INL/CON-23-71740-Revision-0

Simulation-Based Recovery Action Analysis Using the EMRALD Dynamic Risk Assessment Tool

July 2023

Jooyoung Park, Ronald Laurids Boring PhD, Steven R Prescott, Yunyeong Heo

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-71740-Revision-0

Simulation-Based Recovery Action Analysis Using the EMRALD Dynamic Risk Assessment Tool

Jooyoung Park, Ronald Laurids Boring PhD, Steven R Prescott, Yunyeong Heo

July 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Simulation-based Recovery Action Analysis Using the EMRALD Dynamic Risk Assessment Tool

Jooyoung Park[1], Yunyeong Heo[2], Ronald Boring[1], Steven Prescott[1]

[1]Idaho National Laboratory, Idaho Falls ID 83415, USA
[2]Ulsan National Institute of Science and Technology, Ulsan 44919, Republic of Korea

[leave space for DOI, which will be inserted by ANS]

ABSTRACT

A recovery action is defined as an action that prevents deviant conditions from producing unwanted effects. Recovery action evaluations are a critical part of human reliability analysis (HRA). However, limitations arise when treating recovery actions by using currently available HRA methods only. Representatively speaking, the existing recovery analysis methods do not explicitly consider the various recovery task types and recovery sequences that occur at actual NPPs. To handle challenges stemming from the existing recovery analysis methods, this study proposes a way to analyze recovery actions by employing the dynamic HRA method known as the Procedure-based Risk Investigation Method – HRA (PRIME-HRA). Through PRIME-HRA, dynamic simulation models can be developed using dynamic risk assessment tools such as Event Modeling Risk Assessment Using Linked Diagrams (EMRALD) [1] and the Human Unimodel for Nuclear Technology to Enhance Reliability (HUNTER) [2]. EMRALD and HUNTER are dynamic probabilistic risk assessment (PRA)/HRA tools developed at Idaho National Laboratory. This paper explores the differences between THERP, CBDT, and K-HRA in regard to recovery action analysis. It relates the challenges that stem from these approaches, and how we successfully developed PRIME-HRA. Finally, the proposed approach to analyzing recovery human actions within a dynamic context is touched upon, along with an example.

Keywords: Human Reliability Analysis, Recovery Analysis, Dynamic Risk Assessment

1. INTRODUCTION

A recovery action is defined as an action that prevents deviant conditions from producing unwanted effects [3]. The term generally indicates a kind of countermeasure performed in response to failures of human action. Recovery actions play an especially important role in complex systems such as nuclear power plants (NPPs), which consist of highly sophisticated controllers for ensuring that the desired level of performance and safety is achieved and maintained. This is because, when combined with recovery failures, human errors can produce catastrophic effects on a system.

Analyzing recovery actions has been a critical part of human reliability analysis (HRA), a technique for evaluating human errors in order to enable the calculation of human error probabilities (HEPs) for application in probabilistic risk assessment (PRA). If recovery actions are not adequately analyzed and applied to PRA models, the PRA results may be underestimated or rendered unable to reasonably account for failures of human action in the context of PRA. This is why regulatory documents such as ASME/ANS RA-Sb-2013 [4] and NUREG-1792 [5] emphasize the importance of recovery analysis within the context of HRA.

Some existing HRA methods (e.g., Technique for Human Error-Rate Prediction [THERP] [3], Cause-Based Decision Tree [CBDT] [6], and Korean Standard HRA (K-HRA) [7]) entail their own unique approaches to performing recovery analysis within the context of HRA. However, limitations arise when recovery actions are treated using the currently available HRA methods only. The biggest limitation is that the existing recovery analysis methodology does not explicitly consider all the various recovery task types and recovery sequences that occur in actual NPPs.

To handle challenges stemming from the existing recovery analyses, this study proposes a way to analyze recovery actions by employing a dynamic HRA method known as the Procedure-based Risk Investigation Method – HRA (PRIME-HRA). Through PRIME-HRA, dynamic simulation models can be developed using dynamic risk assessment tools such as Event Modeling Risk Assessment Using Linked Diagrams (EMRALD) [1] and the Human Unimodel for Nuclear Technology to Enhance Reliability (HUNTER) [2]. This paper explores the differences between THERP, CBDT, and K-HRA in regard to recovery action analysis. Next, it relates the challenges that stem from these approaches, and how we successfully developed PRIME-HRA. Afterward, the proposed approach to analyzing recovery human actions within a dynamic context is touched upon, along with an example.

2. RECOVERY ANALYSIS IN CURRENT HRA METHODS

The recovery analysis approaches employed by the current HRA methods were all initially based on THERP [3]. Nevertheless, they differ slightly from each other in regard to determining basic recovery HEPs and then adjusting them. Table 1 summarizes how, within the context of THERP, CBDT, and K-HRA, basic recovery HEPs are determined and their values adjusted.

Table 1: Summary of Recovery Analyses in THERP, CBDT, and K-HRA

	Determining basic recovery HEP	Adjusting recovery HEP
THERP [3]	· Basic HEPs for checking operations suggested in THERP Table 19-1	· THERP dependency equations (i.e., conditional probability estimation equations)
CBDT [6]	· Four recovery factors: Self-Review (1.0e-1), Extra Crew (5.0e-1 or 1.0e-1), Shift Technical Advisor Review (1,0e-1), and Shift Change (5.0e-1 or 1.0e-1)	· THERP dependency equations
K-HRA [7]	· Uses decision trees to determine recovery HEPs	· Three performance shaping factors (PSFs): time urgency, man-machine interface, and managing/checking

The currently available recovery analysis approaches are limited in a couple of important ways. First, as already mentioned, they do not explicitly consider the recovery task types and recovery sequences that actually occur in NPPs. In other words, the process of returning to a recovered state is excessively simplified or perhaps omitted altogether. Recovery processes vary depending on the initial task failure type, and they entail different recovery task combinations. Furthermore, once a task failure is fully recovered, the recovery results may totally differ depending on when and where to return to the recovered state. Yet despite all this, the existing HRA methods do not specifically consider these recovery action characteristics so as to evaluate and quantify them within the context of HRA.

Second, recovery of diagnostic errors is rarely considered in current HRA methods, most of which focus on the execution recovery. In actual NPPs, the diagnosis recovery is significant. If operators fail to properly diagnose an initiating event and then enter into a wrong emergency operating procedure, it is essential they re-diagnose the event and determine the correct procedure within the next couple of minutes. The passage of too much time after the initiating event may make correct diagnosis of the event difficult. Thus, diagnosis error recovery is both time-sensitive as well as critical to event mitigation, yet is not treated as such in the currently available recovery analysis methods.

Third, the current definition of recovery actions makes it difficult to collect HRA data for estimating recovery failure probabilities. The existing HRA methods define recovery failure as a task failure that occurs subsequent to another task failure. However, recent HRA data collection studies for supporting HRA data to quantify HEPs have depended on simulator-based experiments [8] [9] in which recovery failures are insufficiently observed, due to the aforementioned definition.

3. EFFORTS TO CONDUCT DYNAMIC (SIMULATION-BASED) HRA

To address challenges stemming from the currently available recovery analysis methods (see Section 2), this study proposes a way to analyze recovery actions by using PRIME-HRA. At Idaho National Laboratory, dynamic HRA research has been performed to complement the existing static HRA approaches [10, 2]. Dynamic HRA offers a couple of important benefits. First, it supports realistic and dynamic modeling of human actions as they would actually be performed at NPPs. It simultaneously models the specific moment at which the action is performed, the time it takes to perform the action, and the failure probability of that action. Second, dynamic HRA enables estimation of the time required to perform an action as well as evaluation of failures over time. (The time required to perform an action was originally estimated based on structured interviews with instructors, operators, and other knowledgeable experts, not on actual data.)

Figure 2 summarizes PRIME-HRA, which consists of four areas: (1) procedure-based task analysis, (2) task unit analysis for procedures applied to a given scenario, (3) development of simulation models using dynamic HRA tools such as EMRALD and HUNTER, and (4) model analysis and integration into the PRA model.

Regarding the first step, task analysis is the process of collecting and analyzing task-related information necessary for performing HRA. In this step, we collect the input data required for modeling procedures and implementing dynamic HRA. These data include static PRA models, information (e.g., PSF data) related to human failure events (HFEs), and relevant procedures. We then develop an event sequence diagram and identify its actual timeline.

In the second step, the procedure paths in the event sequence diagram are decomposed to the task unit level. Basically, a procedure path consists of a couple of procedures that, in turn, include many procedural steps, each of which is comprised of a couple of task units. The task unit represents the procedure task type, as defined in the Human Reliability Data Extraction (HuREX) [9] framework and GOMS-HRA [11]. Time and HEP information are assigned for each task unit. In GOMS-HRA, the time information is assumed to follow a statistical time distribution whose mean value, standard deviation, and 5th and 95th percentile values are dependent on the particular task unit involved. The time data were collected through experiments involving actual operators at the Human Systems Simulation Laboratory (i.e., Idaho National Laboratory's full-scope simulator), which was designed to conduct critical safety-focused human factors R&D. When calculating HEPs, only task units critical to HFEs are considered. Depending on the general approach suggested in existing HRAs, HEPs are calculated based on the relationship between a basic HEP and the PSF multiplier values. In the present study, basic HEPs for task units were derived from the HuREX database. PSFs suggested by the Standardized Plant Analysis Risk-HRA [12] method were also employed.

In the third step, simulation models are developed using dynamic HRA tools such as EMRALD and HUNTER. Application of PRIME-HRA within the EMRALD software is referred to as the Procedure-based Investigation Method of EMRALD Risk Assessment – HRA (PRIMERA-HRA), whereas Procedure-based Investigation of HUNTER Enhanced Risk Assessment – HRA (PRIHERA-HRA) implements PRIME-HRA within the HUNTER tool. The simulation models developed based on these tools include all the information obtained from the previous steps, and are used for evaluating HEPs and time information for HFEs. Only task units relevant to critical human actions are used in the HEP evaluations, whereas the time information is evaluated for every task unit modeled in a given scenario.

In the final step, HFE failure paths, HEPs, and overtime failures for HFEs are evaluated. Those HFE failure paths that are based on cutsets generated from simulation logs explain why a given scenario is considered failed. These can be used to correct modeling errors in dynamic HRA tools. The HEPs generated are provided to the HFEs considered in static PRA models, or to account for human errors in dynamic PRA models. Evaluation of overtime failures for HFEs addresses whether the HFEs are completed within their allotted time windows. If not, this is considered a guaranteed failure (i.e., HEP = 1.0).

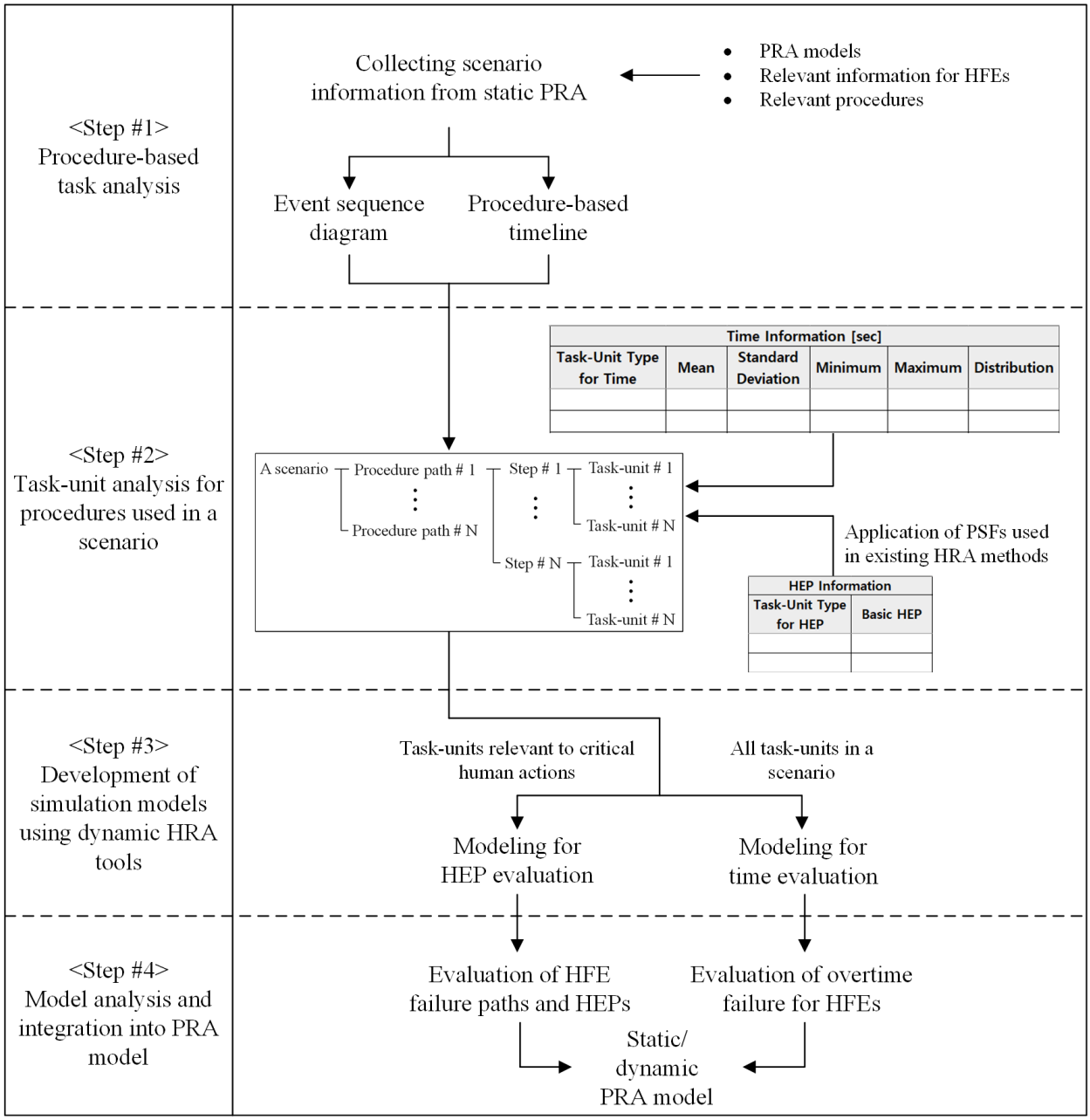

Figure 1. PRIME-HRA Framework

4. RECOVERY ANALYSIS IN A DYNAMIC CONTEXT

To treat recovery actions in a dynamic context, this study proposes a conceptual design for recovery tasks, given in Figure 2. This design views recovery within a scenario-based context rather than focusing solely on individual recovery tasks. In this concept, the term recovery mechanism refers to the entire process of returning to a fully recovered state following a task failure. It is considered a branched scenario, with the recovery mechanism being composed of multiple recovery tasks. An individual recovery task is regarded as a task unit, as defined in the HuREX framework or GOMS-HRA. A recovery task unit represents a typical single-task failure, whereas the legacy recovery analysis has been shown to be a task failure that occurs subsequent to another task failure. Failure of each recovery task may cause total failure of the initial task (i.e., failure of Task #3 in Figure 2).

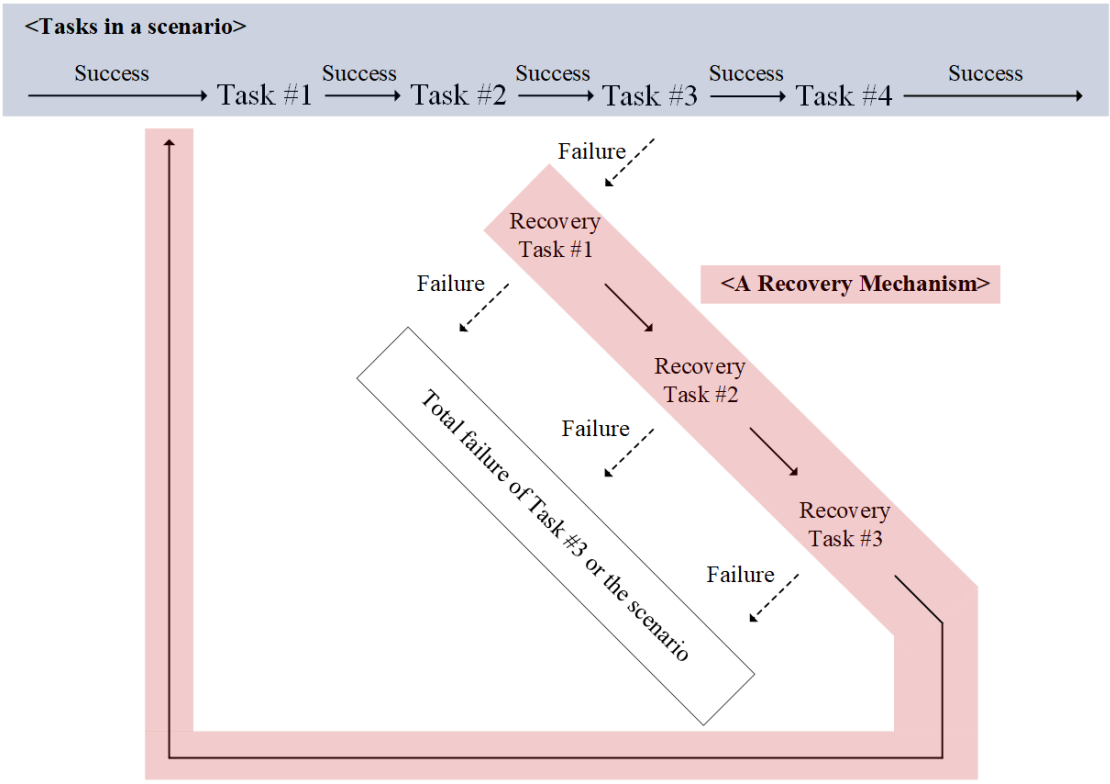

Figure 2. Conceptual Design of the Recovery Mechanisms

In this study, a strategy was constructed for developing a recovery analysis method based on the new conceptual design. Though not yet completely established, it is summarized in this paper. The most important assumption in the design is that recovery mechanisms may be conjugated and generalized based on initial task failure type. In other words, identical recovery mechanisms can be used for different tasks that correspond to the same failure type. Based on this assumption, we suggest three steps for implementing the new method: (1) classify the initial task failure types, (2) investigate and characterize the recovery mechanisms, and (3) use a dynamic risk assessment tool to quantify the recovery mechanisms.

The initial task failure types classified in the first step are used for defining the recovery mechanisms in the second step. The current efforts focus on seven factors potentially useful for classifying initial task failure types: organization (e.g., main control room [MCR] operators or local operators), work equipment (e.g., MCR board or fixed equipment), work location (e.g., MCR or local place), action type (e.g., diagnosis- or execution-based tasks), control room type (e.g., analog or digital), error type (e.g., error of omission or error of commission), and procedure type (e.g., Westinghouse or Combustion Engineering).

The cases derived from these factors are simplified and grouped according to representative initial task failure type.

The second step defines and characterizes the recovery mechanisms, as well as the recovery tasks encompassed by each mechanism. Recovery mechanisms are defined and characterized based on the initial task failure type. Table 2 shows an example recovery mechanism for an initial task failure type related to tasks conducted within the local area. Specifically, the local operators fail to perform a couple of manipulations in the local area, though they should complete all the mission activities locally. They notice the fault after coming back to MCR and communicating with MCR operators, then return to locally perform the correct manipulations. In this specific example, three recovery tasks are considered. However, for this step (i.e., the second step), specific guidance on how to consistently define these tasks within the context of a given recovery mechanism remains under development.

Table 2: Example Initial Task Failure and Its Recovery Mechanism

	Initial task failure type	Recovery mechanism		
		Recovery task #1	Recovery task #2	Recovery task #3
Description	The local operator fails to perform a local action.	The local operator communicates with a shift supervisor in a MCR.	The local operator re-accesses the local area.	The local operator identifies and corrects the error.
Actor	Local operators	Local operators	Local operators	Local operators
Work equipment	Fixed	-	-	Fixed

The third step is to quantify recovery mechanisms by using dynamic risk assessment tools such as EMRALD and HUNTER. Figure 3 shows an example EMRALD simulation model for the case illustrated in Table 2. The initial task failure type and recovery tasks in Table 2 are included in the model. The simulation resulted in a total of eight recovery failures out of the 1,543 recovery opportunities, for a total recovery failure probability of 5.18e-3.

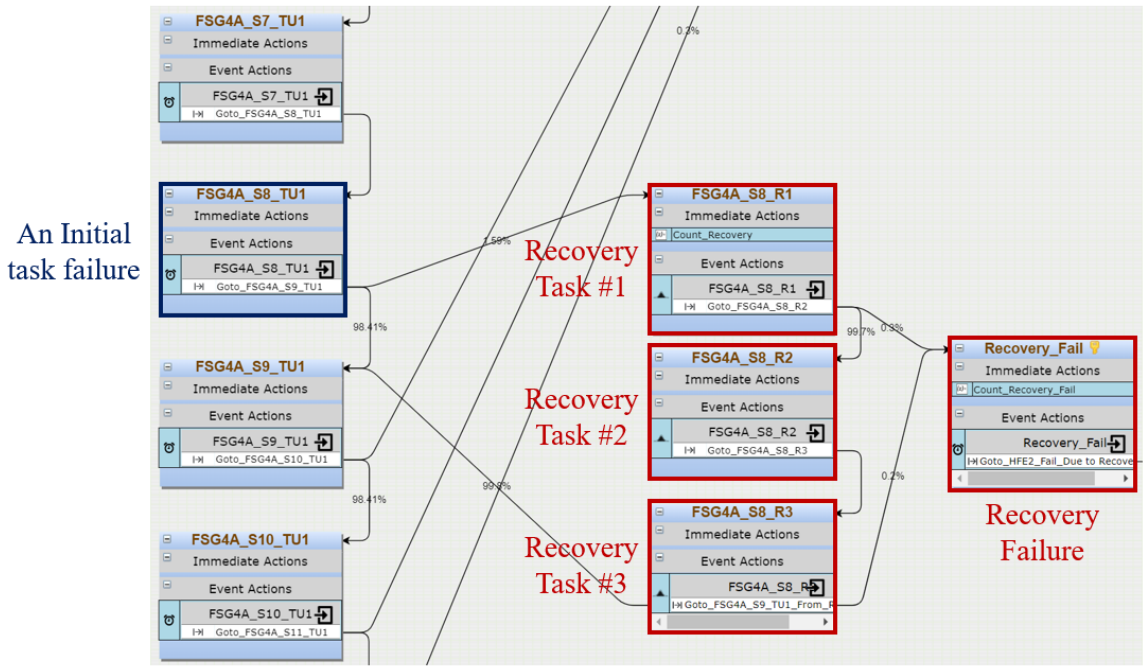

Figure 3. Example of the EMRALD Simulation Model

5. CONCLUSION

This study proposed a structured approach to analyzing recovery actions by using PRIME-HRA, a dynamic HRA method. It explored the differences between THERP, CBDT, and K-HRA in regard to recovery action analysis. It covered the various challenges stemming from these approaches, and explained how PRIME-HRA was initially developed. Finally, the proposed approach to analyzing recovery human actions in a dynamic context was touched upon, along with an example.
This study represents an ongoing effort to better evaluate recovery actions within the context of HRA. Specific guidance on using the proposed method will be further researched and then presented at the conference.

ACKNOWLEDGMENTS

This work was supported by the Risk-Informed System Analysis (RISA) Pathway of the U.S. Department of Energy's Light Water Reactor Sustainability Program and the Laboratory Directed Research and Development funding of Idaho National Laboratory.

REFERENCES

[1] Idaho National Laboratory, https://emrald.inl.gov/SitePages/Overview.aspx.

[2] R. Boring, T. Ulrich, J. Ahn, Y. Heo and J. Park, "Software Implementation and Demonstration of the Human Unimodel for Nuclear Technology to Enhance Reliability (HUNTER)", INL/RPT-22-66564, Idaho National Laboratory, 2022.

[3] A. D. Swain and H. E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report," NUREG/CR-1278, Sandia National Laboratory, Albuquerque, NM (USA), 1983.

[4] ASME/ANS, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, American Society of Mechanical Engineers, 2008.

[5] U. NRC, Good practices for implementing human reliability analysis, NUREG-1792, US Nuclear Regulatory Commission, 2005.

[6] G. Parry, A. Beare, A. Spurgin and P. Moieni, "An approach to the analysis of operator actions in probabilistic risk assessment, " EPRI Report TR-100259, 1992.

[7] W. D. Jung, D. I. Kang and J. W. Kim, "Development of a standard method for human reliability analysis (HRA) of nuclear power plants - Level 1 PSA full power internal HRA, KAERI/TR-2961/2005," Daejeon, Republic of Korea, 2005.

[8] Y. J. Chang, D. Bley, L. Criscione, B. Kirwan, A. Mosleh, T. Madary and R. Nowell, "The SACADA database for human reliability and human performance," *Reliability Engineering & System Safety,* vol. 125, pp. 117-133, 2014.

[9] W. Jung, J. Park, Y. Kim, S. Kim and S. Choi, "HuREX–A framework of HRA data collection from simulators in nuclear power plants," *Reliability Engineering & System Safety,* vol. 194, p. 106235, 2020.

[10] J. Park, R. Boring and T. Ulrich, "An Approach to Dynamic Human Reliability Analysis using EMRALD Dynamic Risk Assessment Tool," in *Probabilistic Safety Assessment and Management (PSAM) 16*, 2022.

[11] R. Boring and M. Rasmussen, "GOMS-HRA: A method for treating subtasks in dynamic human reliability analysis," in *Proceedings of the 2016 European Safety and Reliability*

Conference, 2016.

[12] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H human reliability analysis method, NUREG/CR-6883," US Nuclear Regulatory Commission, 2005.