A System Design Method to Reduce Cable Failure Propagation Probability in Cable Bundles

Article · February 2019

CITATIONS
0

READS
61

3 authors:

Douglas Lee Van Bossuyt
Naval Postgraduate School
66 PUBLICATIONS **168** CITATIONS
SEE PROFILE

Bryan O'Halloran
Naval Postgraduate School
48 PUBLICATIONS **108** CITATIONS
SEE PROFILE

Nikolaos Papakonstantinou
VTT Technical Research Centre of Finland
47 PUBLICATIONS **254** CITATIONS
SEE PROFILE

A System Design Method to Reduce Cable Failure Propagation Probability in Cable Bundles

Douglas L. Van Bossuyt
Bryan M. O'Halloran
Nikolaos Papakonstantinous

Summary & Conclusions

This paper presents a method of assessing cable routing for systems with significant cabling to help system engineers make risk-informed decisions on cable routing and cable bundle management. We present the Cable Routing Failure Analysis (CRFA) method of cable routing planning that integrates with system architecture tools such as functional modeling and function failure analysis. CRFA is intended to be used during the early conceptual stage of system design although it may also be useful for retrofits or overhauls of existing systems.

While cable raceway fires, cable bundle severing events, and other common cause cable failures (e.g., rodent damage, chemical damage, fraying and wear-related damage, etc.) are known to be a serious issue in many systems, the protection of critical cabling infrastructure and separation of redundant cables is often not taken into account until late in the systems engineering process. Cable routing and management often happens after significant system architectural decisions have been made. If a problem is uncovered with cable routing, it can be cost-prohibitive to change the system architecture or configuration to fix the issue and a system owner may have to accept the heightened risk of common cause cable failure. Given the nature of cables where energy and signal functions are shared between major subsystems, the potential for failure propagation is significant.

Through a more complete understanding of power and data cabling requirements during system architecting, a system design can be developed that minimizes the potential for collocation of critical cable infrastructure. Reductions in critical cabling collocation may lead to a reduction in potential failure propagation pathways. The CRFA method presented in this paper relies on functional failure propagation probability calculation methods to identify and avoid potential high-risk cable routing choices. The implementation of the CRFA method may help system engineers to design systems and facilities that protect against cabling failure propagation events (cable raceway fires, cable bundle severing events, etc.) during system architecture. Implementing CRFA in the system architecture phase of system design may help practitioners to increase system reliability while reducing system design costs and system design time.

1. Background

The CRFA method presented in this paper relies upon several key areas of existing research and industry methods including complex system design, Functional Failure Modeling (FFM), and Probabilistic Risk Assessment (PRA). The important aspects of each area necessary to understand and make use of the CRFA method are reviewed in this section.

With increasing system complexity, design methods used for relatively simple product design are replaced by design methodologies specifically suited for complex systems [1, 2]. Functional modeling is often used in the early conceptual phase of system design (generally referred to as system architecture although this definition is not universally accepted) [3]. Functional models represent basic system functions and the basic flows of information, material, or energy transferred between individual functions and through the system boundary [1]. Individual functions perform actions on energy, material, or information flows [4]. Functional modeling as generally practiced in system architecting efforts often only analyzes nominal system configurations and states. Extensions to functional modeling have been developed over the last decade to analyze potential failure propagation paths and determine mitigation strategies [5]. Function Failure Identification Propagation (FFIP) was developed to model failure flows propagating through system functions and the resulting system-level failure outcomes [3, 6]. FFIP can be used to predict failure propagation paths and failure outcomes. However, FFIP cannot account for failures that cross functional boundaries or most common cause failures. The Function Failure Design Method (FFDM) provides a Failure Modes and Effects Analysis (FMEA)-style failure analysis tool to be used with functional modeling [7, 8, 9, 10]. FFDM can be used to find a large variety of potential failure modes for individual functions but FFDM cannot analyze failure propagations across non-nominal flow paths or common cause failure events. The Uncoupled Failure Flow State Reasoner (UFFSR) was developed to address the issue of analyzing uncoupled failure flow propagation in FFM [11, 12]. The UFFSR provides a geometric basis for analyzing failure flow propagation across uncoupled functions. An extension of UFFSR was developed to model failure flow arrestor functions in functional modeling. The Dedicated Failure Flow Arrestor Function (DFFAF) method replicates placing physical barriers between redundant systems to prevent a failure in one system from crossing an air gap to the other system [13]. Other methods such as Function Flow Decision Functions (FFDF) [14], a

method of developing prognostic and health management systems via functional failure modeling [15], the Time Based Failure Flow Evaluator (TBFFE) method [16], and methods to understand potential functional failure inputs to systems that are hard to predict [17] have added additional capabilities to FFM in an effort to develop a more complete FFM toolbox for practitioners.

PRA is a well-established discipline of risk analysis with over 50 years of heritage for complex systems used in a variety of industries including aerospace, petroleum, automotive, and civilian nuclear power, among other areas. System failure models are developed using event and fault trees where event trees generally show the progression of a failure through systems and fault trees generally show the progression of failure within systems. Probabilistic failure data is attached to basic failure events and through Bayesian statistical methods and Boolean algebra, a probabilistic system failure rate can be calculated. However, PRA in its basic form does not capture emergent system behavior during failure events. Instead, specific methodologies are used to assess specific emergent system behavior such as during fire or flood events in civilian nuclear reactors [18, 19, 20, 21, 22, 23, 24, 25]. While many emergent system behaviors are identified by fire and flood analysis, other emergent system behaviors can remain hidden from analysts [26, 19, 27, 28].

Common cause failure in particular has had significant attention paid over the course of PRA methodological development. Failure inducing events such as maintenance errors across a series of identical, redundant valves can lead to a common cause failure of all maintained valves. Fire and flood events often can become common cause failures, causing failure of every system in a specific area of a system. Other examples include explosive, toxic, or radioactive gas clouds; salt mine or hard rock tunnel collapse; airplane, space debris, meteor, and other impacts; and explosive deconstruction of rotating turbomachinery sending out shrapnel. Several methods have recently been developed to address common cause failure in functional modeling [29, 30, 31, 32, 33, 34, 35, 36]. However, no method currently exists in the FFM toolbox to address the issue of common cause failure events destroying or disabling multiple cables routed through the same cable pathways, ducts, raceways, bulkhead or wall penetrations, or other cable routing methods. Most efforts in cable management to prevent common cause failures focus on separating redundant and backup system cabling; isolating control, motive power, and instrumentation cabling from one another; and ensuring adequate breaker coordination to prevent ground fault wire ignition events in cable raceways. These efforts are typically performed after system architecting efforts have been completed and ignore potential benefits of analyzing and planning cable routing and bundling in the early phases of design.

2. Methodology & Case Study

The CRFA method presented in this section provides practitioners a useful method to develop a better understanding of cable routing and management during system architecture from a risk-based perspective. This section details the CRFA methodology and presents a case study of cable routing in a simplified Pressurized Water Reactor (PWR) nuclear power plant primary coolant loop pumping room where three redundant pumping systems are co-located. Two pumps are required to be active at all times for proper core cooling with the third pump acting as a "swing" pump for maintenance purposes or coming online during a failure

CABLE GROUPS
Cable group: Group331
CONTROL_SIGNAL_2
POWER_BUS_1
POWER_BUS_2
POWER_BUS_3
Group failure probability: 0.0077
System fails: true
Cable group: Group415
CONTROL_SIGNAL_3
POWER_BUS_1
POWER_BUS_2
POWER_BUS_3
Group failure probability: 0.0077
System fails: true
Cable group: Group252
CONTROL_SIGNAL_2
CONTROL_SIGNAL_3
POWER_BUS_1
POWER_BUS_2
Group failure probability: 0.0074
System fails: true

Table 1: Representative CRFA results including cable groupings with highest system failure probabilities for the primary coolant loop pumping room case study.

event involving one of the other pumps.

Step 1 of the CRFA method is to develop a functional model. Figure 1 shows the functional model of the pump room.

Step 2 involves calculating the system failure probabilities and failure flow paths using FFIP or other related FFMs as desired. Here we use FFIP to calculate the failure rate of the system. In the case study, the system failure rate is calculated using FFIP at 5.3E-4/yr.

Step 3 associates failure probabilities with individual cables failing leading to a potential common cause failure event of all co-located cables. A practitioner used to the FFIP methodology can think of this step as adding another functional block into the functional model to represent a cable, rather than using a functional flow to represent the transmission of signal, energy, or material. For those who are more familiar with PRA, this is similar to adding a basic event of a common cause failure to a fault tree. For the purposes of the case study presented to illustrate CRFA method presented here, cables are defined as any electrical physical conveyance device which is generally referred to as a cable, wire, conductor, etc. The authors have found that CRFA can also be used with optical cables, pneumatic and hydraulic hoses and hard piping, and some bulk material transport systems (e.g., conveyor belts, pneumatic tubes, slurry chutes, etc.). In the case study, individual cable failure rates were chosen from an appropriate and proprietary generic cabling failure database.

Step 4 determines all possible cable groupings. In this step, the practitioner can identify any specific cables that cannot be located next to other cables for regulatory or other reasons, and any specific cables that must be co-located. For example, if three cables are being analyzed, there are nine total possible cable combinations. The case study has a total of 12 cables with 516 possible combinations.

Step 5 analyzes system failure probability when two or more cables are co-located in a raceway. The cable failure probabilities from Step 3 are used to determine if all cables in a cable bundle may fail simultaneously. FFIP is run with each potential cable grouping identified in Step 4. Results for each cable grouping are kept separate and rank ordered from highest to lowest system failure probability.

Step 6 sets the maximum threshold for system failure probability. The authors advise that the threshold be set above the base FFIP calculation as FFIP does not generally take into account common cause cable failure. Then all cable groupings that exceed the threshold value are marked as unaccept-

able configurations from a risk perspective. All cable groupings that were not marked as unacceptable configurations are thus acceptable from a risk perspective and can be used, assuming no other mitigating circumstances, in physical system design. If no cable configuration is acceptable, this indicates a redesign of the functional model is needed. Additional redundant systems or redundant cables may also be warranted. Table 1 presents partial results from the case study where a total of 516 potential cable groupings were identified, 210 groupings were rejected due to co-location exclusions (Step 4), and 313 groupings were eliminated due to exceeding the maximum threshold set in Step 6, resulting in 38 potential cable routing configurations meeting all criteria identified in the CRFA method.

The CRFA method is now complete. Periodically through the rest of the conceptual design phase, CRFA should be re-run to verify that appropriate cable groupings and separations are maintained to meet failure probability expectations. When moving from system architecture and early system design into physical system design and layout, the information from CRFA can then be used to develop cable raceways and locate individual cables.

3. Discussion

The CRFA method presented in the previous section has been implemented in software and automated. Figure 2 presents the Graphical User Interface (GUI) of the CRFA software tool that the authors developed. The case study in this paper was prepared using the software implementation of CRFA. In the future, the CRFA software is slated for integration with a larger effort to develop a complete FFM software toolkit.

In the authors' experience, evidence of the success of CRFA can often be seen in redundant systems cabling being isolated from one another. Often this is because of Step 4 identifying cables that cannot be co-located. However, the authors have observed CRFA identifying on its own that redundant system cabling should not be co-located due to increased system failure probability. It is also possible that if the maximum threshold set in Step 6 is sufficiently high, redundant system cabling isolation may not be observed. This is potentially indicative of too high of a threshold being set or may also indicate that redundant system cabling is unnecessary. It is recommended that further review of the results and a deeper understanding of why certain cables are more or less isolated is sought before moving forward if either case is identified.

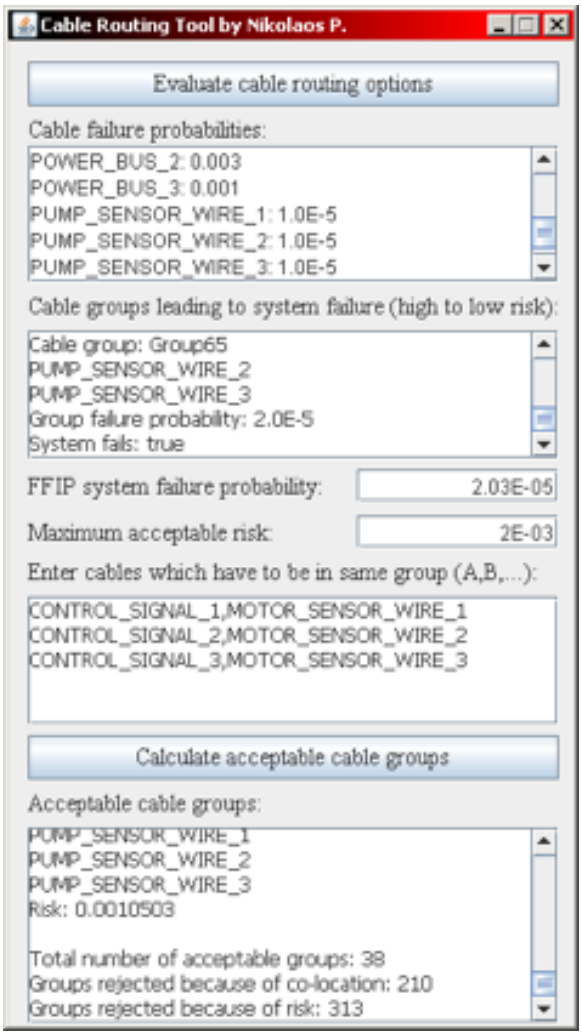

Figure 2: The GUI of the software implementation of CRFA.

While small-scale cable routing studies can be conducted using PRA tools and larger complex system cable routing analysis can be performed using specialized methods, the method presented in this paper integrates cable routing failure analysis with other FFMs, allowing a more holistic and integrated approach to system risk analysis. CRFA also provides the capability of analyzing common cause cable failures much earlier in the system design process during system architecture than existing methods allow. Shifting the analysis of common cause failures from cable routing to earlier in the system design process may save both time and money in the design process.

In the case where PRA is used to analyze cable failures without analyzing fire, flood, or missile (turbomachinery shrapnel) common cause failure, the PRA results will likely underestimate failure probability. Even when analyzing the fire, flood, or missile common cause failure sources, the results will likely not present as full and accurate of a picture of cable grouping failure risks as CRFA does.

CRFA has been used to conduct analysis on a variety of systems including civilian nuclear power plants of several types, aerospace systems, automotive systems, and defense systems. The results are promising and have been useful for practitioners to understand how cable routing and management can be greatly impacted by system architectural decisions. Feedback from some users of CRFA indicate a desire for CRFA to be integrated into commonly used model based systems engineering (MBSE) tools.

Further development of CRFA is anticipated including a more nuanced approach to cable bundling. CRFA assumes that all cables co-located in a raceway will all fail simultaneously when a common cause failure event occurs. However, not all common cause failure events will cause all cables to fail. For instance, a very hungry rat will not simultaneously eat through all data cables in a large bundle. A potential extension of CRFA may be to include aspects of TBFFE in the modeling of cable bundle failures to represent failure of cables in a bundle over time. Thus, CRFA is a conservative method in this regard. Another area of future improvement for CRFA is integrating the method with uncoupled failure flow methods such as UFFSR. Uncoupled failure flows can be accounted for to some degree in Step 3 by assigning failure probabilities for common cause cable failures from potential uncoupled sources such as missiles or floods (of cable insulation-eating liquids). However, some sources of uncoupled failure flow may be missed without integration of UFFSR.

Further future work includes adding the ability to the software implementation of CRFA to automatically add redundant cabling. For instance, civilian nuclear power plants often contain three redundant sensors with three redundant cables where a functional model may only show one functional block to represent the three redundant sensors and cables. Additional automation may provide the practitioner with a more rapid development process.

4. Conclusion

The CRFA method presented here provides a novel way of analyzing cable routing and determining cable routing schemes that are below a desired system failure probability threshold. Protecting critical cabling infrastructure and separating redundant cables is vitally important to ensuring that a common cause failure does not cause a system-level failure event. Cable routing and planning currently happens late in the design process after major architectural decisions have been made and during physical system design. The CRFA method brings the analysis and

design of cable raceways and cable separation to the system architecting phase of system design using FFM as a basis for further analysis. By having a more complete understanding of cable requirements during the early phases of system design, a system architecture and design can emerge that minimizes critical cabling infrastructure co-location and identifies the need for additional redundant cabling needs. Implementing CRFA may help engineering practitioners design complex systems and facilities that guard against cable failure propagation events that could disable or destroy the core functionality of the system. Thus, system reliability is expected to be increased while driving down system risks that may otherwise have gone unaddressed.

5. Acknowledgements

This research was partially supported by United States Nuclear Regulatory Commission Grant Number NRC-HQ-84-14-G-0047 and by the Naval Postgraduate School. 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. The case study or example presented in this paper may not be used or construed as an analysis of a specific system or plant and is only provided for illustrative purposes of the method.

References

1. R. B. Stone and K. L. Wood, "Development of a Functional Basis for Design," ASME Journal of Mechanical design, vol. 122, no. 4, pp. 359-370, 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. 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.
7. 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.
8. 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.
9. 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.
10. 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, Montreal, Canada, 2002.
11. 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.
12. Bryan M. O'Halloran, N. Papakonstantinou and D. L. Van Bossuyt, "Modeling of Function Failure Propagation Across Uncoupled Systems," in Reliability and Maintainability Symposium (RAMS), Palm Harbor, FL, 2015.
13. M. R. Slater and D. L. Van Bossuyt, "Toward a Dedicated Failure Flow Arrestor Function Methodology," in ASME International Design Engineering Technical Conference and Computers in Information Conference, Boston, MA, 2015.
14. A. R. Short and D. L. Van Bossuyt, "Rerouting Failure Flows Using Logic Blocks in Functional Models for Improved System Robustness: Failure Flow Decision Functions," in ASME International Design Engineering Technical Conference and Computers and Information in Engineering Conference, Boston, MA, 2015.
15. G. L'Her, D. L. Van Bossuyt and B. M. O'Halloran, "Prognostic systems representation in a function-based Bayesian model during engineering design," International Journal of Prognostics and Health Management, vol. 8, no. 2, p. 23, 2017.
16. J. Dempere, N. Papakonstantinou, B. O'Halloran and D. Van Bossuyt, "Risk Modeling of Variable Probability External Initiating Events in a Functional Modeling Paradigm," The Journal of Reliability, Maintainability, and Supportability in Systems Engineering, 2018.
17. D. L. Van Bossuyt, B. M. O'Halloran and R. M. Arlitt, "Irrational System Behavior in a System of Systems," in IEEE System of Systems Engineering Conference, Paris, 2018.
18. M. Stamatelatos and D. Homayoon, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA, 2011.
19. 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.
20. D. L. DeMott, "PRA as a Design Tool," in Reliability and Maintainability Symposium (RAMS), 2011.
21. W. E. Vesely, "Extended Fault Modeling Used in the Space Shuttle PRA," in Reliability and Maintainability Symposium (RAMS), 2004.
22. L. Meshkat, "Probabilistic Risk Assessment for Decision Making During Spacecraft Operations," in Reliability and Maintainability Symposium (RAMS), 2009.
23. 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.
24. J. Zamanali, "Probabilistic Risk Assessment Applications in the Nuclear Power Industry," IEEE Transactions on Reliability, vol. 47, no. 3, 1998.
25. 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.
26. C. Dunglinson and H. Lambert, "Interval Reliability for Initiating and Enabling Events," IEEE Transactions on Reliability, vol. 32, no. 2, pp. 150-163, 1983.
27. 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.
28. 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.
29. 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. 375-394, 2013.
30. 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.
31. 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.
32. R. P. Hughes, "A New Approach to Common Cause Failure," Reliability Engineering, vol. 17, no. 3, pp. 211-236, 1987.
33. 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.
34. 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.
35. 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.
36. Idaho National Engineering and Environmental Laboratory, "Common-Cause Event Failure Insights NUREG/CR-6819," 2003.
37. B. M. O'Halloran, N. Papakonstantinou and D. L. Van Bossuyt, "Cable routing modeling in early system design to prevent cable failure propagation events," in IEEE Reliability and Maintainability Symposium (RAMS), 2016.