Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 00 (2015) 000–000

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

The development of dynamic human reliability analysis simulations for inclusion in risk informed safety margin characterization frameworks

Jeffrey C. Joe[a,]*, Rachel B. Shirley[b], Diego Mandelli[a], Ronald L. Boring[a], Curtis L. Smith[a]

[a]*Idaho National Laboratory, PO Box 1625, Mail Stop 3818, Idaho Falls 83402, USA*
[b]*The Ohio State University, Columbus 43210, USA*

Abstract

The United States Department of Energy is sponsoring the Light Water Reactor Sustainability program, which has the overall objective of supporting the near-term and the extended operation of commercial nuclear power plants. One key research and development (R&D) area in this program is the Risk-Informed Safety Margin Characterization pathway, which combines probabilistic risk simulation with thermohydraulic simulation codes to define and manage safety margins. The R&D efforts to date, however, have not included robust simulations of human operators, and how the reliability of human performance or lack thereof (i.e., human errors) can affect risk-margins and plant performance. This paper describes current and planned research efforts to address the absence of robust human reliability simulations and thereby increase the fidelity of simulated accident scenarios.

Keywords: Human reliability analysis (HRA); Time-reliability studies; Risk Informed Safety Margin Characterization; Dynamic HRA

* Corresponding author. Tel.: +1-208-526-4297 ; fax: +1-208-526-0528 .
E-mail address: jeffrey.joe@inl.gov

1. Introduction

The United States (U.S.) Department of Energy sponsors the Light Water Reactor Sustainability (LWRS) program, which has the overall objective of supporting the near-term and the extended operation of commercial nuclear power plants (NPPs). Life extension of existing NPPs is important because they are currently the largest source of carbon free electrical generation, and because the cost to build new NPPs is significantly higher. One key research and development (R&D) area in this program is the Risk-Informed Safety Margin Characterization (RISMC) pathway, which combines probabilistic risk simulation with thermohydraulic and reactor kinetic simulation codes (i.e., mechanistic multi-physics models) to define and manage safety margins for commercial NPPs [1] [2].

Broadly speaking, a "margin" is usually characterized either in deterministic or probabilistic terms. A deterministic margin is typically defined as the difference between capacity and load, or alternatively as the ratio of capacity to load. A probabilistic margin is usually defined as the probability that a load exceeds the capacity. The RISMC pathway uses the probabilistic margin characterization to quantify impacts to reliability and safety. Therefore, a probabilistic safety margin is a numerical value quantifying the probability that a safety metric (e.g., an important process variable such as clad temperature) will be exceeded under accident scenario conditions. This also means that instead of calculating risk as the frequency of an event (e.g., core damage), risk is conceptualized in terms of how close or not the NPP is to key safety related parameters or events, with the purpose of trying to understand how to better quantify and reduce uncertainty, and characterize the safety margin.

The RISMC toolkit was developed at Idaho National Laboratory (INL) to perform these kinds of advanced safety analyses. As seen in figure 1, the toolkit uses the Multiphysics Object Oriented Simulation Environment (MOOSE) [3] as the underlying numerical solver framework, and consists of 1) the Reactor Excursion and Leak Analysis Program (RELAP)-7 code [4], which simulates the thermohydraulics of the plant, and 2) Reactor Analysis and Virtual Control Environment (RAVEN) [5]. RAVEN acts as a controller of the RELAP-7 simulation and generates multiple scenarios by stochastically changing the order and/or timing of events. Specifically, the risk simulation module includes as a "scenario generator" of normal and abnormal events that serve as inputs to the mechanistic codes, while the mechanistic codes input physical parameters (e.g., core temperature) to the risk simulation, thereby creating an advanced RISMC toolkit that NPP owners and operators can use to generate a more accurate representation of NPP safety margins, and their associated influences on operations and economics.

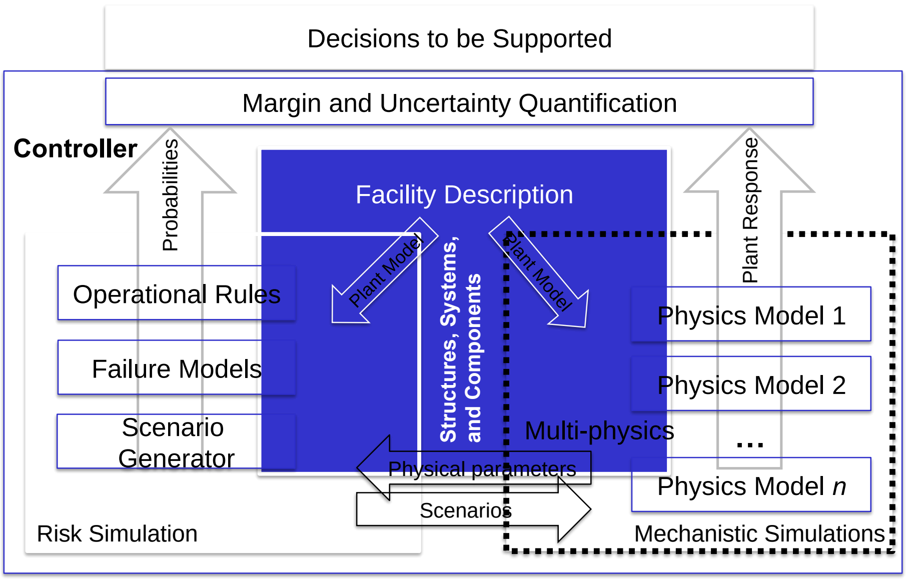

Fig. 1. The approach used to support RISMC analysis.

1.1. Including human reliability analysis in RISMC

In order to more completely model and calculate probabilities within the risk simulation, the RISMC toolkit needs to incorporate human reliability analysis (HRA) into the scenario generator, failure models, and operational rules. In terms of RAVEN's control logic, the insertion point for HRA is through the control logic equations that are part of RAVEN's overall plant equations (which also include mechanistic thermohydraulic equations). The control logic equations control parameters in RELAP-7 such as pump speeds and valve positions, which (along with the aforementioned thermohydraulic equations) affect thermohydraulic variables such as pressure, temperature, and flow rates, which subsequently feed back to the control parameters via monitored variables (e.g., average pressure, delta-t).

In previous RISMC studies [6], human interactions were modeled in a simplified manner by using the Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method [7] contained in the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software was used. Moreover, while SPAR-H uses 8 performance shaping factors (PSFs) to adjust the nominal probability that an action will happen or not, thereby creating a Bernoulli distribution, only two of its 8 PSFs (e.g., *complexity* and *stress/stressors*) were used in the previous RISMC study.

These simplifications aside, from a simulation point of view, the goal of [6] was not to determine if an action is performed but rather when such action is performed. Thus, probability distribution functions (PDFs) that define the probability that a human related action occurs as a function of time were created. As Table 1 shows, the standard lognormal parameters μ and σ were calculated from the 2 SPAR-H PSFs to create distributions representing the uncertainties related to when human related action is performed.

Table 1. Correspondence table between complexity and stress/stressor level and time values.

Complexity	μ (min)	Stress/stressors	σ (min)
High	45	Extreme	30
Moderate	15	High	15
Nominal	5	Nominal	5

From this transformation of SPAR-H PSFs to PDFs, very simple interactions between humans and the scenario evolution could be modeled in the RISMC toolkit, whereby the PDFs created defined when (not if) the human action was performed. However, given the simplified approach used, it also meant that the accident evolution and the human model were uncoupled, and the SPAR-H PSFs were assumed to be constant throughout the scenario. Errors of omission and commission were also not included. As such, the RISMC R&D efforts to date have not included robust simulations of human operators, and how the reliability of human performance or lack thereof (i.e., human errors) can affect risk-margins and plant performance. This paper describes current and planned research efforts to enhance the human modeling components in order to increase the fidelity of simulated accident scenarios.

2. Previous time-based HRA efforts

One obvious way to enhance the research efforts undertaken thus far is to use time-based HRA models in the RISMC toolkit instead of SPAR-H. There are a number of time-based HRA methods and a few seminal HRA data collection efforts that could be used to provide modest improvements to the integration of human reliability into the RISMC approach. Generally speaking, time-based HRA models compute the human failure probability from the time available and the time needed to complete a task. The seminal examples of how timing is modeled include the classic HRA method, the Technique for Human Error Rate Prediction (THERP) [8], and the Human Cognitive Reliability (HCR) method [9]. In addition to HRA methods development, three different research activities collected time-based human reliability data: the Electric Power Research Institute (EPRI) Operator Reliability Experiments (ORE), the Risk Methods Integration and Evaluation Program (RMIEP) [10] [11], and the International HRA Empirical Study [12]. All of these sources provide timing data for NPP operators, with some focusing on high-level tasks (e.g., isolating a ruptured steam generator, manually tripping the plant, etc.), and other looking at diagnosis activities during abnormal events. This timing data may provide useful, empirically based data for the RISMC toolkit.

2.1. Timing in the Technique for Human Error Rate Prediction (THERP)

In THERP, timing is used to predict the probability that an operator will successfully diagnose an abnormal event. The probability of success increases as time increases; immediately following the event, the probability of success is zero, but with infinite time available, the probability of successfully diagnosing the accident is one. Other factors (such as operator expertise) are not addressed in the model for the failure probability for diagnosis [8].

Fig. 2 shows the failure probability, or time reliability curves for diagnosis as a function of time. The failure probability decreases as the time from the event increases. The failure timing model is based on the Nuclear Reliability Evaluation Program (NREP) procedures guide, [13]. Probability of failure to diagnose an abnormal event is assumed to be lognormal over time, generally decreasing as time from the event increases. For multiple abnormal events, a ten minute constant is added to the distribution for diagnosing the second event. Timing estimates are based entirely on expert consensus and are therefore “highly speculative,” with no data behind the model [14].

2.2. Human Cognitive Reliability

The HCR method developed by EPRI improves on THERP’s treatment of timing in two significant ways. First, HCR includes timing considerations in multiple human failure events (not only diagnosis). Second, HCR is built on data from the ORE studies conducted in the 1980s, meaning that the time reliability curves employed in HCR are based on experimental data rather that expert judgment. As with THERP’s diagnosis failure probabilities, HCR estimates the probability of failure of different human interactions (HIs) using the time available and the time required. The method estimates the probability of non-response (i.e., the probability that an operator will not complete a specific HI) [15].

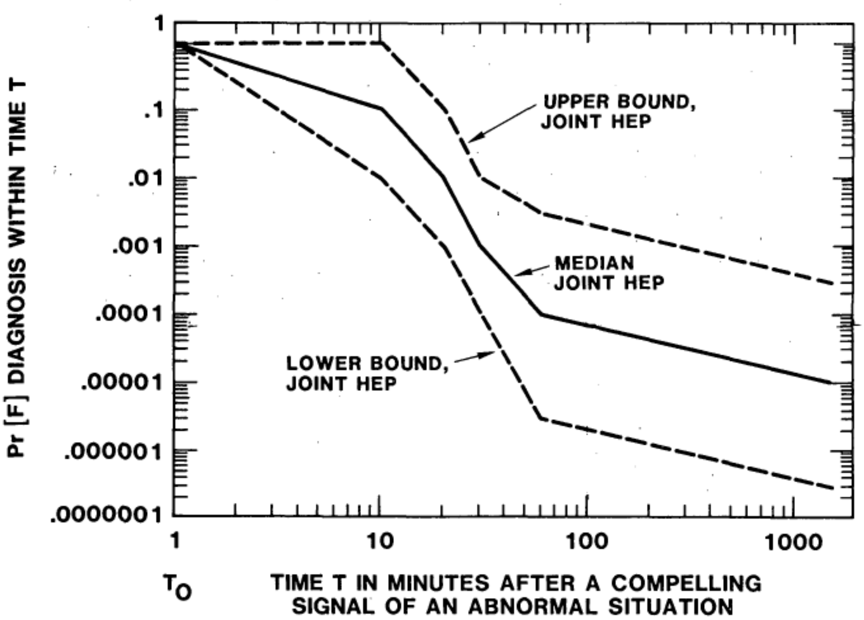

Fig. 2. THERP failure probability curves (Figure 12-4 in [8]).

The general approach calculates the time required for three phases of a HI: recognition of the problem, diagnosis of the problem, and recovery actions. For each phase, the analyst specifies the operator experience, stress, and quality of the human-machine interface. These three factors can increase or decrease the amount of time required for each phase of the HI. After calculating the time required to complete the HI's three phases, the analyst refers to the appropriate HCR curve to estimate the probability of non-response [14].

2.3. Operator Reliability Experiment

EPRI conducted the ORE in the 1980s to test and improve the HCR model. Data were collected at 8 plants. Four of the plants were boiling water reactors (BWRs) and four were pressurized water reactors (PWRs), with multiple crews observed at each plant. Fourteen unique PWR scenarios and 16 unique BWR scenarios were observed for the study, with some scenarios being repeated at multiple plants [12].

HCR defines three types of HIs: pre-initiating event HIs (Type A), initiating event-related HIs (Type B) and post-initiating event HIs (Type C). Data collected in the study emphasizes Type C interactions, specifically post-initiating, proceduralized HIs. Additionally, because Type C HIs are highly dependent on cues the plant provides (e.g., an alarm, a noticeable change in a plant parameter), and because success and failure are essentially defined by whether the operator correctly interprets and responds to that cue, a cue-response structure was defined to categorize operator responses to procedures into 5 different types.

HIs are identified for each scenario, and individual crew response times are reported for each HI, along with scenario timelines for individual crews. The resulting aggregate data provides median response times for specific HIs. The expected standard deviation values for CP1-CP3 HI response times are also calculated. With this information, an analyst can develop a reasonable distribution for expected response times for other interactions without conducting extensive additional simulator studies.

2.4. Risk Methods Integration and Evaluation Program

For RMIEP, HRA researchers used the LaSalle NPP training simulator to collect time-based human reliability data related to diagnosis activities operators perform during accident scenarios. Nineteen crews from LaSalle participated. The objective of the effort was to collect data that would alleviate the heavy reliance on subjective expert judgment to inform the generation of time-reliability curves (i.e., curves showing the probability of non-recovery as a function of time).

The 8 different accident scenarios chosen for this study were based on prior studies that tentatively identified them as the dominant accident sequences for LaSalle, and as [13] states, "The recovery actions were identified and grouped based upon their operational similarities. Once these operational groups were formed, statistical tests were performed on the time data within each of the groups to determine whether the time data could be combined. If the statistical tests supported the operational group, then all data for actions within a group were combined and a function was fitted to the combined empirical data. Ten diagnosis time-reliability curves resulted which provide the PRA analyst with a data-based means of estimating the probability that the operators will fail to correctly diagnose the problem within a specified time." (pg. 3). Overall, the RMIEP effort was one of just a few efforts with the goal of providing an empirical basis to help PRA estimate probabilities of success and failure for non-routine tasks, such as time-dependent diagnosis and misdiagnosis probabilities for accident sequences.

2.5. International HRA Empirical Study

The International HRA Empirical Study involved 14 crews. Each crew completed four scenarios: simple and complex versions of a steam generator tube rupture (SGTR) and a steam line break (SLB). Published reports include timing data for pre-defined human failure events (HFEs), and more detailed timing data are also available in the study data sets (see [16] and [17]). Although these data are limited to variations on two design-basis accidents, the relatively large number of crews in the study provides a distribution of timing data that could be used in the RISMC toolkit. A related study featured similar data for loss of feedwater (LOFW) scenario variants [18]. Characteristic variations in timing that can be applied to other scenarios may be identifiable from these data.

2.6. Next steps

The RISMC toolkit has the opportunity to use the time-based HRA methods that have been developed and data that has been collected to better represent human actions in its risk simulations, thereby improving the overall risk models being used to inform margin and uncertainty quantification. Continued development of dynamic HRA specifically for RISMC applications also holds promise. Dynamic HRA methods are in many ways an extension of the early time-based methods, in that many still use the time needed versus time available logic [19] as a central component of their approach [20] [21]. The more recent dynamic HRA efforts are related to the Accident Dynamics Simulator-Information Decision and Action in Crew (ADS-IDAC) system [22], which ties together a cognitive model, a decision making engine, performance shaping factors, and a dynamic event simulator. ADS-IDAC was further extended to include a crew response model for emergency operations (i.e., a station blackout at a PWR) [23] and severe accidents in nuclear power plants [24]. Next steps include evaluating the feasibility of using ADS-IDAC in the RISMC toolkit for uncertainty quantification and safety margin characterization.

3. Conclusion

Nuclear power is an important component of the U.S. economy in that commercial NPPs provide reliable and cost-competitive base load electricity to homes and businesses. LWRS R&D activities are an important contribution to overall efforts to help maintain the current fleet of commercial NPPs. R&D under the RISMC pathway in particular is working to better define safety by changing the paradigm from calculating the frequency of failure to characterizing the safety margin. The R&D currently underway to include more robust models of human performance and error will help improve the accuracy of the probability calculations and quantification of uncertainties associated with characterizing safety margins.

Acknowledgements

INL is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517. This work of authorship was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately-owned rights. The United States Government retains, and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or any agency thereof. The INL issued document number for this paper is: INL/CON-15-34948. The lead author also thanks Allison C. Joe for her help in preparing this article.

References

[1] C. Smith, C. Rabiti and R. Martineau, “Risk Informed Safety Margin Characterization (RISMC) Pathway Technical Program Plan,” Idaho Falls, 2011.

[2] D. Madelli, C. Smith, T. Riley, J. Nielsen, J. Schroeder, C. Rabiti, A. Alonsi, R. Kinoshita, D. Malijovec, B. Wang and V. Pascucci, “Overview of new tools to perform safety analysis: BWR station black out test case,” in Proceedings of PSAM 12 Conference, Honolulu, 2014.

[3] D. Gaston, G. Hansen and C. Newman, "MOOSE: A Parallel Computational Framework for Couples Systems for Nonlinear Equations," in International Conference on Mathematics, Computational Methods, and Reactor Physics, Saratoga Springs, NY, 2009.
[4] R. David, D. Gaston, R. Martineau, J. Peterson, H. Zhang, H. Zhao and L. Zou, "RELAP-7 Level 2 Milestone Report: Demonstration of a Steady State Single Phase PWR Simulation with RELAP-7," Idaho National Laboratory, Idaho Falls, 2012.
[5] C. R. Alfonsi, D. Mandelli, J. Cogliati and R. Kinoshita, "Raven as a tool for dynamic probabilistic risk assessment: Software overview," in ," in Proceeding of M&C2013 International Topical Meeting on Mathematics and Computation, CD-ROM, American Nuclear Society, LaGrange Park, IL, 2013.
[6] C. S. Mandelli, T. Riley, J. Schroeder, C. Rabiti, A. Alfonsi, J. Nielsen, D. Maljovec, B. Wang and V. Pascucci, "Support and Modeling for the Boiling Water Reactor Station Black Out Case Study Using RELAP and RAVEN," Idaho National Laboratory, Idaho Falls, 2013.
[7] D. Gertman, H. Blackman, J. Marble, J. Byers and C. Smith, "The SPAR-H Human Reliability Analysis Method," NRC, 2005.
[8] A. Swain and H. Guttmann, "Handbook of human reliability analysis with emphasis on nuclear power plant applications. Final report. NUREG/CR-1278.," U.S. NRC, Washington, DC, 1983.
[9] Electrical Power Research Institute, "An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, TR-100259," Electrical Power Research Institute, Palo Alto, CA, 1992.
[10] L. Weston, D. Whitehead and N. Graves, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 1: Development of the Data-Based Method, NUREG/CR-4834 (vol. 1)," U.S. Nuclear Regulatory Commission, Washington, DC, 1987.
[11] D. Whitehead, "Recovery Actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 2: Application of the Data-Based Method, NUREG/CR-4834 (vol. 2)," U.S. Nuclear Regulatory Commission, Washington, DC, 1987.
[12] A. Spurgin and P. Moieni, "Operator Reliability Experiments Using Power Plant Simulators, Volume 3: Appendixes," EPRI, 1991.
[13] A. Papazoglou, R. Bari, A. Buslik, R. .. Hall, D. Ilberg, P. Samanta, T. Teichmann, R. Youngblood, A. El-Bassioni, J. Fragola, E. Lofgren and W. Vesely, "Probabilistic Safety Analysis Procedures Guide," Brookhaven National Laboratory, Upton, NY, 1984.
[14] D. Gertman and H. Blackman, Human Reliability and Safety Analysis Data Handbook, John Wiley & Sons, 1994.
[15] A. Spurgin and P. Moieni, "A human reliability analysis approach using measurements for individual plant examination," EPRI, Palo Alto, CA, 1989.
[16] "International HRA Empirical Study, Phase 1 Report: Description of Overall Approach and pilot phase results from comparing HRA methods to simulator performance data," US NRC, 2009.
[17] "International HRA empirical study, Phase 2 report: results from comparing HRA method predictions to simulator data from SGTR scenarios," US NRC, 2011.
[18] U.S. Nuclear Regulatory Commission, "The International HRA Empirical Study: Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data, NUREG-2127," U.S. Nuclear Regulatory Commission, Washington, DC, 2014.
[19] G. Apostolakis, V. Bier and A. Mosleh, "A critique of current practice for the use of expert opinions in probabilistic risk assessment," Reliability Engineering & System Safety, vol. 22, no. 1, pp. 201-217, 1988.
[20] M. Jae and C. Park, "A new dynamic HRA method and its application," Journal of the Korean Nuclear Society, vol. 27, pp. 292-300, 1995.
[21] M. Jae, "A new dynamic reliability assessment for mid-loop operations in a nuclear power plant," International Journal of Reliability and Applications, vol. 3, no. 1, pp. 25-35, 2002.
[22] Y. Chang and A. Mosleh, "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents, Parts 1-5," Reliability Engineering and System Safety, vol. 92, pp. 997-1101, 2007.
[23] K. Coyne, A predictive model of nuclear power plant crew decision-making and performance in a dynamic simulation environment, College Park,, MD: University of Maryland PhD Dissertation, 2009.
[24] Y. Li, Modeling and simulation of operator knowledge-based behavior, College Park, MD: University of Maryland PhD Disertation, 2013.