Modeling of Function Failure Propagation Across Uncoupled Systems

Conference Paper · May 2015

DOI: 10.1109/RAMS.2015.7105107

CITATIONS
19

READS
120

3 authors:

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS
SEE PROFILE

Bryan O'Halloran
Naval Postgraduate School
64 PUBLICATIONS **476** CITATIONS
SEE PROFILE

Nikolaos Papakonstantinou
VTT Technical Research Centre of Finland
81 PUBLICATIONS **1,045** CITATIONS
SEE PROFILE

Modeling of Function Failure Propagation Across Uncoupled Systems

Bryan O'Halloran[1], Raytheon Missile Systems
Nikolaos Papakonstantinou, VTT Technical Research Centre of Finland
Douglas L. Van Bossuyt[2], Colorado School of Mines

Key Words: Failure Propagation, Emergent System Behavior, Probabilistic Risk Assessment, Functional Modeling, Complex Systems

SUMMARY & CONCLUSIONS

The design of modern complex engineered systems must rapidly and accurately be developed to satisfy customer needs while accomplishing required functions with a minimum number of failures. Failure analysis in the conceptual stage of design, including the propagation of failures, has expanded in recent years to account for failures in functional modeling. However, function failure propagation across uncoupled functions and subsystems has not been fully addressed; failures are known to cross these boundaries in complex systems. To address this research gap, a functional model-based geometric method of predicting and mitigating functional failure propagation across systems, which are uncoupled during nominal use cases, is presented. Geometric relationships including function location and physical properties are established between uncoupled functions to serve as failure propagation flow paths. Mitigation options are developed based upon the geometric relationships and a path toward physical functional layout is provided to limit failure propagation across uncoupled subsystems. The model-based geometric method of predicting and mitigating functional failure propagation across uncoupled engineered systems guides designers toward improved protection and isolation of cross-subsystem failure propagation. The proposed method is validated using the case study of a pressurized water nuclear reactor modeled using APROS, a first principal simulator. Results identified that the top 10 failures exceeded those of PRA in importance based on the probability of failure.

1 INTRODUCTION

Predicting and mitigating undesirable emergent behavior for complex systems is a known and significant challenge present across a variety of industries. Failure Modes and Effects Analysis (FMEA), and related analysis, exist but are generally poor at thoroughly predicting and mitigating all adverse emergent behavior. Efforts in Probabilistic Risk Assessment (PRA) have approached the issue through several methods including fire and flood event evaluations, radiation transport models, and failure propagations through fault and event trees. However, as the analysis portion of design efforts for complex systems shifts into the early stage of design, techniques are being sought that can incorporate the system's functionality. In general, methods are poorly suited for application during functional design and would require significant effort to become useful. Function Failure Modeling (FFM) efforts have examined failure propagation through functional models of systems and recently tentative work has been done to investigate failure propagation across uncoupled functions.

This paper investigates emergent behavior in complex systems by developing a method to examine failure flow propagation across uncoupled functions in functional models. By understanding the consequences of failure flows across functional boundaries, emergent complex system behaviors caused by either a system, subsystem, or by component failures can be more accurately accounted for and mitigated in the design and operation of complex systems. The method developed in this paper is applied to a large Pressurized Water Reactor (PWR) case study. Through a better understanding of emergent behavior in complex systems, plant engineers and system designers can develop safer designs that are more risk-informed than by existing methods.

2 BACKGROUND

The method presented in this paper relies upon several key areas of existing research and industry methods including complex system design, FFM, and PRA. This section reviews pertinent details of each of the key areas.

As systems increase exponentially in complexity, the design methods often employed for simple products are subsumed by design methods specifically tailored for highly complex systems [1, 2]. One method of system modeling that is often used in the design and assessment of complex systems is functional modeling [3]. A functional model is a representation of a system decomposed to the functional level which addresses what the system does [1]. Individual functions can perform one of a number of well-defined actions on energy, material, or signal flows [4]. Flows transmit energy, material, or signals between functions. Functions, and flows between functions, are modeled assuming a nominal system state and configuration. Under standard functional modeling techniques, functions that are not coupled by flows during nominal system operations are not modeled as being coupled even when in a failed state where potential coupling across functional

[1] Presenting author
[2] Corresponding author

boundaries could occur [5]. Three methods begin to address the issue of modeling failure flows that propagate between nominally uncoupled functions including Function Failure Identification Propagation (FFIP), Function Failure Design Method (FFDM), and a new geometric method of examining fault propagations across uncoupled functions [6].

The first methodology, FFIP, was developed to assess the health of functions (i.e., the functional model) within a system by propagating failures using the connections in the functional model [3, 7]. FFIP predicts failure propagation in cases where failure flows across functional boundaries are not anticipated. The second methodology, FFDM, provides a mathematical relationship between nominal function modes and failure modes for use in design. FFDM is used in the conceptual stage of design and allows Failure Modes and Effects Analysis (FMEA)-style failure analysis to be conducted from functional models of the conceptual system. While FFDM has the benefit of finding potential failures from a wide variety of individual functional solutions of a system, emergent system failure behaviors that cross functional boundaries are not explicitly examined [8, 9, 10, 11]. The third methodology examines failure flows across uncoupled functions and relies upon physical geometric location information of functions in a functional model. The method is used to develop a new geometric arrangement that mitigates risks identified from the method. However, no attempt is made to integrate the method with PRA or other existing methods, and calculating failure probabilities to determine order of importance for addressing failure flows is only briefly mentioned. The methodology also was entirely done by hand [6].

PRA is a well-established field of risk assessment used in a variety of industries including the civilian nuclear power, aerospace, and petroleum. In PRA, a system failure model is built from event trees and fault trees where event trees document possible accident progressions from initiating events and fault trees provide detailed probabilistic information of individual subsystems and components failing to mitigate accident sequences. Within PRA, emergent system behavior during failure events is modeled using specific methodologies targeted at fire and flooding events that impact specific rooms or areas of a plant or facility [12, 13, 14, 15, 16, 17, 18, 19]. These assessments are used to identify common cause failures that result from a room or zone of a plant being destroyed by fire or submerged by flood. Emergent system behaviors are sometimes identified by fire and flood analysis, although not all combinations of potential failure flow across functional or system boundaries are discovered during fire and flood analysis [20, 13, 21, 22].

Common cause failure events occur when more than one component or function in a system fails due to a common cause. Fire and flood are often intrusive enough to become common cause failures. Other examples include toxic, explosive, or radioactive gas clouds; hard rock or salt mine tunnel collapse; meteor, space debris, and airplane impacts; and shrapnel from rotating equipment. Several methods linking common cause failures to functional modeling have been recently developed [23, 24, 25, 26, 27, 28, 29, 30].

3 METHODOLOGY AND CASE STUDY

The method presented in this paper is comprised of six steps. Each of these steps are explained in this section and are provided with a case study. By following the methodology, room-level failure flows that cross functional boundaries can be identified and the probability of failure propagation along the uncoupled failure flow path can be determined.

In order to illustrate the method, a case study derived from a pressurized light water reactor spent fuel pool cooling system is presented. Plant layout and configuration data was graciously supplied by Fortum Power and Heat. The system uses two redundant Main Cooling System (MCS) loop trains labeled MCS-A and MCS-B, and one Emergency Cooling System (ECS) to control the spent fuel pool temperature. These systems are connected to the Pools A and B. During normal plant operations, the spent fuel pool temperature is kept at safe levels using only one MCS loop. The case study presented in this paper is limited to Room B3, shown in the Piping and Instrumentation Diagram (P&ID) in *Figure 1*, and was selected as the focus of the case study because it contains several key automation and process components of the two primary cooling systems. A list of the components and component locations of MCS-A and MCS-B in Room B3, can be found in Table 1.

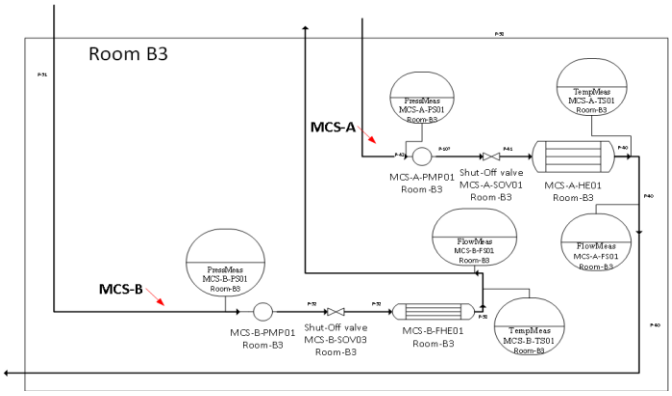

Figure 1: Room B-3, Spent Fuel Pool Pump and Heat Exchanger Room P&ID

Component ID	Component type	X,Y,Z Coordinates (m)
MCS-A-PS01	Pressure sensor	1.5,5,1
MCS-A-PMP01	Pump	2.5,5,1
MCS-A-SOV01	Shutoff valve	4,5,1
MCS-A-HE01	Heat exchanger	6,5,1
MCS-A-TS01	Temperature sensor	8,5,1
MCS-A-FS01	Flow sensor	8.5,5,1
MCS-B-FS01	Flow sensor	8.5,2,1
MCS-B-HE01	Heat exchanger	6,2,1
MCS-B-SOV03	Shut-off valve	4,2,1
MCS-B-PMP01	Pump	2.5,2,1
MCS-B-PS01	Pressure sensor	1.5,2,1
MCS-B-TS01	Temperature sensor	8,2,1

Table 1: Component List and Location within Room B-3

Step 1 of the methodology is the creation of a functional model from the P&ID of the system(s) of interest. In the model, functions should be modeled to the level where adequate functional detail is present and can provide meaningful results. A functional model of MCS-A in Room B3 can be found in *Figure 2*. Note that the functional model of MCS-B is identical save for labeling of components that are mapped to functions.

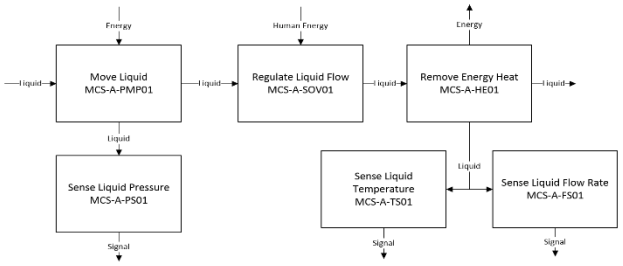

Figure 2: Functional Model of MCS-A

Step 2 requires the development of failure flow information for 1) potential failure flows that can be emitted from or pass through functions (i.e., output ports), 2) failure flows that can be accepted by functions (i.e., input ports), and 3) failure flow distance information. This information is populated into a database with probability information detailing the probability of a failed function exporting a failure flow along an uncoupled flow path, the probability of a failure flow traveling specific physical distances between functions, and the probability of a failure flow causing a function to go to a failed state. For example, a failed heat exchanger with a leak may cause water to spray onto a pump in a separate train, thus causing the pump to fail. Probabilities associated with the heat exchanger failure, the water traveling to the pump over the distance between the two components, and the pump failing due to the water determine the likelihood that the heat exchanger failure will cause a pump failure in a separate cooling loop train. Physical component location information is mapped to the functional representations of the components in order to assign propagation probability on a per unit length basis. In the heat exchanger and pump example, as the pump is moved farther away from the heat exchanger, the probability of water from the leak reaching the pump decreases.

Step 3 uses FFIP to determine failure flows along nominal flow paths. Detailed information on FFIP is available in Kurtoglu & Tumer, 2008 [7]. Due to there being no redundant functions or flow paths within the individual MCS trains, the case study omits this step.

Step 4 uses an Uncoupled Failure Flow State Reasoner (UFFSR) developed as part of the research presented in this paper to determine which failed functions will propagate failure flows to other uncoupled functions. An example of an uncoupled failure flow is water flowing from a failed shutoff valve in one MCS train to a pump in the other MCS train, thus failing both the MCS trains. *Figure 3* shows the graphical user interface (GUI) of the UFFSR.

Step 5 analyzes the uncoupled failure flow paths found using the UFFSR and failure flow paths found using FFIP with initiating event information. Probabilities developed in Step 2 are used to determine system failure probabilities. Then, as with normal PRA procedures, various failure scenarios can be analyzed and the overall probability of system failure can be determined. Table 2 shows the results for Room B3 where system failure is defined as both MCS-A and MCS-B being in a failed state.

Step 6 combines the uncoupled failure flow information generated in this method with standard PRA analysis cut sets. Failures that cross functional boundaries may then be found that are of high priority for mitigation or monitoring efforts that otherwise would not have likely been discovered through PRA analysis.

Two tables are presented here that summarize the findings of the proposed method. Table 2 represents the results from the proposed method while Table 3 shows the top ten cut sets of a simplified PRA study of Room B3.

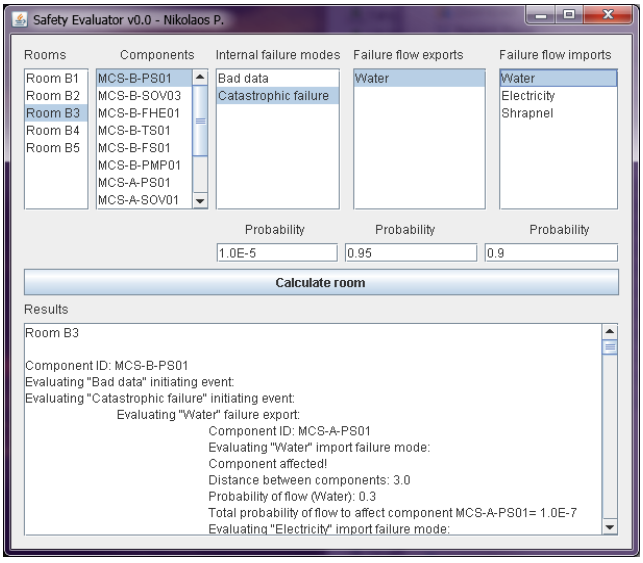

Figure 3: UFFSR GUI

Prob/Freq	Total %	Top 10 UFFSR Cut Sets
1.38E-08	100	
2.85E-09	20.64	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_LIQUID,MCS-B-PMP01
2.56E-09	18.55	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_LIQUID,MCS-B-PS01
1.42E-09	10.30	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-PS01
1.34E-09	9.71	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-HE-01

1.29E-09	9.36	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_LIQUID,MCS-B-TS01
1.21E-09	8.74	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_LIQUID,MCS-B-FS01
1.00E-09	7.24	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-PMP01
7.45E-10	5.40	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-SOV01
7.18E-10	5.20	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-TS01
6.71E-10	4.86	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,EXPORT_SOLID,MCS-B-FS01

Table 2: Top 10 cut sets from UFFSR tool of Room B3

Prob/Freq	Total %	Cut Sets
1.35E-10	100	Total of 240 Cut Sets. Dsply. Top 10.
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,MCS-B-PMP01-FTR
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-SOV03-HE,MCS-B-PMP01-FTR
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-HE-01-PLG,MCS-B-PMP01-FTR
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,MCS-B-SOV03-HE
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-SOV03-HE,MCS-B-SOV03-HE
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-HE-01-PLG,MCS-B-SOV03-HE
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-PMP01-FTR,MCS-B-HE-01-PLG
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-SOV03-HE,MCS-B-HE-01-PLG
1E-11	7.41	IE_ELECT_LOSS_TRAIN_A,MCS-A-HE-01-PLG,MCS-B-HE-01-PLG
1E-12	0.74	IE_ELECT_LOSS_TRAIN_A,MCS-A-SOV03-CAT,MCS-B-PMP01-FTR

Table 3: Top 10 cut sets from PRA model of Room B3

4 DISCUSSION

The case study in this paper is useful for demonstrating the methodology, which focuses on uncoupled failure flows (e.g., such as water from a leak traveling between two uncoupled systems) that would only be found in careful, specialized PRA analysis. In a more complex analysis of an entire plant, previously undiscovered uncoupled failure flows resulting in catastrophic system failures are expected to be found. These emergent system failure modes are often not identified in standard PRA analysis. The results in Table 3 show that a large quantity of cut sets are identified using PRA. However, failure flows that cross functional boundaries are not identified or are identified only as low importance failure events. In comparison, the cut sets identified in Table 2 are dominated by uncoupled failure flows not seen in Table 3. Additionally, the probabilities attached to the uncoupled failure flows are more accurate as compared to the estimation of common cause failures (e.g.: flooding, fire) used in PRA. With this information, a better understanding of potential failure scenarios becomes available for the practitioner to determine where new areas of mitigation can be employed to reduce overall plant risk.

PRA is a well-known analysis tool that provides valuable risk findings used by a variety of industries. The method presented in this paper provides additional failure insights not typically available from PRA. The method in this paper has the additional advantage of being automated by using the UFFSR simulation tool developed by the authors. This allows for an improved capability of finding previously unknown failure propagation paths. From the case study presented in this paper, the top ten results (Table 2) have a higher probability than those found from the PRA. Further, these results were altogether missed or minimized by the PRA and therefore cannot be effectively evaluated during the plant's life cycle.

5 CONCLUSION AND FUTURE WORK

The method presented in this paper focuses on the improvement of finding failure flows that propagate across uncoupled functions in complex systems. Results are compared to PRA and show a strong case for the inclusion of this method when performing PRA. In the case study, many potential failure scenarios that would disable both cooling system loops were missed or minimized in importance by the PRA but were discovered by the method and the UFFSR tool.

While at the current maturity of this research, the method presented compliments PRA, future work will develop the method in a more comprehensive solution to determine a larger set of failures. In doing this, only a single analysis would need to be performed rather than combining with PRA results.

Additional future work includes developing the method into a design tool. Currently the method does not address mitigation of failures and propagation paths. The future work will optimize component location, and the addition of components, such that failures are mitigated; especially those crossing normally uncouple functional boundaries. Since the current method ties well into functionality, the future work will mesh well with systems engineering approached for design. A better understanding of the feedback loop between sensors, electrical control systems, and actuators may also be achieved through further expansion of this method.

6 ACKNOWLEDGEMENTS

The authors wish to thank Fortum Power and Heat for providing plant P&ID drawings and other relevant information. 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] R. B. Stone and K. L. Wood, "Development of a Functional Basis for Design," vol. 122, 2000.

[2] D. L. Van Bossuyt, I. Y. Tumer and S. D. Wall, "A case for trading risk in complex conceptual design trade studies," Research in Engineering Design, vol. 24, no. 3, pp. 259-275, 2013.

[3] D. Jensen, T. Kurtoglu and I. Y. Tumer, "Flow State Logic (FSL) for Analysis of Failure Propagation in Early Design," in ASME International Design Engineering Technical Conference IDETC/CIE, San Diego, CA, 2009.

[4] J. Hirtz, R. Stone, D. McAdams, S. Szykman and K. Wood, "A Functional Basis for Engineering Design: Reconciling and Evolving Previous Efforts," Research in Engineering Design, vol. 13, no. 2, pp. 65-82, 2002.

[5] I. Y. Tumer and R. B. Stone, "Mapping Function to Failure Mode During Component Development," Research in Engineering Design, vol. 14, no. 1, pp. 25-33, 2003.

[6] I. Ramp and D. L. Van Bossuyt, "Toward an Automated Model-Based Geometric Method of Representing Function Failure Propagation Across Uncoupled Functions," in ASME International Mechanical Engineering Congress and Exposition IMECE, Montreal, Canada, 2014.

[7] T. Kurtoglu and I. Y. Tumer, "A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems," ASME Journal of Mechanical Design, vol. 130, no. 5, 2008.

[8] M. Stock, R. B. Stone and I. Y. Tumer, "Going Back in Time to Improve Design: The Function-Failure Design Method," in ASME Design Engineering Technical Conference DTM, Chicago, Il, 2003.

[9] K. G. Lough, R. B. Stone and I. Y. Tumer, "Function Based Risk Assessment: Mapping Function to Likelihood," in ASME International Design Engineering Technical Conference DET, Long Beach, CA, 2005.

[10] M. Stock, R. B. Stone and I. Y. Tumer, "Linking Product Functionality to Historic Failure to Improve Failure Analysis in Design," Research in Engineering Design, 2005.

[11] R. A. Roberts, R. B. Stone and I. Y. Tumer, "Deriving Function-Failure Information for Failure-Free Rotocraft Component Design," in ASME Design Engineering Technical Conference DETC, Montrea, Canada, 2002.

[12] M. Stamatelatos and D. Homayoon, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA, 2011.

[13] US Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Severe Accidents (NUREG-0800, Chapter 19)," US NRC, 2012.

[14] D. L. DeMott, "PRA as a Design Tool," in Reliability and Maintainability Symposium (RAMS), 2011.

[15] W. E. Vesely, "Extended Fault Modeling Used in the Space Shuttle PRA," in Reliability and Maintainability Symposium (RAMS), 2004.

[16] L. Meshkat, "Probabilistic Risk Assessment for Decision Making During Spacecraft Operations," in Reliability and Maintainability Symposium (RAMS), 2009.

[17] L. L. Lydia, A. J. Ingegneri, L. Ming and D. F. Everett, "Probabilistic Risk Assessment: A Practical and Cost Effective Approach," in Reliability and Maintainability Symposium, 2007.

[18] J. Zamanali, "Probabilistic Risk Assessment Applications in the Nuclear Power Industry," IEEE Transactions on Reliability, vol. 47, no. 3, 1998.

[19] T.-Y. Hsiao and C.-N. Lu, "Risk Informed Design Refinement of a Power System Protection Scheme," IEEE Transactions on Reliability, vol. 57, no. 2, pp. 311-321, 2008.

[20] C. Dunglinson and H. Lambert, "Interval Reliability for Initiating and Enabling Events," IEEE Transactions on Reliability, vol. 32, no. 2, pp. 150-163, 1983.

[21] M. Garvey, F. Joglar and E. P. Collins, "HRA for Detection and Suppression Activities in Response to Fire Events," in Reliability and Maintainability Symposium (RAMS), 2014.

[22] US Nuclear Regulatory Commission, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants (NUREG/CR-2300)," US NRC, 1983.

[23] S. Sierla, B. O'Halloran, T. Karhela, N. Papakonstantinou and I. Y. Tumer, "Common Cause Failure Analysis of Cyber-Physical Systems Situated in Constructed Environments," Research in Engineering Design, vol. 24, no. 4, pp. 375-94, 2013.

[24] M. Myrsky, H. Nikula, S. Sierla, J. Saarinen, N. Papakonstantinou, V. Kyrki and B. O'Halloran, "Simulation-Based Risk Assessment of Robot Fleets in Flooded Environments," in IEEE Conference on Emerging Technologies and Factory Automation (ETFA), 2013.

[25] N. Papakonstantinou, S. Sierla, D. C. Jensen and I. Y. Tumer, "Simulation of Interactions and Emergent Failure Behavior During Complex System Design," Journal of Computing and Information Science in Engineering, vol. 12, no. 3, 2012.

[26] R. P. Hughes, "A New Approach to Common Cause Failure," Reliability Engineering, vol. 17, no. 3, pp. 211-236, 1987.

[27] K. N. Fleming, A. Mosleh and R. K. Deremer, "A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models," Nuclear Engineering and Design, vol. 93, no. 2, pp. 245-273, 1986.

[28] W. E. Vesely, "Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin Specalizations," Nuclear Systems Reliability Engineering and Risk Assessment, pp. 314-341, 1977.

[29] H. W. Lewis, R. J. Budnitz, W. D. Rowe, H. C. Kouts, F. Von Hippel, W. B. Loewenstein and F. Zachariasen, "Risk Assessment Review Group Report to the US Nuclear Regulatory Commission," IEEE Transactions on Nuclear Science, vol. 26, no. 5, pp. 4686-4690, 1979.

[30] Idaho National Engineering and Environmental Laboratory, "Common-Cause Event Failure Insights NUREG/CR-6819," 2003.

BIOGRAPHIES

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 Reliability Engineer at Raytheon Missile Systems and the Lead Reliability Engineer for the Paveway™ Laser Guided Bomb. 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).

Nikolaos Papakonstantinou, PhD
VTT Technical Research Centre of Finland
Espoo, Finland
nikolaos.papakonstantinou@vtt.fi

Dr. Nikolaos Papakonstantinou has a diploma in Electrical & Computer Engineering from the University of Patras (Greece, 2008) and a doctorate degree in Information Technology in Automation from Aalto University (Finland, 2012). 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. Earlier, 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. He has also done research on automation software design, using IEC61131 and IEC61499 based controllers, with applications on machine, batch and continuous process automation control.

Douglas L. Van Bossuyt, PhD
Assistant Professor at the Colorado School of Mines
1500 Illinois St. Golden CO 80401
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, design for the developing world, and prognostics and health management.