

System-Level Reliability Analysis for Conceptual Design of Electrical Power Systems

Ying Zhang and Tolga Kurtoglu

Palo Alto Research Center
Palo Alto, CA, 94304
{yzhang, kurtoglu}@parc.com

Irem Y. Tumer and Bryan O'Halloran

Oregon State University
Corvallis, OR, 97331
irem.tumer@oregonstate.edu
ohallorb@onid.orst.edu

Abstract

The safety-critical nature of new complex cyber-physical systems mandates a thorough analysis to fully understand and quantify failure mechanisms and their impact on system design. This paper introduces a system-level reliability analysis method for assessing the dependability of alternative conceptual design architectures. The method enables the analysis of criticality and sensitivity of components to the system-level requirements, based on component connections and their failure probability. The analysis performed at this earliest stage of design facilitates the development of more robust and reliable system architectures. Application of the presented method to the design of a representative aerospace electrical power system (EPS) demonstrates these capabilities.

Introduction

The safety-critical nature of new complex cyber-physical systems mandates a thorough analysis to fully understand and quantify failure mechanisms and their impact on system design. A key technical challenge in developing such complex systems is to ensure that both individual components and the overall system are dependable resulting in turn in reliable designs. On the other hand, ensuring safety and reliability requires the incorporation of subsystem and component models, knowledge, and decisions into the system design process as early as possible. Furthermore, formal tools and methodologies need to be in place to allow design teams to formulate a clear understanding of reliability implications during the early design phases.

To address some of these challenges, this paper introduces a system-level reliability analysis method for assessing the dependability of alternative conceptual design architectures. The technique is based on identification of criticality and sensitivity of system components, and a simulation model that incorporates probability and failure rates of individual components such that system-level reliability measures can be computed. This analysis at the system-level supports decision-making early in the design process and guides the designers to understand and quantify faults and their impact on system design so that design alternatives for component selection, configuration and built-in redundancy can be explored. In the paper, we outline the details of the constituent pieces of the developed method and present the reliability analysis capabilities using an aircraft electrical power system (EPS) example.

Electrical Power System Design

An electrical power system is designed to deliver power to select loads, which in an aerospace vehicle would include subsystems such as the avionics, propulsion, life support, and thermal management systems. The EPS is required to provide basic functionality common to many aerospace applications: power storage, power distribution, and operation of loads (Poll et al. 2007).

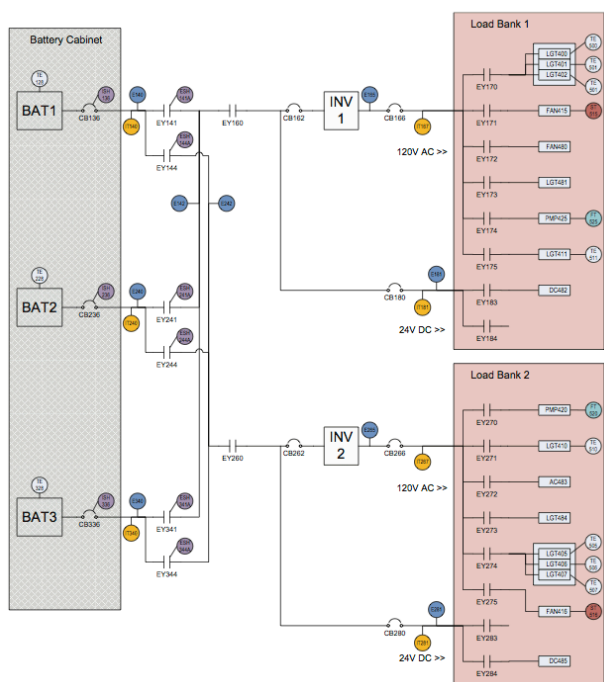


Figure 1. The schematic of an existing electrical power system design architecture (Poll et al., 2007).

An EPS system was originally designed by one of the co-authors using a failure-based design methodology at the early concept design phase (Kurtoglu et al. 2010). Using this design approach, several critical elements were identified and incorporated into the final design and realization of the system.

In the current realization of the system, which is illustrated in Fig. 1, the power storage consists of one or multiple battery modules, which are used to store energy for the operation of the loads. Any of the battery modules can be used to power any number of loads in the system. This requires the EPS to have basic redundancy and reconfiguration capability. Electromechanical relays or other electrical actuators can be used to route the power from the batteries to the loads. In addition, circuit breakers are added to the design at various points in the distribution network to prevent over-currents from causing unintended damage to the system

components. Moreover, a sensor suite is designed in to allow monitoring of voltages, currents, temperatures, switch positions, etc. and to provide an integrated health management functionality. (More information on the existing electrical power system can be found in (Poll et al. 2007)). The list of components that are used in this paper for reliability analysis is shown in Table 1.

Table 1: Summary of EPS failure rates and failure probabilities

Component	Function	Failure Rate λ (1/MHR)	Failure Probability (1 KHR)
Battery (BAT)	Power Source	4.077	0.004096
Circuit Breaker (CB)	Current Breaker	0.242	0.000242
Relay (EY)	Current Relay	2.0031	0.002001
Inverter (INV)	DC to AC Inversion	6.7123	0.00669
Fan (FAN)	Load	11.9639	0.01189
Light (LGT)	Load	3.0415	0.003037
Pump (PMP)	Load	43.6546	0.042715

Reliability Based Design

Reliability of a component is the probability that a component will perform its intended function during a specified period of time. Reliability of a system is the probability that the system performs intended functions during a specified period of time. Reliability modelling is the process of predicting or understanding the reliability of a system given reliability of its components. Design For Reliability (DFR) is a discipline that refers to the process of designing reliability into products. This process encompasses several tools and practices, one of which is *redundancy*, i.e., if one part of the system fails, there is an alternate success path, such as a backup system. However, redundancy is difficult and expensive, and is therefore limited to critical parts of the system. It is important to decide which component needs to be reinforced with more reliability by incorporating redundancy.

Traditional reliability analysis techniques look at system components, critical events, and system characteristics to assess risk and reliability during the design phase. These methods include Failure Modes Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), and Reliability Block Diagrams (RBD). Each of these analyses accomplishes a slightly different goal and in many cases they are each used during the design process for optimal results. FMECA (MIL-STD-1629) is a method that systematically examines individual system components and their failure mode characteristics to assess risk and reliability. FTA (Vesely, 1981) is performed to capture event paths from failure root causes to top-level consequences. Probabilistic Risk Assessment (PRA) (Greenfield, 2000) is a method used for quantification of failure risk by answering three questions: what can go wrong, how likely is it to happen, and what are the consequences (Stamatelatos, 2002). PRA combines a number of fault/event modelling techniques such as master logic diagrams, event sequence diagrams and fault trees and integrates them into a probabilistic framework to guide decision making during design. RBD's is another method used to determine system level reliability of a design during the design stage (Xu, 2009).

Technical Approach: System Modelling

To perform our proposed reliability analysis, we introduce a representation called *Configuration Graph* (CG). A CG consists of a set of components, each with a probability of failure, and possibly a set of *parallel* and/or *serial* connectors, with a set of *directed* connections between components or connectors. The assumptions are: (1) Component fails *independently* with each other, (2) inputs of any component are from *different* sources, (3) the function provided by a

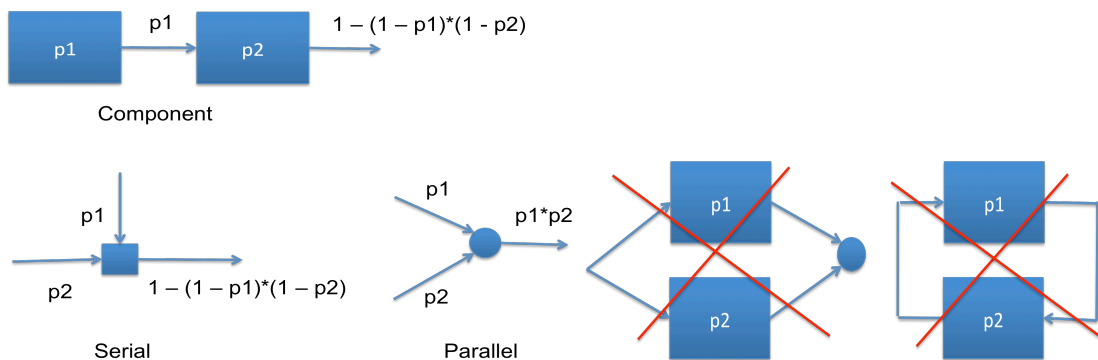


Figure 2. Examples of component and connector failure propagation and invalid connections.

component fails if *any* of its inputs fails or the component fails, (4) the function of a *serial* connector fails if *any* of its inputs fails, and (5) the function of a *parallel* connector fails if *all* its inputs fail.

The *failure probability* propagation of components and connectors from sources to sinks is defined as follows:

- Component connection: $p_f = 1 - (1 - p_c) \prod_i (1 - p_i)$
- Serial connector: $p_f = 1 - \prod_i (1 - p_i)$
- Parallel connector: $p_f = \prod_i p_i$

where p_c is the failure probability of the component, p_i is the failure probability of an input, and p_f is the failure probability of the output, respectively (Fig. 2). A component fails to function correctly, either because it has failed or because it has an input that has failed. For example an electrical component fails its function, either because there is a disconnection in the component or because there is no current coming in. In this modelling representation, we assume that connectors do not fail. A parallel connector provides a mechanism to support redundancy and a serial connector is used for sequential failures. The propagation assumes that input failures are independent from each other; therefore, no loops are allowed (Fig. 2).

Our system modelling approach is similar to several existing reliability modelling techniques, namely to FTA and RBD, but differ in the following ways: (1) FTA is a tree that defines the failure propagation from leaves to the root, while CG is an acyclic graph that defines the component connectivity from sources to sinks; multiple sinks are possible, and (2) RBD defines parallel and serial connections, but does not support dataflow-type computations directly. CG shows component connections that in many cases directly correspond to the physical connections. RBD can be translated to CG easily. One of the advantages of CG is that the failure probability at a sink component can be computed easily and the computation is linear in terms of the number of components in the configuration graph.

Component Reliability Data

Nonelectronic Parts Reliability Data-95 (NPRD-95) was used as the source of the component failure rate data. This is a report (published by RIAC - a DoD Information Analysis Center) which includes high volumes of data from a variety of sources including both military and commercial platforms. This comprehensive data includes the component manufacturer, model or part number, nominal performance specifications specific to each part, population tested, number of operation hours, and number failed. The operating hours and number of parts failed is used to generate failure rates for both specific components and component classes. For example, a failure rate is provided for a specific type of actuator, and then a combined failure rate is given for the actuator class. The failure rate for each component class is the sum of the total components failed for that class divided by the sum of the operating hours for each component in that class. Calculating both types of data lets the user employ the data at a generic or specific level.

Criticality and Sensitivity Analysis

For a given system with a set of sink components, one can compute the failure probability of each of the sink components. For example, for an EPS system, one can compute the probability of failure for the different loads. We propose two ways to combine the failure probability of sink components of a system:

Weighted Failure Probability: $w = \sum_i w_i p_i$ where $\sum_i w_i = 1$.

In this case, the result is a weighted average of failure probabilities of all the sinks. For example, let sinks be the loads (Fan, Light and Pump, respectively). The weighted failure is an expected failure probability with probability distribution w_i and failure probability p_i . This combination makes sense if each sink can function independently.

Maximum Failure Probability: $m = \max p_i$.

This is a worst-case analysis, i.e., a component fails its function if any of the sinks fails. This combination makes sense if all sinks have to co-exist. If any of the sinks fails its function, the system fails completely.

System Failure Index

Given failure probability of each component and a set of sink components, one can compute *Weighted* or *Maximum* Failure Probability, which we call *System Failure Index* (SFI). The computation of SFI is linear to the number of components in CG. In addition, we can compute the *criticality* and *sensitivity* of any component with respect to this SFI. The criticality c_i of a component is defined to be the SFI given that the failure probability p_i of this component is 1. The sensitivity s_i of a component is defined to be the difference of SFIs when the failure probability p_i of this component is 1 and 0. The larger the criticality or sensitivity of a component, the more important is this component's contribution to the overall SFI. The criticality and sensitivity rely on not only the connectivity but also the failure probabilities and weights used in SFI formulation. In general, criticality and sensitivity may not always be correlated. A more sensible component may be less critical. In cases when the failure probabilities are not available, one can simply put a small constant to all the components, and compare relative criticality and sensitivity.

Given a system and SFI, one can determine the component with maximum criticality ($C_{mc} = \max \arg_i c_i$) or sensitivity ($C_{ms} = \max \arg_i s_i$). The *criticality* (*sensitivity*) of the system is the maximum criticality (*sensitivity*) of its components. This computation is quadratic in terms of the number of components.

Implementation: Reliability Analysis Modelling Environment

We have implemented a reliability analysis tool in Simulink/Matlab environment for EPS, where component, serial and parallel connectors are directly modelled. Fig. 3 shows an example of a simple EPS architecture, where the battery cabinet and the load bank are modelled as sub-systems. The number shown in each box is the failure probability of the component. (We obtained the failure probabilities from failure rate specifications in Table 1 based on NPRD-95 data).

To compute criticality (or sensitivity) of a component, one can simply select the component, open the selection dialog box and choose **Criticality** (or **Sensitivity**), then click the **Compute** button. The results are shown in the red (or green) box. For the example shown in Fig. 3, the criticality of a relay component EY244 is 1, while the criticality of the circuit breaker CB280 is 0.1365. EY244 is more critical than CB280. Furthermore, the sensitivity of EY244 is 0.9619, while the sensitivity of CB280 is 0.0965.

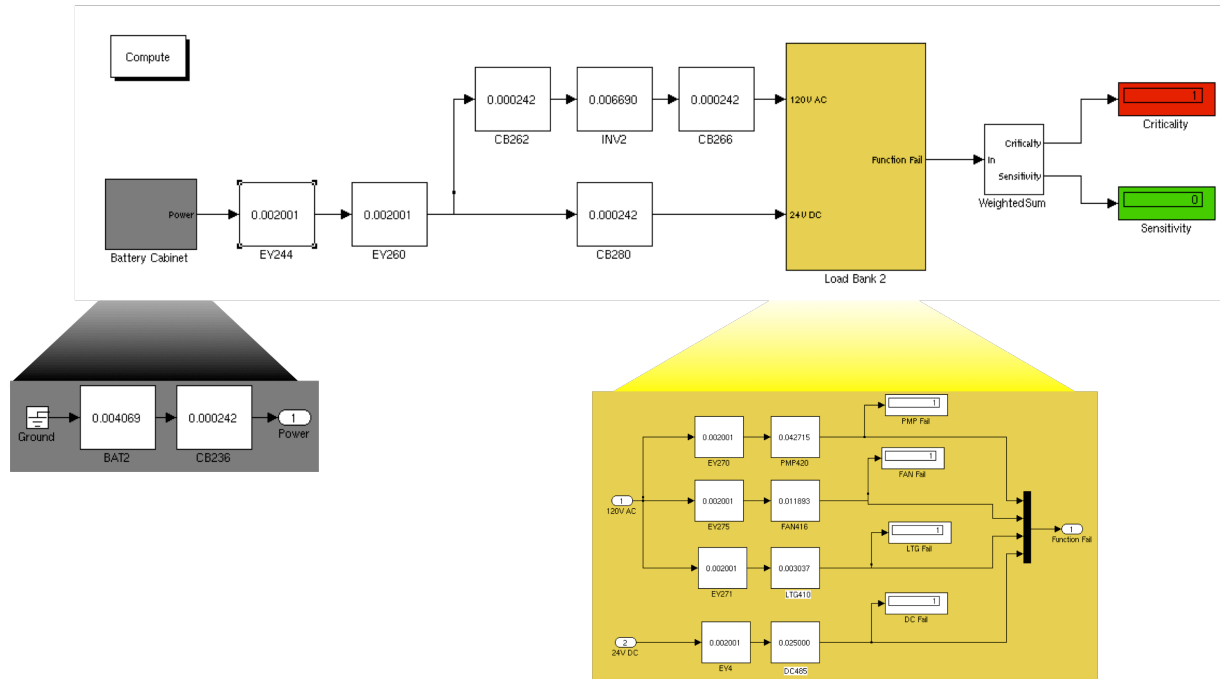


Figure 3. A basic EPS architecture, where the battery cabinet and load bank are modeled as subsystems. Each component has a failure probability (shown in the box) that is calculated from failure rate specification and operation time.

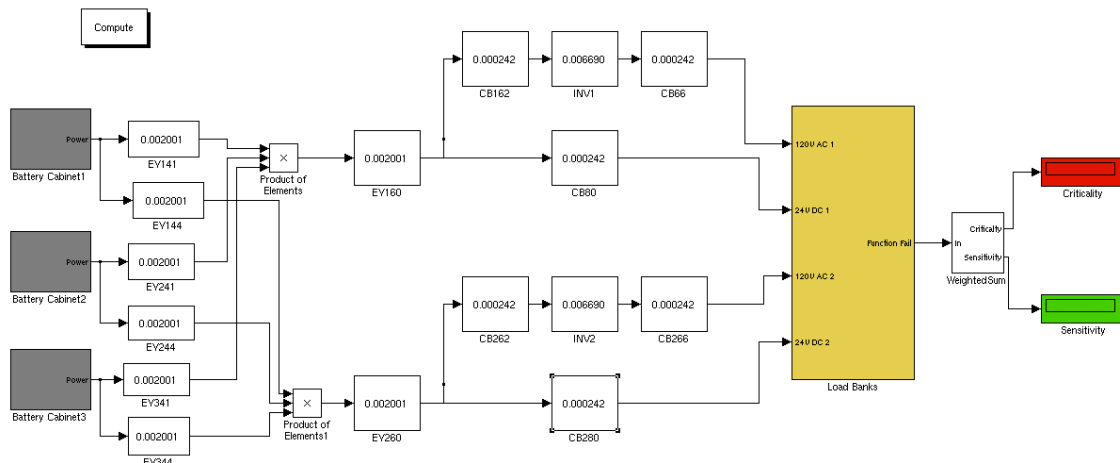


Figure 4. Model of a triple redundant EPS architecture with three battery cabinets and two load banks.

From this analysis, we see that a single failure in EY244 can cause the malfunction of the whole system. Clearly, the reliability of the system can be improved if *redundancy* is introduced. This case is shown Fig. 4. This EPS architecture (schematic previously shown in Fig. 1) includes three battery cabinets and two load banks. Using the same failure probabilities used in the previous design, EY244 now has a criticality of 0.03398 and a sensitivity of 1.91e-5, while CB280 has a criticality of 0.08251 and a sensitivity of 0.04856. Similar analyses can be used to study criticality or sensitivity of system components and to refine design architectures by incorporating redundancy where it is most needed in the system.

Lifetime Analysis

Failure rate λ of components can be obtained by experiments, which are normally given in specifications of those components. The *mean time to failure* is thus $1/\lambda$. The relationship between failure rate and failure probability is as follows: $\lambda = \dot{p}/(1-p)$, or, $p = 1 - e^{-\lambda t}$, i.e., given λ and t , we can obtain failure probability. For the EPS system, failure rates and their failure probabilities at 1000 hours are given in Table 1.

We define expected lifetime of a system as the time duration that the system failure index SFI is below a threshold. Using simulation, we can estimate how long the system will be operational in terms of its SFI, i.e., the lifetime for a given function. Fig. 5 shows the basic EPS architecture where the lifetime is 0.08 MHR.

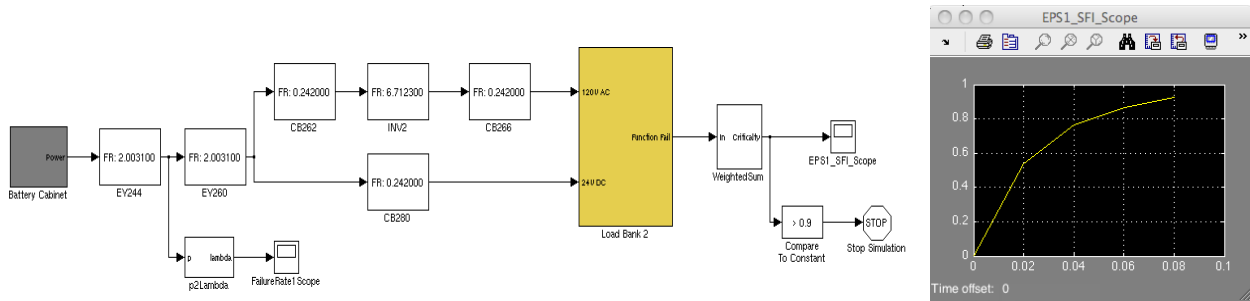


Figure 5. Simulation of lifetime of the basic EPS architecture shown in Fig. 3.

One interesting observation about lifetime analysis is that redundancy may not increase lifetime significantly. This again is shown in Fig. 6 for an EPS architecture with more redundancy (one which includes two redundant batteries). The lifetime for this architecture is computed to be 0.1 MHR, which is only slightly better than the simple design.

This may be attributed to the following: Consider λ_1 and λ_2 are failure rates of two components connected by a parallel connector; the mean time of failure of the output can be obtained by:

$$1/\lambda_p = \int_0^\infty [1 - (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t})] dt = 1/\lambda_1 + 1/\lambda_2 - 1/(\lambda_1 + \lambda_2)$$

If $\lambda_1 = \lambda_2 = \lambda$, we have $\lambda_p = 2\lambda/3$.

In general, given n components with the same failure rate λ , the output failure rate would be:

$$1/\lambda_p = \int_0^\infty [1 - (1 - e^{-\lambda t})^n] dt = [\sum_{i=1}^n (1/i)]/\lambda \approx (\ln n)/\lambda$$

However, if the redundant components are *stand-by*, i.e., at any time only one component is turned on, the expected time of failure would be:

$$1/\lambda_p = \sum_{i=1}^n (1/\lambda_i), \text{ i.e. } n/\lambda \text{ if they are equal.}$$

As future work, we plan to extend our method in order to incorporate both parallel and stand-by redundancy to compute system lifetime.

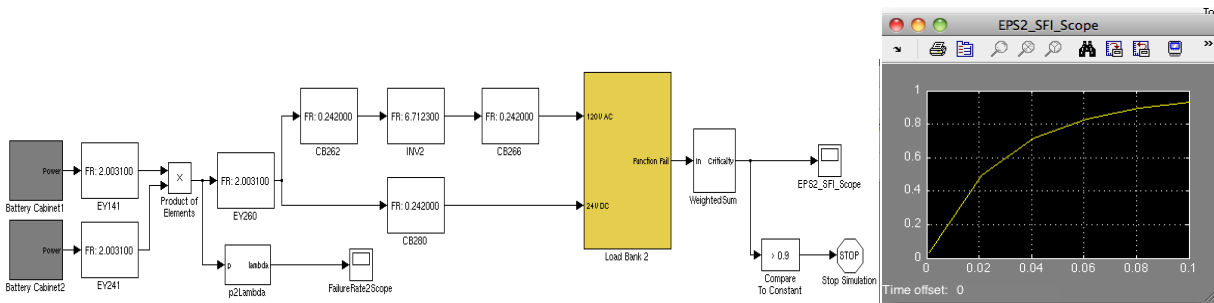


Figure 6. Simulation of lifetime of the EPS with redundant battery cabinet.

Conclusions and Future Work

We have outlined a technique for assessing the reliability of alternative conceptual design architectures. The method is based on identification of criticality and sensitivity of system components, and a simulation model that incorporates probability and failure rates of individual components such that system-level reliability measures can be computed. This analysis at the system-level supports decision-making early in the design process and assists the designers evaluate and identify critical elements of different conceptual architectures, and to select among or integrate different architectural solutions to ensure improved reliability. In this paper, we presented preliminary results of our study. In the future, we plan to further extend the analysis capabilities described in this paper and to fully integrate the developed technique with an automated architectural synthesis tool.

Acknowledgement

This research was funded in part by DARPA (Award #FA8650-10-C-7079). The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

References

Department of Defense, "Procedures for performing failure mode, effects, and criticality analysis." MIL-STD-1629.

- Greenfield, M.A. "NASA's Use of Quantitative Risk Assessment for Safety Upgrades". In IAAA Symposium. 2000. Rio de Janeiro, Brazil.
- T. Kurtoglu, Jensen, D., Tumer I.Y., "A Functional Failure Reasoning Methodology for Evaluation of Conceptual System Architectures," *Journal of Research in Engineering Design*, published online, January 31, 2010.
- S. Poll, A. Patterson-Hine, J. Camisa, D. Garcia, and D. Hall, "Advanced Diagnostics and Prognostics Testbed," *International Workshop on Principles of Diagnosis (DX-07)* Nashville, TN, 2007.
- Stamatelatos, M. and Apostolakis, G. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners v1.1". 2002, NASA, Safety and Mission Assurance.
- A. Vesely, W. E., Goldberg, F. F., Roberts, N. H. and Haasi, D. F., *The Fault Tree Handbook*, US Nuclear Regulatory Commission, NUREG 0492, 1981.
- L. X. H. Xu, R. Robidoux, "DRBD Dynamic reliability block diagrams for system reliability modelling," *International Journal of Computers and Application*, vol. 31, pp. 132-141, 2009.

Biography

Dr. Ying Zhang is a member of research staff at Palo Alto Research Center. She received a Ph.D. in Computer Science from University of British Columbia, Canada, in 1994. Her current research interests are robotic sensor networks, mobile entity localization and tracking, and analysis of large complex systems and networks. Dr. Zhang is a principle investigator and key technical contributor to many DARPA funded projects on distributed robotics, sensor networks, and physical intelligence. She is the information director of the ACM Transaction on Sensor Networks, and has organized various workshops and served on many technical program committees.

Dr. Tolga Kurtoglu is a member of research staff at Palo Alto Research Center (PARC) working for the Embedded Reasoning Group. His research focuses on the design and development of complex systems, design theory and methodology with a specialization in conceptual design, design automation and optimization, and artificial intelligence in design. He conducts research in the areas of development of prognostic and health management technologies, model-based diagnosis, automated reasoning, systems engineering, and risk and reliability-based design. Dr. Kurtoglu has published over 50 articles and papers in various journals and conferences and is an active member of ASME, AIAA, AAAI, ASEE, Design Society, and the Prognostics and Health Management Society. Prior to his work with PARC, he worked as a researcher at NASA Ames Research Center and as a systems design engineer and lead at Dell Corporation.

Dr. Irem Y. Tumer is an Associate Professor at Oregon State University, where she leads the Complex Engineered System Design Laboratory. Her research focuses on the overall problem of designing highly complex and integrated engineering systems with reduced risk of failures, and developing formal methodologies and approaches for complex system design and analysis. Her expertise touches on topics such as risk-based design, systems engineering, function-based design, failure analysis, and model-based design. Since moving to Oregon State University in 2006, her funding has largely been through NSF, AFOSR, DARPA, and NASA. Prior to accepting a faculty position at OSU, Dr. Tumer led the Complex Systems Design and Engineering group in the Intelligent Systems Division at NASA Ames Research Center, where she worked from 1998

through 2006 as Research Scientist, Group Lead, and Program Manager. She received her Ph.D. in Mechanical Engineering from The University of Texas at Austin in 1998.

Bryan O'Halloran is currently a Master's of Science student in Mechanical Engineering at Oregon State University and holds a B.S. degree from the same school in 009 with a Bachelor's of Science degree in Engineering Physics. His current research interests are reliability engineering and system design.