location that is flooded.
    - If a case can be made that the quantity of water in the area would not significantly impact the deployment activity, the HRA analyst may choose to document the issue and credit EME deployment. However, due to the uncertainty in assessing the impact of flood events, it is suggested that EME not be credited when flood conditions exist in the zone where the activity is required.
    - Consideration should be given to scenarios where the EME itself may not be damaged, but access to the EME for refueling is not possible (etc.).
- For external flooding scenarios, determine if the installation of flood barriers would prevent access to equipment or transportation routes.

Safety Limits: No credit should be taken for EME deployment in conditions that exceed any safety limits established for personnel protection by the plant. For example:
No credit should be taken for the EME deployment activity for high wind events which exceed the safety limits established for plant personnel.

Communications: If EME deployment relies on communication between the deployment team and any other group, it must be verified that the communication equipment will be capable of operating in the scenario in which it is used. For example, if the communications equipment requires an antenna that would be failed in certain seismic events, then that equipment should be considered to be unavailable for those events.

Other required equipment: If any equipment is required for EME deployment that is not stored with the EME, it must be demonstrated that this additional equipment will be available and the time required to obtain it must be accounted for in the timing assessment. For example, if self-contained breathing apparatus (SCBA) or portable lighting is required, but not included with the EME, it must be demonstrated that the location of the additional equipment is known, that it can be accessed, and the deployment time must be increased to account for obtaining and using the equipment (if not already accounted for).

Other Considerations: While not technically a feasibility issue, the scenarios in which EME deployment actions are credited should be consistent with the PRA. For example, if the PRA does not credit operator actions in seismic events greater than a certain magnitude, the same limitations should apply to the EME deployment activity. Any exceptions should be documented and a basis for the exception should be provided.

3.2. Use of the decision trees

The HRA decision trees developed for this methodology should not be treated as event trees (i.e., each node does not necessarily represent an event probability). The logic for the decision node describes how the HEPs are impacted based on the paths taken for each decision node. In some cases a multiplier greater than 1 may be applied as part of the quantification, while in others, the deployment time may be doubled and its impact will be accounted for in assessing the branch points related to time margin. Each path through the decision tree will result in a separate HEP that is applicable to the conditions defined by the decision node choices.

The branches on the decision trees represent performance shaping factors that are considered to be the most critical for this activity. If other PSFs are considered relevant, additional branches could be added. For example, since some of these activities may be protracted, it might be thought that fatigue could become an issue. However, this would have already been factored into the assessment when the feasibility of the action was assessed (see Section 3.1.1).

4. ASSUMPTIONS

The following assumptions were made to support the development and initial applications of this methodology:

1. The use of EME is proceduralized, the cues that would lead to deployment are addressed in validated plant procedures that provide step-by-step guidance, and the contribution related to the diagnosis of the need for and decision to implement EME can be evaluated using an existing HRA approach.
2. The personnel responsible for deploying the EME have been trained on the procedures and are qualified to perform the necessary tasks.
3. At least one member of the on-shift deployment team has practiced deploying the EME, and therefore can help the entire team work through problems.
4. The Main Control Room operators (or personnel responsible for controlling the EME) have been trained on the operation of the EME once installed, and the procedures provide sufficient guidance that the contribution to the HEP from failure in execution can be evaluated using current HRA methodologies.
5. For multi-unit site response, the analyzed unit is the last unit to which the EME is deployed. In reality, units with more time critical conditions would likely be prioritized for deployment; however, for this revision of the methodology, no attempt has been made to credit prioritized deployment.
    - If it is desirable or necessary to account for the prioritization of EME deployment, the HRA analyst can model that decision making process and include it in the PRA using existing HRA methodologies as long as the timeline used for EME deployment is adjusted to account for the modified deployment order.
6. The self-check and independent check recovery activities are considered to be most relevant to the “installation” portion of the EME deployment activity; therefore, the time margin assessment is focused on recovering errors committed during the “installation” activity.
7. EME deployment is assumed to be performed in the absence of high radiation conditions that would affect EME deployment for one or more units.
8. In the initial applications, for seismic events with magnitudes greater 0.3g PGA, actions taken in non-seismically qualified buildings were assumed to fail, consistent with other post-seismic human response assumptions in the seismic model. (This threshold could be varied and justified based on the specific seismic model.) The exception is for the EME storage structures, which may be designed to not damage the EME when they collapse. The impacts of EME structure failure, however, should explicitly be considered in the feasibility assessment.
9. The site has developed and is in compliance with guidance that maintains the EME and plant grounds in a state that will not hinder deployment of the EME.

5. EXAMPLE DECISION TREE - HIGH WINDS

The High Winds HRA decision Tree is provided in Figure 1. The guidance for interpreting and using each of the decision tree nodes is provided below.

High Wind Induced Obstruction?

As identified in the "Equipment and Location Accessibility" bullet in Section 3.1.1, deployment is considered to be failed for wind events in which deployment is precluded by the effects of the hazard. Reasons for this include:

- Failure of the structure(s) that house the EME,
- Failure of the structure(s) along the access path (or the access path itself) between where the EME is stored and the point where it is deployed, which if failed, could prevent access,
- Failure of the structure(s) where the EME is deployed (if applicable),
- Obstruction of path due to debris accumulation that is beyond the capability of on-site sources to remove.

It is expected that in these cases, no additional assessment is required.

For scenarios in which the impact is not so severe as to prevent successful deployment, there could still be an impact on the deployment action. An example of this condition may be one in which an EME pump (or fire truck to be used as the EME pump) is stored under a lightweight structure that would not damage the truck when it fails (and there are no other postulated wind generated failures that would impact the truck).

Other conditions that would classify as a "high wind induced obstruction" are those in which wind speeds are adequate to introduce impediments that would require additional time to address, but would not require equipment that is not part of the EME deployment set to move (e.g., fallen branches). Some sites may store heavy equipment, such as bulldozers, with the EME to provide the capability to move larger debris. In the event that this equipment is stored with the EME or is otherwise stored such that its use would be feasible by a qualified member of the deployment team, the EME may be credited for higher severity events that may result in the deposition of larger obstructions (e.g. trees) in the areas where deployment activities are required. The determination of the potential for wind induced obstructions will require a site and scenario-specific assessment of the EME location, access path, and deployment area.

For cases with no expected wind damage, the "no" (down) branch is taken, and no time penalty is assessed.

For cases in which wind induced obstructions/impediments are expected, the "yes" (up) branch is taken and a time penalty is assigned to the deployment task. Because of the nature of the event, there is no means of determining how much of an impact the wind damage may have on the deployment task. In order to provide a means of accounting for potential setbacks, it is assumed that the deployment time for each unique impacted leg (e.g., transportation, installation) of the deployment is doubled, subject to the following:

- If the installation is in an area that is protected from the impacts of high winds (e.g., inside a structure that has not failed), it is not necessary to double the installation time ($T_{Install}$).
- Account for the impacts of increases to the T_{Trans} and $T_{Install}$ (if necessary) times for all of the units that are included in the evaluation of T_{delay} (as defined in the "Time Margin >100%" node of Appendix A) for the analyzed unit. Also, account for increases in the T_{Trans} and $T_{Install}$ times for the analyzed unit if they have not already been accounted for.

- For cases in which multiple units are assessed, there may be some common activities. For example, if a four unit site is being assessed, the timing assessment would double T_{Trans} from the EME storage area to the deployment area if the EME is used for all of the units. If different equipment needs to be deployed for the additional units it may be possible to assume that the pathway has been cleared and only the first unit's T_{Trans} would to need be doubled. This would depend on whether the transportation paths were common.

If a plant specific review demonstrates that doubling the deployment time is not appropriate for the conditions at the site, the analysis can be adjusted to employ a revised deployment time multiplier judged to be more appropriate to the situation being analyzed. The revised multiplier and basis should be documented with the HRA.

<u>Take Action After Event?</u>

This node addresses timing of the deployment relative to the wind event. The "yes" (up) branch corresponds to the condition in which the action can successfully be taken after the wind event has passed. The "no" branch corresponds to the condition in which the action must be taken during the high wind event to ensure success, which is considered to be a high stress condition.

Primarily, this node is most useful for events where there may be high intensity, but short lived strong winds (e.g., during a tornado).

If the up branch is taken for non-high-intensity/short lived events, a clear description of why the node is applicable must be provided.

For the "yes" (up) branch, no multiplier is applied.

For the "no" (down) branch, a multiplier of 2 is applied to represent the impact of the stress associated with having to perform the EME deployment during a high wind event. This is based on the THERP [5] Table 20-16 moderately high stress multiplier of 2, as applied to skilled personnel performing step-by-step tasks.

<u>Wind Below Safety Limits?</u>

This node addresses the potential for high wind events to preclude work outside the plant. An actual physical limit that would prevent work in a high wind event would be difficult to determine, but each plant/site/organization may have safety guidelines that define a wind speed threshold above which actions are not allowed in a high wind event.

For cases where the action may be taken after the high wind event, this node is a pass through (i.e., is not evaluated).

If the wind speed of the event is greater than the safety limits specified for the plant where the action is taken, then the no (down) branch is taken and the action is set to FAILURE. These are cases in which the action is required to be performed during an extreme wind event where outside action is not possible.

If the wind speed of the event is less than the safety limits specified for the plant where the action is taken, then the "yes" (up) branch is taken. A multiplier of 2 is also applied here to represent the physical difficulty of performing the task in a high wind event. The doubling of the failure probability relative to the case in which no high wind conditions exist is based on judgment.

Cases in which actions are required during a storm for which wind does not impact the reliability of the action are not considered to be high wind events.

Time Margin >100%?

This node is used to account for the potential for the deployment team to correct an error in the installation of the EME (i.e., a self-check recovery). Self-checking in this context is defined as the process of checking that, upon completion, the installation has been performed correctly. In order for the error correction to be credited, it must be demonstrated that the time margin is ≥100%. The time margin requirement of 100% is assumed in order to account for the time required to:

- Perform the initial installation (which includes actions such as making temporary piping and/or power connections, loading a generator, and/or pressurizing a water system header),
- Identify if the installation has not been performed correctly,
- Review and re-perform the installation steps, when required,

The time margin definition is borrowed from NUREG-1921 [4] and modified to address the deployment assessment:

Equation 1: Time Margin (expressed as a percentage) =

$$100 * [(T_{SW} - T_{Delay}) - (T_{Trans} + T_{Install} + T_{Exe})] / (T_{Install})$$

Where,

- T_{SW} = the system window, or the time window within which the action must be performed to achieve the function provided by the EME. For example, this time could be measured from the time the hazard impacts the plant to the time at which the EME must be delivering water to its load(s).
- T_{Delay} = time delay, or the duration of time it takes to begin initiating EME deployment for the analyzed unit, measured from the time the hazard impacts the plant. For a multi-unit site, since the analysis is for the last unit for which the EME is deployed, the time delay includes the sum of the times taken to deploy the EME for the other unit(s). Because the order of deployment is not known for multi-unit sites, it is assumed that the analyzed unit is the LAST unit to which the EME is deployed. In reality, units with conditions with more time critical conditions would likely be prioritized for deployment; however, for this revision no attempt has been made to credit prioritized deployment.
    - If it is desirable or necessary to account for the prioritization of EME deployment, the HRA analyst can model that decision making process and include it in the PRA using existing HRA methodologies as long as the timeline used for EME deployment is adjusted to account for the modified deployment order.
- T_{Trans} = the time required to transport the EME from the storage area to the area where the EME is deployed and unload any equipment that is required.
- $T_{Install}$ = the time to perform tasks such as making any necessary temporary piping and/or power connections, loading a generator, and/or pressurizing a water system header such that water is available for the load, when directed.
    - If the installation activity does not include steps that would validate EME operation such that the first opportunity to identify an error would be when the EME was required to provide power/flow to a station load, credit for error correction should not be taken unless some equivalent validation process exists and is performed at or near the time of installation.
- T_{Exe} = the time to perform the steps required to initiate water flow and/or energize electrical equipment from the time when it is directed. [Note that the failure probability of this portion of the EME implementation action is not assessed by this methodology, but the timing assessment for the deployment portion of the action is required to account for the execution time in the time margin assessment.]

Because the deployment team is attempting to correct its own error, a high dependence condition is assumed to exist between the commission of the error and the work to correct it. The THERP guidance provides equations in Table 20-17 for determining dependent failure probabilities for a range of different dependence levels. Because the equation for "high dependence" generally yields results in the 0.5 range, the self-check recovery has been assigned a failure probability of 0.5.

<u>Independent Check Available?</u>

An independent check is considered to be an assessment of the EME installation by a qualified member of the plant staff that was not part of the deployment activity. In order for the check to be credited, it must be demonstrated that the time margin is >=200% using Equation 1.

The time margin requirement of 200% is assumed in order to account for the time required to:

- Perform the initial installation (e.g., making temporary piping and/or power connections, loading a generator, and/or pressurizing a water system header),
- Identify if the installation has not been performed correctly,
- Review and re-perform the installation steps, when required,
- Determine that the EME is still not functioning,
- Have an independent checker trouble shoot and direct the crew to re-perform the installation, when required, to correct the error.

The benefit of concurrent verification (i.e., step review by a team member who did not perform the step, but was present when the step was performed) has not been considered in this methodology. If it is necessary to credit concurrent verification in an application to remove unnecessary conservatism, it may be used in place of independent verification provided that a basis is documented for concurrent verification failure probability.

The "yes" (up) branch is taken for cases in which independent check credit is available. A multiplier of 0.1 is used based on the probability for item 1 in THERP table 20-22. While that item is for routine tasks in normal plant conditions, it represents failure to identify errors in connections, positions of locally operated valves, and breaker positions. The application of the event specific PSF multipliers is considered to address the impact of the events on this credit.

The "no" (down) branch is taken for cases in which no independent check credit can be justified. No multiplier is applied for this branch.

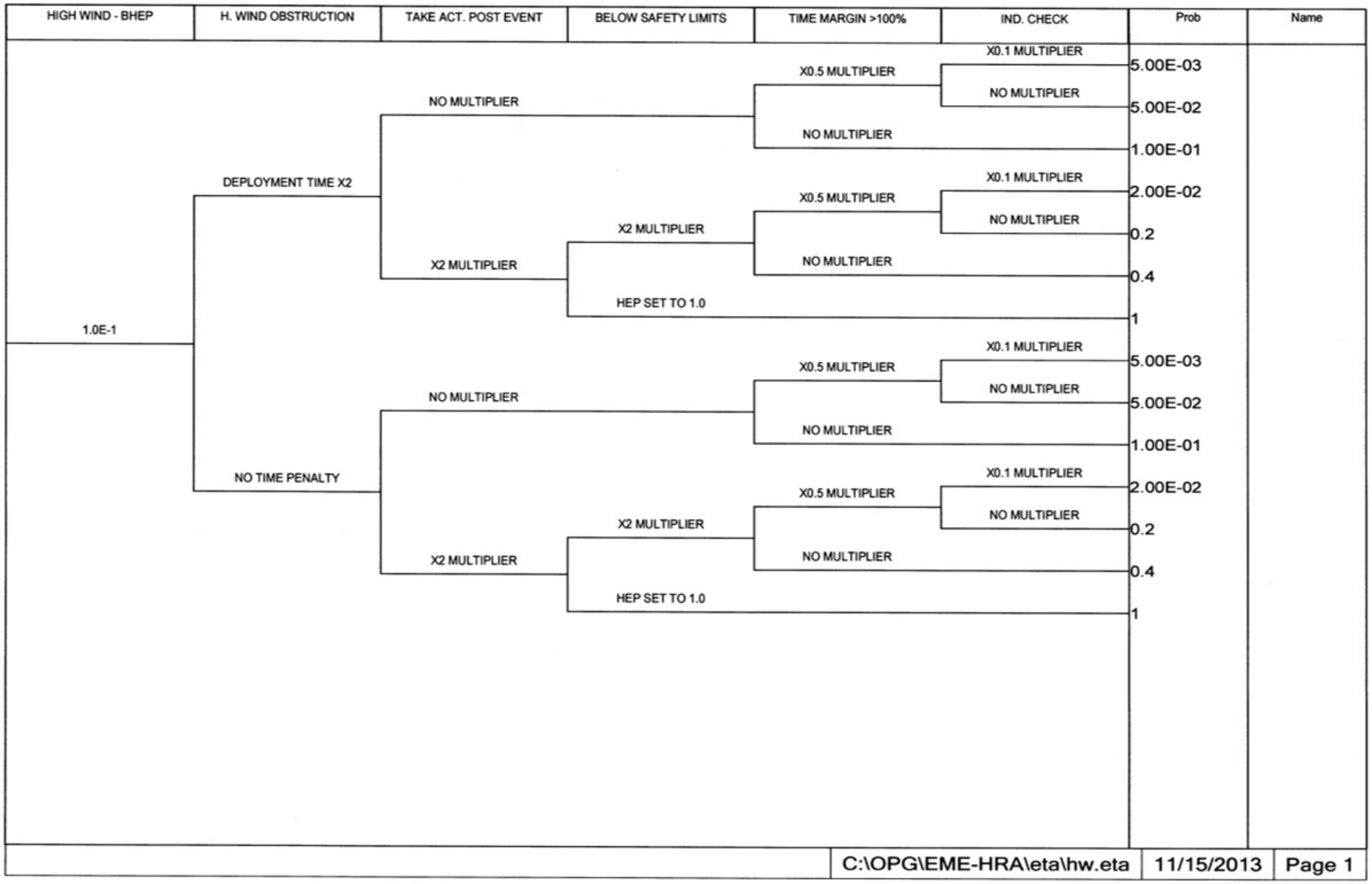
6. CONCLUSION

The methodology documented in this paper is intended to provide a means of quantifying an HEP for the deployment of portable equipment for internal events and selected external events scenarios. Because hazard events, i.e., specific occurrences of the hazard, occur in different ways, the methodology is of necessity bounding in nature and therefore tends to be somewhat conservative. The results, when combined with detailed assessments of the remaining components of the human failure event (i.e., the decision to initiate deployment of portable equipment and the use of the equipment once deployed), are considered to be adequate for use in PRA applications as long as it is understood that there is considerable uncertainty associated with the numerical values.

Acknowledgements

Funding for the development of this methodology was provided jointly by OPG and Bruce Power.

Figure 1: High Wind Events



References

[1] NRC (U.S. Nuclear Regulatory Commission), “Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)”, NUREG-1624, Revision 1, May, 2000.

[2] S.H. Chien A.A. Dykes, J.W. Stetkar, and D.C. Bley, “Quantification of Human Error Rates Using a SLIM-Based Approach”, IEEE Fourth Conference on Human Factors and Power Plants, Monterrey, CA. June 5-9, 1988.

[3] A. Kolaczkowski et. al (U.S. Nuclear Regulatory Commission). “Good Practices for Implementing Human Reliability Analysis”. NUREG-1792. April, 2005.

[4] S. Lewis. (U.S. Nuclear Regulatory Commission). “EPRI/NRC Fire Human Reliability Analysis Guidelines”. NUREG-1921. July, 2012.

[5] A.D. Swain and H.E. Guttman (U.S. Nuclear Regulatory Commission). “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”. NUREG/CR-1278. August, 1983.