A Model-driven Approach for Incorporating Human Reliability Analysis in Early Emergency Operating Procedure Development

Nikolaos Papakonstantinou[[1]](#footnote-1)

Markus Porthin

Bryan M. O’Halloran

Douglas L. Van Bossuyt[[2]](#footnote-2)

Key Words: Human Reliability Analysis, Human Error Probabilities, Probabilistic Risk Assessment, HRA, HEP, PRA

SUMMARY & CONCLUSIONS

Current Probabilistic Risk Assessment (PRA) methods analyze operator actions in accident scenarios using Human Reliability Analysis (HRA) methods after Emergency Operating Procedures (EOPs) and complex system design are largely complete. This paper proposes the early Model-based HRA (eMHRA) method that couples PRA, HRA, and EOP development together and shifts analysis earlier into the complex system design process. By moving the development of these related and important steps in complex system design earlier in the design process, significant modifications to the complex system can be made much more inexpensively and consume much less time to address critical issues found in PRA, HRA, and EOP development. Further, EOP developers can benefit from rapid and early feedback from the HRA and PRA information. A software tool was developed to implement the eMHRA method presented in this paper and is demonstrated in the paper. A case study is presented of a subsystem of a generic Pressurized Water Reactor (PWR) civilian nuclear power plant. The case study shows that HRA and EOP insights can be incorporated into PRA models early in the design process to better inform system designers of potential high likelihood failure events in operator actions. The eMHRA method presented in this paper provides a new tool for risk analysts to better predict and understand failure scenario outcomes early in the design process. With this information, engineers will be better able to develop new EOPs and operator interfaces to reduce failure likelihood in due to missed operator recovery actions.

1. Introduction

Complex systems such as nuclear power plants, commercial aircraft, and crewed spacecraft are analyzed for potential failure modes to determine system failure probability. Methods such as Probabilistic Risk Assessment (PRA) are used to conduct detailed analysis of potential failure scenarios that can lead to redundant, highly reliable systems to fail. In all but the most highly automated systems or the most rapid of failure progressions, human intervention can occur to attempt to mitigate and stop the progression of complex system failures to prevent system-level failure. Emergency Operating Procedures (EOPs) are developed as part of the design and testing phases of complex system development to provide a guide for human operators to follow in the event of a failure. Risk analysts use EOPs and other information to further refine PRA models and credit human recovery actions to reduce system failure probability. The field of Human Reliability Analysis (HRA) attempts to inform PRA analysis of the reliability of operators in critical human recovery actions through the use of Performance Shaping Factors (PSFs) to determine Human Error Probabilities (HEPs). However, there is no formalized process to connect the development of EOPs with determining HEPs to better inform PRA models, especially during the early phases of design.

This paper introduces a novel model-driven approach, the early Model-based HRA (eMHRA) method, for coupling HRA and early EOP development. Tightly coupling the development of EOPs, the PRA model, and the design process of a complex system will provide system design engineers with insights into how humans can effectively interact with the system during a failure event. The proposed methodology involves the development of an EOP metamodel that includes HRA-related metadata useful for early HRA and for defining the communication interface between the EOP developer and the safety engineer performing the full HRA. eMHRA can be applied to any HRA method based on PSFs. The SPAR-H HRA method is used as the basis of a case study on a portion of a Pressurized Water Reactor (PWR) nuclear power plant although the method presented in this paper can be used with any of the common HRA methods and on any complex system being analyzed with PRA or similar risk analysis methods.

1. Background

The eMHRA method presented in this paper relies upon several key developments in complex system design methods. While much of the background presented below focuses on civilian commercial nuclear power plant design, the core concepts apply more broadly to complex system design. Of specific relevance to the eMHRA methodology are safety analysis in complex systems, EOP development, HRA processes, the SPAR-H tool, and Unified Modeling Language (UML) modeling approaches.

According to NUREG-711 [1], PRA and HRA should be used at an early stage in the design of commercial nuclear power plants to identify important human actions (HA) that should be paid special attention to in the nuclear power plant’s systems development and the human factors engineering design of the operator interfaces with plant systems. The PRA/HRA should be updated iteratively as the design progresses to ensure the actual important HAs are captured and considered.

The development of procedures, both for emergencies as well as for normal situations, testing, maintenance etc., is an important part of the human factors engineering design along with human-system interface (HSI) design and training program development. Procedures are essential to plant safety because they support and guide personnel interactions with plant systems and personnel responses to plant-related events [1]. Procedures are typically written documents, including both text and graphic formats, that present a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) in order to accomplish a goal safely and efficiently [2]. Traditionally, procedures have been paper-based, but the industry is gradually shifting to the use of computer-based procedures (CBP) [3]. EOPs are used to guide the operators to bring the plant to a safe state after a disturbance has occurred.

EOPs are written in multidisciplinary teams including operators, designers, process experts, human factors experts, etc. [4, 5]. According to Wieringa and Farkas [4], the main challenges in procedure writing in the nuclear domain are the consequences of potential errors in the procedures, the complexity of the system and the process and its unanticipated ways of responding in emergency situations, the complexity of the user interface in the control room, and that the procedures are used by a group of operators rather than one individual. In addition, the procedure writer should take into account that the usage situation may be affected by time constraints and other factors that may raise the possibility of errors (acts of omission or commission). What is also distinctive to nuclear power plants and other complex systems that have dedicated operators is that the users are highly trained in understanding physical phenomena and the usage of the system and procedures. According to Niwa and Hollnagel [5], the EOPs should be effective in bringing about desired changes in the process being controlled and their development should be explicit and transparent so that related decisions can be traced, facilitating maintaining of the procedures. The operators should be able to carry out the EOPs without any undue difficulties, not causing too much task overload. The EOPs should also be structured and presented in a way that they are easy to understand and follow. The design principles for EOPs and especially CBPs followed by Électricité de France (EdF) are [6]:

* The CBP should leave operators in-the-loop, meaning that the final decision should be left to the operators, and the procedure should only have an advisory role.
* The CBP screens should present the control objectives, the current process solution, and the required actions.
* Operators should be able to navigate freely within the procedure to make up for its deficiencies.
* The procedures should be represented at different levels to accommodate various operator skill levels.

The EOPs are reviewed as part of the human factors engineering verification and validation, including monitoring of human performance in simulator settings [1, 7]. The initial HRA, however, is often updated only when the design of the plant and HSI are mature or even complete, making it harder to take insights gained from the HRA and PRA into account in the design process.

Current HRA software tools, such as the EPRI HRA Calculator [8], are designed to facilitate a standardized approach to HRA. However, they are not integrated into the EOP design process, thus not serving early feedback from HRA to the EOP designer.

The basic principle for the quantification of human errors in many HRA methods is to assign a basic human error probability (BHEP) to the human failure event and then adjust it using PSFs [9, 10]. The case study in this paper uses the Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) method [11], which uses a generic error rate of 0.001 per occurrence for action, and 0.01 for diagnosis, modified to account for eight PSFs and dependence. The SPAR-H PSFs are available time, stress and stressors, experience and training, complexity, ergonomics (including the human-machine interface), procedures, fitness for duty and work processes [11].

The proposed eMHRA methodology to be introduced in the next section uses the activity diagram of the Unified Modelling Language (UML) to define the EOP metamodel. UML is a standardized open language for defining models. It is widely used in the software engineering domain, but it has also been utilized in other engineering fields [12].

1. Methodology

The eMHRA method presented here develops a method of connecting the development of EOPs and the HRA portion of a PRA model in the early phases of complex system design. The first step in the method is the development of a simple EOP metamodel with additional HRA metadata. The specification of this metamodel allows the modeling of specific EOPs. The PSFs of the selected HRA method are analyzed in two groups. The first group holds the PSFs that are considered EOP-wide and the second group contains PSFs which are EOP step-specific. A set of rules is defined to guide the early estimation of the PSF levels.

During the development of the EOP, the developer adds the PSF information (PSF levels and reasoning) that is known at this phase of the design of the complex system. A software tool can calculate an estimation of the HEP for every EOP step based on the information added by the EOP developer and aspects of the structure of the EOP. This tool is used by the EOP developer to identify EOP steps with high HEP and proceed to improve the EOP. After the EOP is considered mature, a full HRA can be performed. The safety engineer uses the HRA information present in the EOP model, edits and adds the remaining information and calculates the final HEP. Figure 1 presents the workflow of the proposed eMHRA method.



*Figure 1: Workflow of the proposed methodology. This paper focuses on the preparation and early EOP modelling phases.*

1. Case Study

In this section, the proposed eMHRA method is demonstrated using the SPAR-H method on a portion of a generic PWR. A potential operator recovery action during a specific failure scenario is being analyzed for its potential as a system failure risk mitigator. The case study follows the steps shown in Figure 1 from the methodology section of this paper.

Five out of the eight PSFs defined in the SPAR-H method were considered to be EOP step-specific. This choice, which affects the early HRA part of the EOP development workflow, should be made by an HRA expert. An expert is also needed to define rules that will guide the EOP developer to estimate the PSF levels and the software tool to further edit them based on the EOP structure and information. Table 1 contains the scope of the SPAR-H PSFs (EOP wide vs EOP step specific) and also the rules for the automatic processing of the EOP.

*Table 1: Case Study PSFs*



The EOP metamodel is described as an UML activity diagram. A UML profile was developed to add the necessary HRA-related metadata to the data model. The SPAR-H analysis is split into two parts, one related to diagnosis and one related to action. Separate stereotypes were developed for the action and diagnosis HRA parts. The information which is related to EOP-wide PSFs is contained into stereotypes which can be applied to the initial node of the activity diagram. The information related to step-specific PSFs is contained into stereotypes which can be applied to the action and decision elements of the activity diagram. Figure 2 shows a stereotype defining the additional HRA-related information needed to be added to an EOP step element that are related to EOP step diagnosis-specific HRA.

An example EOP was modelled using the proposed metamodel. This model contains the basic elements of a typical EOP including: decisions, actions, loops and parallel processes. While the example shown here is generic and intentionally contains no specific decisions or defined actions to prevent the use of the generic case study in a real plant analysis, in a real EOP development process, the EOP model will contain detailed information.

The EOP of the case study contained five parallel branches and 24 steps (decisions and actions). The Papyrus modelling tool [13] was used for modelling the EOP profile and for the development of the EOP model example. Figure 3 presents part of the EOP model.



*Figure 2: Part of the UML profile, this stereotype describes the EOP step specific early HRA metadata*

The EOP developer then applies the decision and action elements to the stereotype that contains relevant HRA-related properties. The HRA information added in this phase is the early estimation for the PSF levels while the PSF levels which cannot be estimated are considered nominal. In this example, the decision EOP steps have only a diagnosis HRA part and the action EOP steps have only action HRA part. Figure 4 contains the dialogs used by the EOP developer to enter her estimation for the action step specific PSF levels.



*Figure 3: Part of the EOP model example. The model is a UML activity diagram using the proposed early HRA profile.*

A prototype software tool was developed to assist the EOP developer as part of the methodological development presented in this paper. This tool can calculate the HEP for every EOP step using the HRA information present in the model and the rules set by an HRA expert. The EOP developer can use this tool to get an early estimation of the HEP and a short analysis for every EOP step. This information should be used to support an iterative process for improving the EOP. Figure 5 presents a screenshot of this software tool and the results that it can provide.

1. Discussion

The eMHRA method presented in this paper allows for the coupled development of a PRA model, the HRA model within the PRA model that analyzes potential operator recovery actions, and EOPs for a complex system. One of the main benefits of closely tying these related areas together in the early part of complex system design is that intelligent decisions can be made early that will impact complex system design, EOP development, and the system level risk to the complex system where large changes are relatively easy and inexpensive to make. Later in the design process where detailed EOP development, HRA modeling, and PRA modeling is conducted is an expensive and time-consuming time to discover that a critical operator recovery action has a low likelihood of being performed successfully because of the complex system’s design. By using the eMHRA method presented here, complex system designers can find potential operator actions in failure scenarios that, in spite of EOPs and other aids, will most likely not be completed successfully. This can lead to early redesign efforts or studies of potential options to mitigate the potential operator failure during an accident scenario. EOP design can also be impacted by the eMHRA method through identifying critical operator actions that require more EOP support than other, less critical operator actions.

While the software tool that was developed as part of the research presented here is effective at better developing HRA analysis for PRA models in conjunction with EOP development efforts, further development of the tool is needed to fully integrate it with existing PRA tools such as SAPHIRE is needed. The authors of this paper envision an integrated toolchain where the early modeling of complex systems, assessment of risk, analysis of HRA considerations, and development of EOPs is fully integrated. Further future work includes the automation searching for potential operator actions during failure events to determine the most effective operator actions automatically during the early phase of complex system design. Thus, significant time savings could be realized by engineers who are investigating potential mitigating actions to be included in EOPs and credited in PRA models. Acts of commission remain an unaddressed issue in the eMHRA method in this paper. In the future, a method needs to be developed that analyzes potential acts of commission that can lead to greater complex system harm than acts of omission.

1. Conclusion

The eMHRA method presented in this paper is useful to complex system engineers who are developing complex systems where operator actions can be taken to recover a system during a failure event to a nominal or safe state. EOP development is often not conducted until after major design decisions have been made. Detailed HRA analysis is often not done until after EPOs have been developed. Crediting operator actions in PRA models is not finalized until after detailed HRA analysis is complete. This can lead to operator actions either being left out of initial PRA analysis, thus potentially showing that a system has a higher risk of failure than it otherwise will when the design is complete, or operator actions being included and credited as recovery events when the operator actions are unlikely to succeed.



*Figure 1: Entry of the estimation for the action EOP step specific PSF levels*

The software tool developed by the authors can help human reliability analysts, EOP analysts, complex system designers, and risk analysis professionals to better communicate early in the complex system design process. The case study presented in this paper shows the software tool in use. Development of the tool is ongoing and an eventual release of the tool for general use is planned.



*Figure 5: Software tool which uses information from the EOP model (entered by the EOP developer and extracted by the EOP structure) to analyze the HEP for every EOP step.*

1. Aknowledgements

This research is partially supported by United States Nuclear Regulatory Commission Grant Number NRC-HQ-84-14-G-0047. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.

REFERENCES

[1] J. O’Hara, J. Higgins, S. Fleger, and P. Pieringer, “Nureg 711 (revision 3): Human factors engineering program review model,” US Nuclear Regulatory Commission, Tech. Rep., 2012.

[2] J. O’Hara, W. Brown, P. Lewis, and J. Persensky, “Nureg 700 (revision 2): Human system interface design review guideline,” US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research Washington, DC, Tech. Rep., 2002.

[3] L. Norros, L. Salo, and P. Savioja, “Operating with procedures: Literature review and research model,” VTT Technical Research Centre of Finland, Tech. Rep. VTT-R-00773-12, 2012.

[4] D. R. Wieringa and D. K. Farkas, “Procedure writing across domains: nuclear power plant procedures and computer documentation,” in Proceedings of the 9th annual international conference on Systems documentation. ACM, 1991, pp. 49–58.

[5] Y. Niwa and E. Hollnagel, “Integrated computerisation of operating procedures,” Nuclear Engineering and Design, vol. 213, no. 2, pp. 289–301, 2002.

[6] J. O’Hara, J. Higgins, W. Stubler, and J. Kramer, “Nureg/cr-6634: Computer-based procedure systems: Technical basis and human factors review guidance,” US Nuclear Regulatory Commission, Tech. Rep., 2000.

[7] J. Laarni, P. Savioja, L. Norros, M. Liinasuo, H. Karvonen, M. Wahlstrom, and L. Salo, “Conducting multistage hfe validations- constructing systems usability case,” in Proceedings of ISOFIC/ISSNP, Jeju, Korea, August 2014.

[8] “Epri hra calculator version 5.1.” [Online]. Available: http://­www.epri.com/­abstracts/­Pages/­ProductAbstract.aspx?ProductId=000000003002003149

[9] J. Forrester, A. Kolaczkowski, E. Lois, and D. Kelly, “Nureg-1842: Evaluation of human reliability analysis methods against good practices,” US Nuclear Regulatory Commission, Tech. Rep., 2006.

[10] J. Bell and J. Holroyd, “Review of human reliability assessment methods,” Health and Safety Laboratory, Derbyshire, UK, Tech. Rep., 2009.

[11] D. Gertman, H. Blackman, J. Marble, J. Byers, and C. Smith, “Nureg/cr-6883: The spar-h human reliability analysis method,” US Nuclear Regulatory Commission, Tech. Rep., 2005.

[12] J. Rumbaugh, I. Jacobson, and G. Booch, The Unified Modeling Language Reference Manual,. Pearson Higher Education, 2004.

[13] [Online]. Available: http://­www.eclipse.org/­papyrus/­

BIOGRAPHIES

Nikolaos Papakonstantinou, PhD

VTT Technical Research Centre of Finland LTD

Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT

Espoo, Finland

nikolaos.papakonstantinou@vtt.fi

Dr. Nikolaos Papakonstantinou has a diploma in Electrical & Computer Engineering from the University of Patras (Greece) and a doctorate degree in Information Technology in Automation from Aalto University (Finland). Currently he is a research scientist at VTT Technical Research Centre of Finland in the area of system modeling and simulations. He focuses on simulation and model driven approaches to system design, operation and safety assessment. Before moving to VTT, as a post-doctoral researcher at Aalto University, he focused on simulation based safety assessment of complex systems using case studies from the nuclear power production industry. He managed the IFAPROBE project, part of the Finnish Research Programme on Nuclear Power Plant Safety and was the responsible teacher for the "Managing the product life cycle" master level course. His earlier research was in the area of automation software design, mainly targeting IEC61131 and IEC61499 based controllers, with applications on machine, batch and continuous process automation control.

Markus Porthin, M.Sc. (Tech.)

VTT Technical Research Centre of Finland LTD

Vuorimiehentie 3, P.O. Box 1000, FI-02044 VTT

Espoo, Finland

markus.porthin@vtt.fi

Markus Porthin is a Senior Scientist and Risk Analyst at VTT Technical Research Center of Finland. He graduated (M.Sc. Tech) from Helsinki University of Technology from the Engineering Physics department in 2004 with a major in Operations research (oriented on risk analysis). Since 2005 he has worked at VTT mainly with risk analysis concerning many different fields of application such as maritime traffic. Since 2012 Markus has increasingly worked in the nuclear safety field, focusing on PRA, and since 2013 he has focused mainly on HRA and software reliability. He is a member of the OECD/NEA/CSNI Working Group on Risk Assessment and the HRA Society.

Bryan M. O'Halloran, PhD

Senior Reliability Engineer at Raytheon Missile Systems

1151 E Hermans Rd, Tucson, AZ 85756

Bryan.M.OHalloran@raython.com

Bryan O'Halloran is currently a Senior Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for two hypersonic missile programs. He holds a Bachelor of Science degree in Engineering Physics and a Master of Science and Doctorate of Philosophy in Mechanical Engineering from Oregon State University. His current research interests include risk, reliability, safety, and failure modeling in the early design of complex, cyber-physical systems. He is a member of the American Society of Mechanical Engineers (ASME) and the Institute of Electrical and Electronics Engineers (IEEE) and regularly attends the International Design Engineering Technical Conference (IDETC), the International Mechanical Engineering Congress and Exposition (IMECE), and the Reliability and Maintainability Symposium (RAMS).

Douglas L. Van Bossuyt, PhD

Assistant Professor at Colorado School of Mines

1500 Illinois St.

Golden, CO 80401

USA

dvanboss@mines.edu

Douglas Van Bossuyt is an assistant professor in the Mechanical Engineering Department at the Colorado School of Mines. He is also part of the faculty of the Nuclear Science and Engineering Program, and participates in the Center for Space Resources. He holds a Ph.D. in mechanical engineering from the Complex Engineered Systems Design Laboratory at Oregon State University, a M.S. in mechanical engineering from the National Center for Accessible Transportation at Oregon State University, and a HBS in mechanical engineering and HBA in international studies from Oregon State University. His current research interests include additive manufacturing, risk and reliability engineering, complex system design, functional failure modeling, design for the developing world, and prognostics and health management.

1. Presenting Author [↑](#footnote-ref-1)
2. Corresponding Author [↑](#footnote-ref-2)