2017

A Graph Theory Approach to Functional Failure Propagation in Early Complex Cyber-Physical Systems (CCPSs)

O'Halloran, Bryan M.; Papakonstantinou, Nikolaos; Giammarco, Kristin M.; Van Bossuyt, Douglas L.

INCOSE

O'Halloran, Bryan M., et al. "A Graph Theory Approach to Functional Failure Propagation in Early Complex Cyber-Physical Systems (CCPSs)." INCOSE International Symposium. Vol. 27. No. 1. 2017.
https://hdl.handle.net/10945/63119

27th Annual INCOSE International Symposium (IS 2017)
Adelaide, Australia, July 15-20, 2017

A Graph Theory Approach to Functional Failure Propagation in Early Complex Cyber-Physical Systems (CCPSs)

Bryan M. O'Halloran
Naval Postgraduate School
bmohallo@nps.edu

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

Kristin Giammarco
Naval Postgradute School
kmgiamma@nps.edu

Douglas L. Van Bossuyt
KTM Research
Douglas.vanbossuyt@gmail.com

Abstract. This paper presents a framework to quantify failure propagation potential for complex, cyber-physical systems (CCPSs) during the conceptual stages of design. This method is referred to as the Function Failure Propagation Potential Methodology (FFPPM). This research is motivated by recent trends in engineering design. As systems become increasingly connected, an open area of research for CCPSs is to move reliability and failure assessments earlier in the engineering design process. This allows practitioners to make decisions at a point in the design process where the decision has a high impact and a low cost. Standard methods are limited by the availability of data and often rely on detailed representations of the system. As such, they have not addressed failure propagation in the functional design prior to selecting candidate architectures. To develop the metrics, graph theory is used to model and quantify the connectedness of the functional block diagram (FBD). These metrics quantify (1) the summation of the reachability matrix and (2) the summation of the number of paths between nodes (functions within system models) i and j for all i and j. From a practical standpoint, these metrics quantify the reachability between functions in the graph and the number of paths between functions defines the failure propagation potential of that failure. The unique contribution of this research is to quantify failure propagation potential during conceptual design prior to selecting candidate architectures. The goal of these metrics is to produce derived system requirements, based on an analysis, that focus on minimizing the impact of failures.

Introduction

An increased demand for suitable design techniques used in developing engineered systems has become more prevalent. Expectations for system designs continue to be for higher performance at less cost. In addition, designers are forced to meet aggressive delivery schedules. As a result, systems often suffer major reliability concerns. Consequently, it has become well known that making correct early design decisions offers several advantages including reduced design and analysis cost, increased freedom to make decisions that have a high impact on the design, and potential for applying methods to a larger number of design alternatives [1]. This is shown by the general trends in Figure 1.

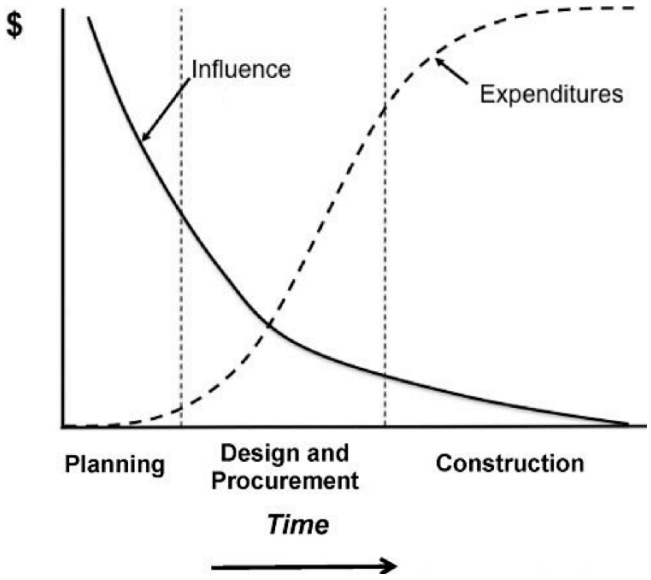

Figure 1. Cost and impact of decision making across a design process

Traditional failure propagation techniques lack a comprehensive ability to analyze the propagation of failures in the conceptual design of complex, cyber-physical systems (CCPSs). By their nature, CCPSs have a high degree of connectedness (e.g., networks, automation equipment, etc.), and therefore have significant risk of failure propagating throughout the systems. Well-developed physics-based models that contain simultaneous equation solvers allow analysis of both forward and backward failure propagation, which propagate failures either with or against the nominal flows in the functional block diagram (FBD). However, in the earliest stages of engineering design where detailed physics-based models are not available, existing failure analysis methods seek only to forward propagate failures. While forward propagation is a major element of how failures propagate, backward propagation and also propagation across uncoupled subsystem boundaries can have significant impacts on the system. In this research, we seek to model failure propagation during conceptual design by using FBDs and graph theory with the goal of describing the behavior of how propagation can occur before physics-based simulators are available.

Graph theory is used to quantify attributes of a system including connectedness and reachability. Directed graphs are used to model the system where edges represent flows (e.g., material, energy, and signal) and nodes represent functions. The reachability matrix R(G) defines the reachability of a failure between any connected functions. To gather relevant failures, we present and then implement Function Failure Rate Design Method (FFRDM). This method uses a novel structuring of the design process to share information from historical failures to early points in the design process. For a specific failure mode, the reachability matrix indicates the propagation potential of that failure. The failure is assessed by distributing points to all functions that are affected. For all potential failures in the system, the summed score is an estimate of the risk due to failure propagation.

Related Research

Early design failure analysis has become a thrust area in research related to CCPSs and reliability engineering. Identifying and mitigating failures in early design has been addressed by several methods in literature. Failure Modes Effects and Criticality Analysis (FMECA) quantifies a failure mode's criticality and likelihood against the system [2]. Failure Modes and Effects Analysis (FMEA) extends FMECA by including a failure mode's likelihood of detection into the risk quantification. The different representation in risk leads to FMECA being preferred in the aerospace and nuclear industry and FMEA in the automotive industry. Both

FMECA and FMEA rely heavily on expert experience to generate risk values. While these basic methods provide a foundation for many failure methods, there are several limitations including intensity of manual labor, usability during functional design, and informality. As a result, several other methods and software tools have been developed to improve on the original FMEA and FMECA methods.

FMEA streamlining [3], WIFA [4], FLAME [5, 6], CFMA [7], and Advanced FMEA (AFMEA) [8, 9] are examples of improved software tools and methods for performing FMEA and FMECA. FLAME and WIFA reduce high user workload by using an archived knowledge base. WIFA, AFMEA, and CFMA indicate the physical cause of the failure and are practical for mechanical systems while FLAME is not. However, FLAME, CFMA, and AFMEA can be used during functional design. A major limitation to these methods is that they do not use a formalized failure language to accurately and consistently define failure modes. One answer to this is the Function Failure Design Method (FFDM), which uses a formalized failure language to improve the automation of identifying failure modes and improving scalability to complex systems through a conceptual system modeling approach implemented using a functional modeling technique [10]. Further, FFDM is extended by the Risk in Early Design (RED) method which introduces failure mode severity and likelihood of occurrence [11–13]. These techniques have broadened the capability of failure analysis by allowing designers to evaluate the functionality of a system prior to formal architecture being defined. While these methods encourage the early discovery of failures, they are unable to address the propagation of failures.

Probabilistic Risk Assessment (PRA) was developed partially in response to the shortcomings of FMEA and FMECA [14]. A failure probability can be calculated via fault and event tree modeling of a system [15]. PRA and its extensions are heavily used in the aerospace and nuclear power industries [16]. While PRA informally models failure propagation through the use of fault and event trees, these are not an accurate and complete representation of the failure propagation. PRA is also not well suited for early conceptual design studies of system risk.

Kurtoglu and Tumer develop a failure propagation method to assess a system once the basic architecture is defined [17]. This is done by propagating failures through the system and results in the system's functional health. Work by O'Halloran et al. models failure propagation across uncoupled boundaries [18] in early conceptual designs. These advances investigate failure propagation once components have been selected. The proposed method in this research is used to quantify the propagation of failures in a purely functional architecture.

The summary of related research clarifies the lack of reliability-based methods applicable to conceptual design. Those that do exist primarily focus on aspects of reliability other than propagation of failures. As a result, this research focuses on the quantification of failure propagation potential in FBDs.

Methodology

This section explains the tenets of the proposed Function Failure Propagation Potential Method (FFPPM). To accomplish this, an example system of a Pressurized Water Reactor (PWR) is presented. Basic explanations for functional modeling and graph theory are provided. The method contains the following steps: 1) Functional Block Diagrams (FBDs) are expressed as graphs using the fundamentals of graph theory. 2) Since functions can be linked to failures, and flows to behavior variables, we establish a process to determine the connection between a given failed function and other functions in the system model (represented in this research by block diagrams), whereas a connection represents a potential failure propagation path. 3) The result is then a FBD with both nominal and potential failure flows represented. Further, metrics are proposed to quantify the failure propagation potential including (1) a summation of the reachability matrix and (2) a summation of the number of

paths between nodes i and j. These metrics are intended to be developed as derived requirements during conceptual design.

3.1 Functional Modeling. The development of functional modeling has become a well-established step in the systems engineering design process. As a part of functional modeling, FBDs are used to describe the network of connections between a system's functions and flows. A FBD defines the design intent of a system; however, a FBD does not indicate how the function is accomplished. This is captured in the physical architecture which is produced at a subsequent step in design. A system boundary delineates the border between the functions included in the system and functions that are outside the system boundary. External flows cross the system boundary and are acted on by functions within the system, and vice versa. Specification of a system boundary produces the desired set of output flows and also the appropriate set of flow conversions inside the system boundary. An important element of FBD is the language used; we use the Functional Basis for Engineering Design (FBED) [19] to describe FBDs. Use of a common language allows a FBD to be consistently developed, well-defined, and to leverage design methods and automation techniques. As a part of the FBED common language, FBDs use material, energy, and signal flows to describe the connection of functions. To demonstrate the proposed methodology, an example FBD design model of a PWR Emergency Core Cooling System (ECCS) is presented (see Figure 2). It should be noted that while the PWR ECCS example is representative of such systems found on commercial PWRs, we explicitly state that the example is not to be used verbatim for any purpose other than the demonstration of FFPPM.

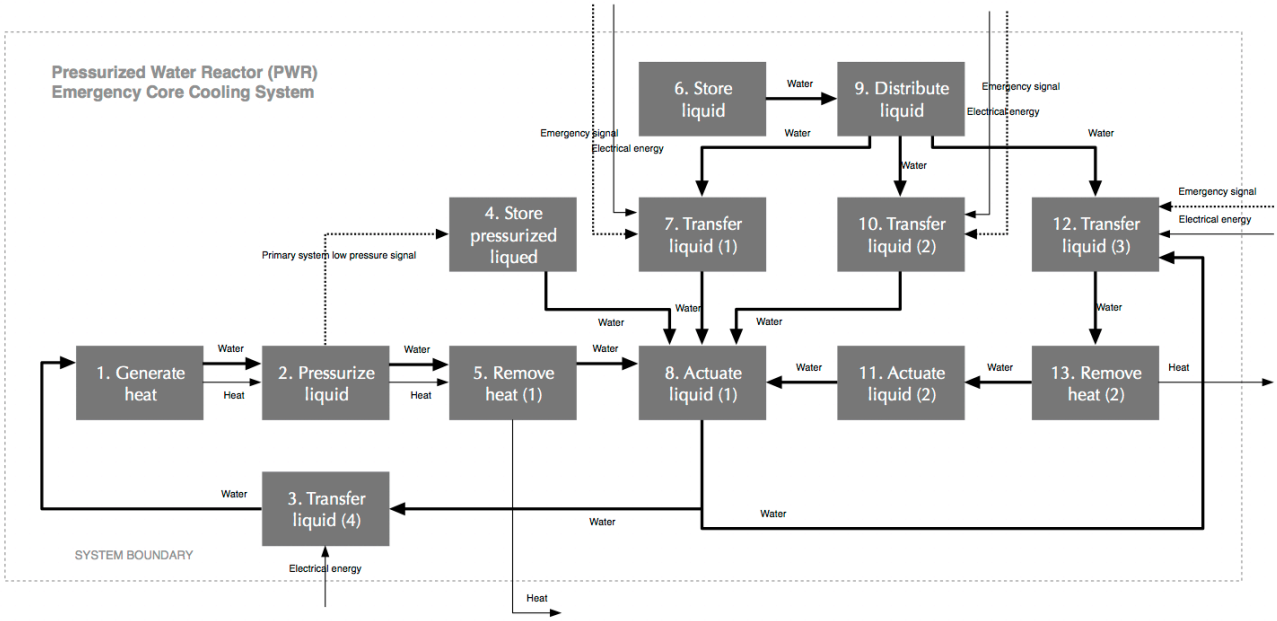

Figure 2. An example FBD of a Pressurized Water Reactor (PWR)

3.2 Constructing Functional Graphs. Graph theory is a well-developed field in mathematics originated by Euler in 1735 [20]. Graphs are models that contain nodes and edges, where edges are used to connect nodes. A node can be connected to any other node including itself. Edges can contain direction (directed graphs) or no direction (undirected graphs). Further, edges can contain weight representing the strength or importance of the connection.

The FBD in Figure 2 is modeled as a directed graph. This graph is also represented mathematically using a matrix (see Figure 3). Note that node 14 represents anything outside the system (i.e., flows that cross the system boundary). The adjacency matrix represents the connectivity of the nodes. Since adjacency matrices are binary, we define connection matrices

as adjacency matrices that allow values outside 1s and 0s. The value of an element Xi, j in the connection matrix represents a connection between elements i and j.

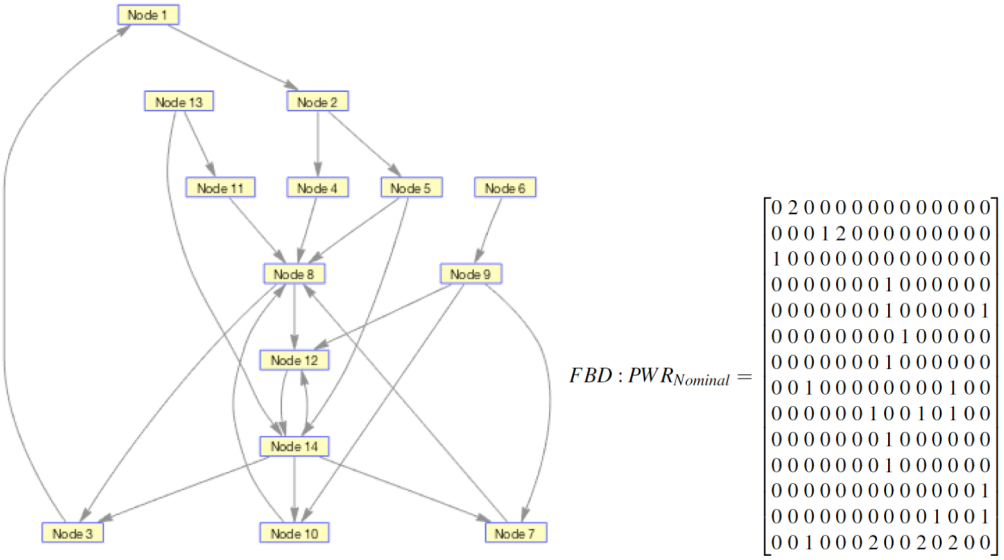

Figure 3. Matrix representation to describe nodes and connections for the Pressurized Water Reactor (PWR) Functional Block Diagram (FBD)

3.3 Proposed Functional Failure Propagation Types. In this research, we propose three types of failure propagation: 1) forward propagation, 2) backward propagation, and 3) uncoupled boundary propagation. Each of these failure propagations behave differently, and are explicitly modeled using the method presented. In all failure propagation types, an initiating failure begins the propagation. Figure 4 depicts an overview of the failure propagation types where the red, solid line represents the flow of the failure. The top left side of Figure 4 is a snippet of a nominal FBD, whereas the other three quadrants represent example failure propagation for that FMD snippet.

The goal of representing types of failure propagation is to have a robust method for inserting new failure connections in the FBD that result when the system experiences a failure. These types are explained here.

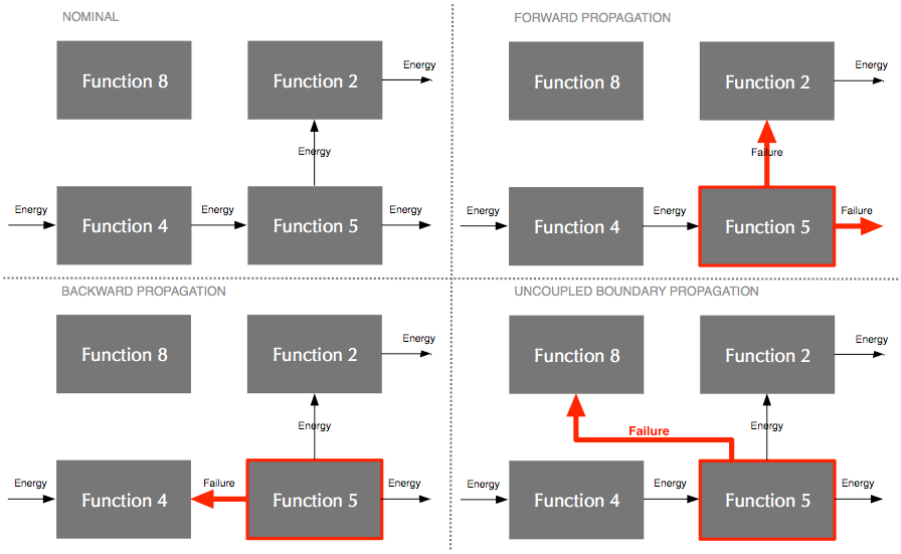

Figure 4. Types of failure propagation modeled in the Function Failure Propagation Potential Method (FFPPM)

1. *Forward propagation*. Forward propagation is the most commonly analyzed type of failure propagation where a failure propagates from the failed function to the next function in line. This propagation is in the direction of the flow for flows that exist in the nominal FBD. In Figure 4 (top right), where function 5 has failed, the effect flows out of function 5 along the existing energy flows.
2. *Backward propagation*. Backward propagation is less common and not always analyzed in existing methods. It occurs when a failure propagates against the nominal direction of the material, energy, and signal flows. In Figure 4 (bottom left), where function 5 has failed, the failure flows backwards against the energy flow.
3. *Uncoupled boundary propagation*. Propagation across uncoupled boundaries is a case where functions interact unexpectedly. In this scenario, failures propagate between functions that were not intended to interact. In Figure 4 (bottom right), where function 5 has failed, the effect flows between function 5 and function 8. Prior to this connection, the two functions do not share a direct relationship.

To demonstrate the three propagation types, consider the following example. While the proposed FFPPM applies to functional designs, this example uses a physical architecture. Consider leaking in a pipe where the pipe exists as part of a larger system. Leaking in this pipe causes a reduced throughput of fluid, and a reduction in the fluid pressure. The reduction in throughput is in the direction of the flow rate (forward propagation) while the pressure occurs throughout the fluid (both forward and backward propagation). While this appears to be the extent of the failure mode's effect, the other aspect depends on the location of the leaking pipe relative to the remainder of the system. There are many components which are affected by fluid, namely electronics. In cases where electronics are submerged, contact a fluid, or degrade faster due to high humidity, avoiding the interaction between fluids and electronics is a standard design practice. This interaction addresses the uncoupled boundary propagation for the leaking pipe.

3.4 Developing Failure Propagation Flows. Generating new connections in the functional graph requires several aspects to be considered. First, a set of initiating failures is used to determine the failures that occur. Our prior work is used to identify functional failures [21]. The Function Failure Rate Design Method (FFRDM) developed a knowledge base to relate functions directly to failure. The knowledge base of functions to failure is comprised of 36,700 failures organized with a failure taxonomy [22]. Assumptions used to develop this database are that the data represents the system being analyzed, the data is accurate, and that failures are independent. Given a set of functions, the knowledge base is used to gather failure rates. This knowledge base is used for the example in this section (see Figure 5).

Failure	Store liquid (includes 'store pressurized liquid')	Distribute liquid	Transfer liquid (x4)	Actuate liquid (x2)	Remove heat (x2) (export thermal energy)	Generate heat (import thermal energy)	Pressurize liquid (regulate pneumatic energy)
	Failure Rate (Failure per Million Hours)						
Breakdown, time dependent dielectric	0	2.0E-04	0	0	0	0	0
Contamination	0	0	0	0	2.0E-04	1.0E-04	0
Control issue	5.0E-03	0	0	1.2E-03	1.3E-02	6.0E-04	0
Corrosion	4.0E-03	5.8E-03	4.0E-04	0	1.3E-02	3.0E-04	0
Cracking	2.0E-04	4.0E-04	1.2E-03	0	1.5E-02	6.0E-03	1.1E-03
Creep	0	7.0E-04	2.4E-03	6.0E-04	1.0E-02	4.1E-03	4.0E-03
Direct chemical attack	0	0	4.8E-03	0	2.6E-03	1.3E-03	4.9E-03
Failure mechanism	2.0E-04	1.2E-03	4.4E-03	0	1.3E-02	6.1E-03	6.2E-03
Fatigue	0	3.0E-04	0	0	0	0	0
Fretting	0	7.0E-04	4.0E-04	0	6.0E-04	3.0E-04	1.0E-04
Galling and seizure, seizure	0	2.0E-04	0	8.0E-04	1.3E-02	5.9E-03	0
Impact, deformation	0	0	0	0	2.0E-04	1.0E-04	0
Latch-up	6.0E-04	0	0	0	1.2E-03	0	0
Noise	0	1.0E-04	0	0	8.0E-04	0	0
Other	6.0E-04	3.0E-04	8.0E-04	4.0E-04	1.0E-02	3.3E-03	1.2E-03
Overstress of incorrect current magnitude	8.0E-04	1.0E-04	0	4.0E-04	1.0E-02	3.5E-03	0
Rupture	0	2.0E-04	4.0E-04	0	2.0E-04	0	4.0E-04
Unknown	0	1.1E-03	2.0E-03	3.6E-03	3.5E-02	1.5E-02	5.7E-03
Wear	4.0E-04	3.6E-03	1.2E-02	5.2E-03	2.0E-01	9.2E-02	1.2E-02

Figure 5. List of failures acquired for the Pressurized Water Reactor (PWR) functional block diagram (FBD)

By presenting the FBD as a graph, forward and backward failure propagation paths are implicitly present. More specifically, failures can potentially propagate along any flow that is present in the graph, in either direction. Failures may also propagate along undiscovered propagation paths not present in the FBD. The discovery of new failure propagation paths requires knowledge about both the initiating failure, which may come from the environment beyond the system boundary, and the behavior of the system being designed.

One approach to modeling new failure propagation paths is to assert that failures propagate along singular flow types (e.g., rotational mechanical energy). In this case, a failure would only affect the rotational mechanical energy flows in the FBD. While this approach was considered in this research, failures are known to be physics-based when emerging in the system and often affect only a portion of the flow. As such, the mechanism to model the propagation paths should be physics-based and more detailed than the flow type. As a result, the discovery of new failure propagation paths uses the behavior variables associated with each flow. Further, various flow types share common behavior variables. In this case, the failure would continue to propagate with the behavior variable that it affects.

To accomplish the modeling of new failure propagation paths using behavior variables, we propose a set of behavior variables for each flow in the FBED. A set of these variables were previously proposed alongside the FBED [19]. However, the original work proposed only energy flow variables. We extend this to include material and signal flow variables. The complete list of behavior variables is shown in Figure 6.

FBED flow hierarchy	FBED flow and definition	Behavior variable (*New)	Variable des.
Material	**Human**. All or part of a person who crosses the device boundary.	*volume, *location	
	Gas. Any collection of molecules characterized by random motion and the absence of bonds between the molecules.	*volume, *location, *chemical elements	V, L, Ce
	Liquid. A readily flowing fluid, specifically having its molecules moving freely with respect to each other, but because of cohesive forces, not expanding indefinitely.	*volume, *location, *chemical elements	V, L, Ce
	Solid. Any object with mass having a definite, firm shape.	*volume, *dimensions, *location, *chemical elements	V, L, D, Ce
	Plasma. A collection of charged particles that is electrically neutral exhibiting some properties of a gas, but differing from a gas in being a good conductor of electricity and in being affected by a magnetic field.	*volume, *location, *chemical elements	V, L, Ce
	Mixture. A substance containing two or more components which are not in fixed proportions, do not lose their individual characteristics and can be separated by physical means.	*volume, *location, *chemical elements	V, L, Ce
Energy	**Human**. Work performed by a person on a device.	force, velocity	F, Ve
	Acoustic. Work performed in the production and transmission of sound.	pressure, particle velocity	P, Pv
	Biological. Work produced by or connected with plants or animals.	pressure, volumetric flow	P, Vf
	Chemical. Work resulting from the reactions by which substances are produced from or converted into other substances.	affinity, reaction rate	A, Rr
	Electrical. Work resulting from the flow of electrons from a negative to a positive source.	electromotive force, current	Ef, C
	Electromagnetic. Energy that is propagated through free space or through a material medium in the form of electromagnetic waves. It has both wave and particle-like properties.	intensity, velocity	I, Ve
	Hydraulic. Work that results from the movement and force of a liquid, including hydrostatic forces.	pressure, volumetric flow	P, Vf
	Magnetic. Work resulting from materials that have the property of attracting other like materials, whether that quality is naturally occurring or electrically induced.	magnetomotive force, magnetic flux rate	Mf, Mfr
	Mechanical. Energy associated with the moving parts of a machine or the strain energy associated with a loading state of an object.	torque, angular velocity, force, linear velocity	T, Av, F, Lv
	Pneumatic. Work resulting from a compressed gas flow or pressure source.	pressure	P
	Radioactive (Nuclear). Work resulting from or produced by particles or rays, such as alpha, beta and gamma rays, by the spontaneous disintegration of atomic nuclei.	intensity, decay rate	I, Dr
	Thermal. A form of energy that is transferred between bodies as a result of their temperature difference.	temperature, heat rate	Te, Hr
Signal	**Status**. A condition of some system, as in information about the state of the system.	*time, *location, *amplitude	Ti, L, Am
	Control. A command sent to an instrument or apparatus to regulate a mechanism.	*time, *amplitude	Ti, Am

Figure 6. Functional behavior variable, their designators, and their relationship to Functional Basis flows

Given the list of behavior variables in Figure 6, each failure in Figure 5 is assessed. This assessment determines all behavior variables affected by a specific failure. In this case, as with all analyses, expert knowledge of the failure and similar systems is relevant.

To demonstrate this process, corrosion is used as an example to generate a new failure propagation path. Failure propagation connections in the FBD are made by connecting the identified failure to affected behavior variables. As shown in Figure 5, the function distribute liquid is connected to this failure. Corrosion leads to pitting, voids, and cracks in the material. The purpose of distributing liquid is to direct liquid to multiple locations based on one or more inputs. This failure therefore leads to leaking and has several failure propagation effects. First, reduced liquid volume (i.e., behavior variable V) is distributed to subsequent components. Second, the pressure (i.e., behavior variable P) to move liquid is also reduced in the forward and backward direction. Third, the leaked liquid has the potential to interfere with all electrical energy (i.e., behavior variable C) flows. The result of these failure propagation paths is shown in Figure 7. This example is for corrosion in the distribute liquid function, and therefore only represents a subset of all flows that should be added to complete this step in the methodology.

The previously mentioned leaking pipe example is used to demonstrate failure propagation types using an example with real architecture. This example indicates that not all failure paths developed are equal. For example, the probability of a leaking pipe interacting with electronics is less likely than a leaking pipe delivering less fluid to subsequent components. In the event of a leak, subsequent components are guaranteed to lack the desired flow rate and fluid volume. However, a leak affecting components through an uncoupled failure propagation path is far less probable. This is directly addressed using lower weight values in the connection matrix. Specifically, the connection weight is determined in the following way:

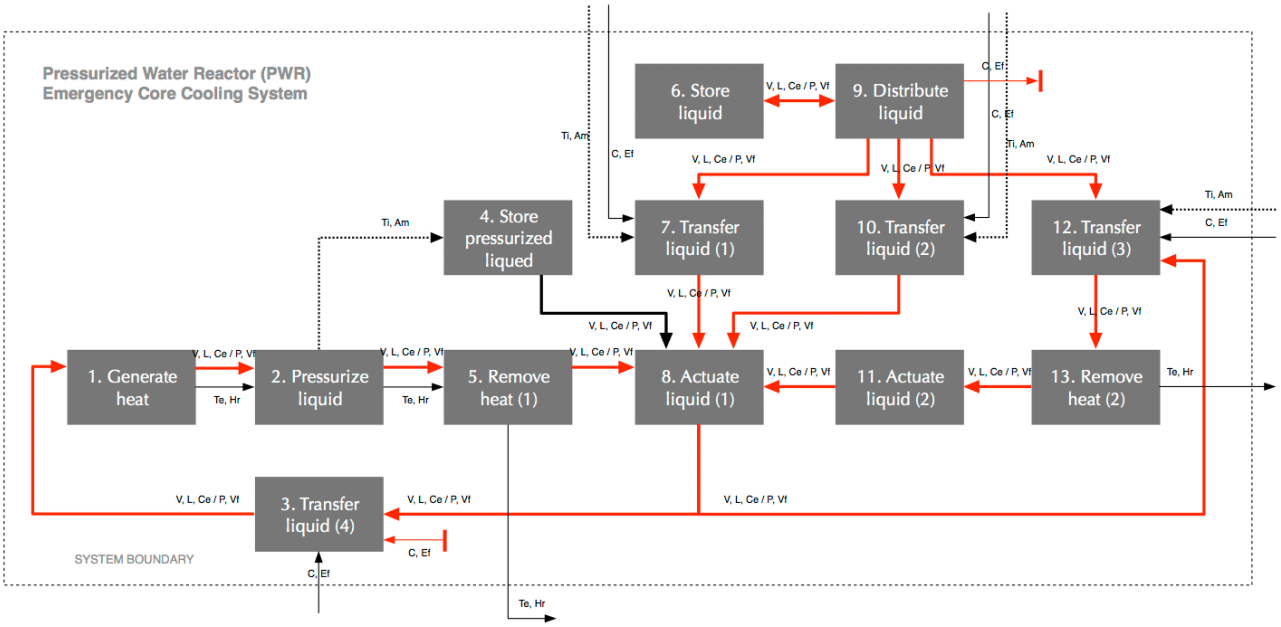

Figure 7. Example FBD with failure propagation paths (red) for leaking due to corrosion

1. Nominal connections: Connections that are present in the nominal FBD (i.e., provided prior to applying this method) have a weight equal to 1.
2. Failure propagation paths that are likely to occur have a weight equal to λ of the failure.
3. Failure propagation paths that are unlikely to occur have a weight equal to λ /2 of the failure.

Beyond these three types of weights, we determine how those values (i.e., λ or λ /2) are distributed across the entire failure propagation path. This applies to Types 2 and 3; a nominal connection always has a value of 1. For types 2 and 3, the full failure propagation path is assumed to follow along the flow it has affected. In the example in Figure 7, the failure affected water flow in nearly all functions. Function 4 was not impacted since no water flows into function 4. To understand how λ (or λ /2 for type 3) is distributed along these paths, two approaches are considered. The first approach is to say that a failure has a total value of 1, which is distributed across the functions that it propagates across. Thus, the longer a failure propagation path, the less affected each function is. For example, if a likely (i.e., type 2) failure propagates across 5 functions, the impact to each function is λ /5.
However, this approach does not model reality since failures do not weaken with longer propagation paths. The motivation of this research is to inform designers on how produce systems that are robust to failure propagation. As a result, the selected approach is to distribute the λ to each function that is affected by a specific failure propagated. This promotes reducing the length of propagated failures and meets the goal of this research. Figure 8 shows the connection matrix for the PWR FBD with all failure propagation connections included.

$$FBD: PWR_{FailProp} = \begin{bmatrix} 0 & 2.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1.0 & 2.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.5 & 0 & 0 & 0 & 0 & 0 & 1.0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1.5 & 0.5 & 0 & 0 & 0.5 & 0 & 0 & 0.5 & 0 & 1.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 1.0 & 0 & 0 & 1.0 & 0 & 1.0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.0 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 & 1.0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.5 & 0 & 0 & 1.0 \\ 0 & 0 & 1.0 & 0 & 0 & 0 & 2.0 & 0 & 0 & 2.0 & 0 & 2.0 & 0 & 0 \end{bmatrix}$$

Figure 8. New connection matrix for the directed graphs in Figure 3

3.5 Quantifying Graph Failure Propagation Potential. The graph's connectedness is the baseline knowledge for how failures are propagated. We propose two metrics to quantify failure propagation potential using graph connectedness. The first is determined using the reachability matrix, R(G). A cell Xi, j in R(G) represents the number of steps required to traverse the graph from node i to node j. In this case, nodes represent functions within the system model. An example R(G) is presented in Figure 9. In this example, is shows that 7.1 steps are required to traverse from node 10 to node 5. This value of the number of steps is determined by the weight of the connections. In some cases, the value in R(G) is less than 1, which represents where only a failure propagation paths exists.

$$R(G): PWR_{FailProp} = \begin{bmatrix} 0 & 2.5 & 3.5 & 3.5 & 5.1 & 4.6 & 3.5 & 4.5 & 4.0 & 3.5 & 5.6 & 3.5 & 4.1 & 4.5 \\ 2.5 & 0 & 1.0 & 1.0 & 2.5 & 2.0 & 1.0 & 2.0 & 1.5 & 1.0 & 3.1 & 1.0 & 1.5 & 2.0 \\ 1.5 & 4.1 & 0 & 5.1 & 6.6 & 6.1 & 5.1 & 6.1 & 5.6 & 5.1 & 7.1 & 5.1 & 5.6 & 6.1 \\ 1.5 & 4.1 & 0 & 0 & 6.6 & 1.0 & 0 & 1.0 & 0.5 & 0 & 2.1 & 0 & 0.5 & 1.0 \\ 3.5 & 6.1 & 2.0 & 2.0 & 0 & 3.1 & 2.0 & 1.5 & 2.5 & 2.0 & 4.1 & 2.0 & 2.6 & 1.0 \\ 1.5 & 4.1 & 0 & 1.5 & 6.6 & 0 & 0 & 1.0 & 0.5 & 0 & 2.1 & 0 & 0.5 & 1.0 \\ 2.0 & 4.6 & 0.5 & 1.5 & 7.1 & 1.0 & 0 & 1.0 & 0.5 & 1.0 & 3.1 & 1.0 & 1.6 & 2.0 \\ 2.0 & 4.6 & 0.5 & 0.5 & 7.1 & 1.5 & 0.5 & 0 & 1.0 & 0.5 & 2.6 & 0.5 & 1.0 & 1.5 \\ 1.5 & 4.1 & 0 & 2.0 & 6.6 & 0.5 & 0.5 & 1.5 & 0 & 0.5 & 2.6 & 0.5 & 1.0 & 1.5 \\ 2.0 & 4.6 & 0.5 & 1.5 & 7.1 & 1.0 & 1.0 & 1.0 & 0.5 & 0 & 3.1 & 1.0 & 1.6 & 2.0 \\ 1.5 & 4.1 & 0 & 1.5 & 6.6 & 1.0 & 0 & 1.0 & 0.5 & 0 & 0 & 0 & 0.5 & 1.0 \\ 2.0 & 4.6 & 0.5 & 2.5 & 7.1 & 1.0 & 1.0 & 2.0 & 0.5 & 1.0 & 2.1 & 0 & 0.5 & 1.0 \\ 3.1 & 5.6 & 1.5 & 3.1 & 8.1 & 2.6 & 1.5 & 2.5 & 2.0 & 1.5 & 1.5 & 1.5 & 0 & 1.0 \\ 2.5 & 5.1 & 1.0 & 3.5 & 7.6 & 3.0 & 2.0 & 3.0 & 2.5 & 2.0 & 4.1 & 2.0 & 2.5 & 0 \end{bmatrix}$$

Figure 9. R(G) matrix to define the connectivity of the FBD

To understand the relative difference in failure propagation potential between the nominal FBD and the FRB where failure propagation flows has been added, we quantify theoretical minimum and maximum values. The minimum value, which is associated with a high degree of failure propagation, is found by using a complete graph with the same number of nodes (i.e., n=14 for the PWR example). In a complete graph, each node is connected to every other node in the graph. Thus, a failure is transmitted to every other function of the system in a single step. On the other hand, the maximum value is found by using a ring graph. In a ring graph, there are connections between each node and the adjacent node. To quantify one aspect of the failure propagation potential, the summation of R(G) is used. For the PWR example, the summation of R(G) is quantified for each graph (See Figure 10).

Graph	sum(R(G))	Norm sum(R(G))	Interpretation
Complete graph	182	0%	Max failure propagation potential
Ring graph	1274	100%	Min failure propagation potential
Nominal PWR FBD	489	28%	Baseline failure propagation potential for nominal PWR FBD
FailProp PWR FBD	436	23%	Failure propagation potential for PWR FBD with added failure propagation

Figure 10. Comparison of the summation of the reachability matrix, R(G), for the nominal PWR FBD, updated PWR FBD with added failure propagation paths, a 14-node ring graph, and a 14-node complete graph

Results in the sum(R(G)) column are generated by summing all rows and columns in R(G). In the Norm sum(R(G)) column, the difference between 1274 and 182 are set as the maximum value (i.e., 100%) and 182 is set as the minimum (i.e., 0%). The value of 23% relative to 28% represents that the FailProp PWR FBD has, on average, less distance between functions for failures to propagate along. In this case, a lower value is more detrimental to the system since the average steps between functions is lower.

While R(G) contains much of the graph connection information, it should be recognized that failure propagation can be inhibited by certain failures. While this paper does not model this directly, it is addressed with a metric for the total number of paths present in the graph. For a given graph, this metric is the summation of all paths between nodes i and j. Figure 11 displays the results for the PWR example for the FBD with failure propagation included. The results show that most functions have several paths between them, showing a high degree of failure propagation potential.

To node \ From node	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	n/a	373	1	179	194	179	80	68	68	80	223	95	183	126
2	1	n/a	1	179	194	179	80	68	68	80	223	95	183	126
3	27	373	n/a	179	194	179	80	68	68	80	223	95	183	126
4	27	27	27	n/a	131	198	71	35	78	71	198	110	175	112
5	1	1	1	179	n/a	179	80	68	68	80	223	95	183	126
6	79	79	79	89	96	n/a	27	47	1	27	157	75	142	77
7	130	130	130	187	205	336	n/a	137	186	123	173	139	299	160
8	72	72	72	135	97	198	51	n/a	78	51	173	105	159	112
9	79	79	79	89	96	209	27	47	n/a	27	157	75	142	77
10	130	130	130	187	205	336	123	137	186	r/a	329	139	299	160
11	55	55	55	75	90	110	49	37	44	49	n/a	1	1	89
12	55	55	55	75	90	110	49	37	44	49	191	n/a	280	89
13	55	55	55	75	90	110	49	37	44	49	191	1	n/a	89
14	61	61	61	145	39	215	98	70	84	98	273	47	166	n/a

Figure 11. Number of paths between functions i and j for the PWR example

While the two metrics contain similar information, the following example motivates the inclusion of both. In the graph shown in Figure 12, there are many paths between function 2 and 8. For example, some of the shorter paths are [2 5 8], [2 4 8], and [2 4 7 8]. While the first metric capture the connection between function 2 and 8, it quantifies this with a value of 2 since the shortest path between these is 2 steps. However, in the event that certain functions have failed, and the shortest paths are eliminated, there are a significant number of remaining paths that will propagate the failure. Thus, the metrics address different aspects of the failure propagation potential.

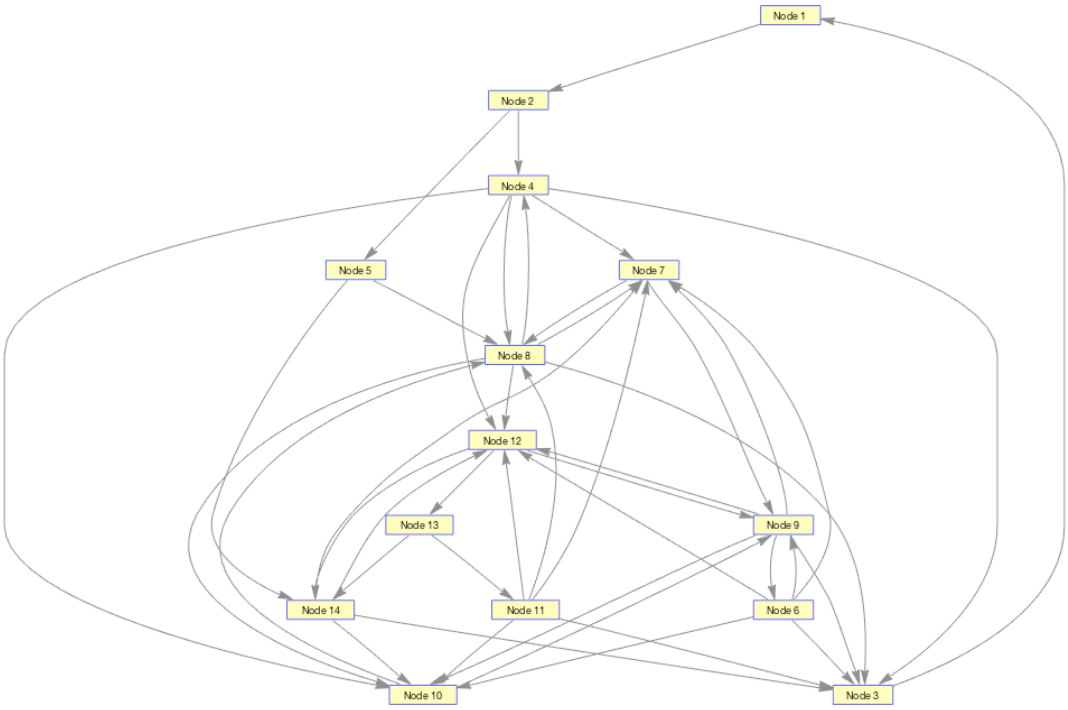

Figure 12. Graph representation for the PWR example with failure propagation flows included

The metrics developed from this research can be used by systems designers to identify potential short failure paths that exist within the system. The number of functions (nodes) shown in Figure 9 is indicative of the probability that a failure in one function can traverse through the rest of the system to reach another function. Another useful outcome of this research is the number of failure paths between functions, shown in Figure 11. Functions with many pathways between them have a higher probability, when all propagation paths are equally likely to occur, as compared to functions with few pathways between them. However, functions with few pathways between them may also be indicative of critical flow pathways [23]. Critical flow pathways with few or no redundancy could then be redesigned with additional redundancy or risk mitigation may be imposed via other means (e.g., high reliability safety system designation, reduced reliance on critical flow path, etc.).

The authors note several assumptions made in this research. First, propagated failures are modeled as sudden and complete. The first result of this is that partial failures are not being investigated. Further, the time-based element of failure propagation is not modeled. A propagation path can go through a function that slowly degrades, and in this paper, the degradation occurs immediately. Additionally, failure effect is disregarded. The system's connectivity determines the system's effect of a failure mode, which is based on the length of the propagation path. Even if the length were changed by the system being reconfigured, the initial failure value remains λ.

Conclusion

This paper presents a framework to quantify failure propagation potential for CCPSs during the conceptual stages of design. Specifically, three types of failure propagation are proposed: forward, backward, and uncoupled. Current modeling of failure propagation does not cover these most of the these types. Further, these are traditionally ignored entirely during functional design. With the inclusion of failure propagation paths to the FBD, metrics are proposed to quantify the failure propagation potential for FBDs. To develop the metrics, graph theory is used to model the connectedness of the FBD and the reachability of one function to another. Directed graphs are used to model the system where edges represent flows (i.e.,

material, energy, and signal) and nodes represent functions. The reachability matrix R(G) defines the reachability of a failure between any connected functions.
For a specific failure mode, the reachability matrix indicates the propagation potential of that failure. The metrics proposed in this research are (1) the summation of the reachability matrix and (2) the summation of the number of paths between nodes i and j for all i and j. These metrics are intended to be developed as requirements during conceptual design.

Future Work

In this research, we show the connectedness of a FBD, which presents a mathematical approach to quantifying failure propagation during functional design. The limitation of this is that all connections are weighted equally. Not all connections in a system are equally needed; safety features in a system would be weighted stronger than most other features. Also, many flows are used during the system's common operation while others are reserved for specialized and infrequent operation. As a result, the failure of these safety features is also not equal. To extend the work presented in this research, the weight of the connections in the FBD graph will be estimated. This addition will improve the graph-based predictors presented in this paper.
Further, an important aspect for methodologies is their scalability to large systems. The presented analysis of the FBD would present challenges when applied to systems with a large number of functions. As a result, the authors plan to formalize the approach with dedicated rules such that the process to add failure propagation flow can be automated.

Acknowledgements

This research is partially supported by United States Nuclear Regulatory Commission Grant Number NRC.HQ-84-14-G-0047 and the Naval Postgraduate School (NPS). 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] Kai Yang and Basem S. EI-Haik. Design for Six Sigma. McGraw-Hill, New York City, May 21, 2003 2003.
[2] Army. Failure modes, effects and criticality analysis (fmeca) for command, control, communications, computer, intelligence, surveillance, and reconnaissance (c4isr) facilities. United States Government, 2006.
[3] Thomas A. Montgomery and Kenneth A. Marko. Quantitative fmea. In Reliability and Maintainability Symposium, 1997.
[4] R. Wirth, B. Berthold, A. Kramer, and G. Peter. Knowledge-based support analysis for the analysis of failure modes and effects. Engineering Applications of Artificial Intelligence, 9(3):219–229, 1996.
[5] C.P. Price. Effortless incremental design fmea. In Annual Reliability and Maintainability Symposium, Las Vegas, NV U.S.A., 1996.
[6] J.E. Hunt, D.R. Pugh, and C.P. Price. Failure mode effects analysis: A practical application of functional modeling. Applied Artificial Intelligence, 9(1):33–44, 1995.
[7] A. Hari and M. P. Weiss. Cfma-an effective fmea tool for analysis and selection of the concept for a new product. In ASME Design Engineering Technical Conference, Design Theory and Methodology Conference, volume DETC99/DTM-8756, Las Vegas, NV, 1999. ASME.
[8] Charles F. Eubanks, Steven Kmenta, and Kosuke Ishii. Advanced failure modes and effects analysis using behavior modeling. In ASME Design Engineering Technical Conferences, volume DETC97/DTM-3872, Sacramento, CA, 1997.
[9] S. Kmenta, P. Fitch, and K. Ishii. Advanced failure modes and effects analysis of complex processes, 1999.

[10] Michael Van Wie Robert B. Stone, Irem Y. Tumer. The function-failure design method. Mechanical Design, 127(3):397–407, 2004.
[11] K. Grantham Lough, R.B. Stone, and I.Y. Tumer. The risk in early design (red) method: Likelihood and consequence formulations. In ASME International Design Engineering Technical Conferences, volume DETC2006-99375, Philadelphia, PA, 2006. ASME.
[12] K. Grantham-Lough, R. B. Stone, and I. Y. Tumer. Implementation procedures for the risk in early design (red) method. Journal of Industrial and Systems Engineering, 2(2):126–143, 2008.
[13] K. Grantham Lough, R.B. Stone, and I.Y. Tumer. The risk in early design method (red). Journal of Engi.neering Design, 18(1), 2007.
[14] William Keller and Mohammad Modarres. A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor norman carl rasmussen. Reliability Engineering & System Safety, 89(3):271–285, 2005.
[15] Mohammad Modarres. Risk analysis in engineering: techniques, tools, and trends. CRC press, 2006.
[16] Steven L Cornford, Todd Paulos, Leila Meshkat, and MS Feather. Towards more accurate life cycle risk management through integration of DDP and PRA. Pasadena, CA: Jet Propulsion Laboratory, National Aeronautics and Space Administration, 2003.
[17] T. Kurtoglu and I. Y. Tumer. A graph-based fault identification and propagation framework for functional design of complex systems. Journal of Mechanical Design, 130(5), 2008.
[18] Bryan M O'Halloran, Nikolaos Papakonstantinou, and Douglas L Van Bossuyt. Modeling of function failure propagation across uncoupled systems. In 2015 Annual Reliability and Maintainability Symposium (RAMS), pages 1–6. IEEE, 2015.
[19] Julie Hirtz, Robert B Stone, Daniel A McAdams, Simon Szykman, and Kristin L Wood. A functional basis for engineering design: reconciling and evolving previous efforts. Research in engineering Design, 13(2): 65–82, 2002.
[20] Dennis M Buede. The engineering design of systems: Models and methods. 1999.
[21] Bryan M O'Halloran, Robert B Stone, and Irem Y Tumer. Link between function-flow failure rates and failure modes for early design stage reliability analysis. In ASME 2011 International Mechanical Engineering Congress and Exposition, pages 457–467. American Society of Mechanical Engineers, 2011.
[22] S. J. Uder, R. B. Stone, and I. Y. Tumer. Failure analysis in subsystem design for space missions, 2004.
[23] Briana Lucero, Vimal K Viswanathan, Julie S Linsey, and Cameron J Turner. Identifying critical functions for use across engineering design domains. Journal of Mechanical Design, 136(12):121101, 2014.

Biography

Dr. Bryan O'Halloran is currently an Assistant Professor in the Systems Engineering (SE) department at the Naval Postgraduate School (NPS). Prior to joining NPS, he was a Senior Reliability and Systems Safety Engineer at Raytheon Missile Systems and the Lead Reliability and Safety Engineer for 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 (CCPSs). 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).

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 works as a senior scientist at VTT Technical Research Centre of Finland in the area of system modeling and simulations. He focuses on simulation, model and data driven approaches to system design, operation and safety assessment. Even 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.

Kristin Giammarco is an Associate Professor in the Department of Systems Engineering at the Naval Postgraduate School, where she teaches courses in system architecture & design, system integration, and model-based systems engineering, and conducts research in the use and development of formal methods for systems architecture modeling. Dr. Giammarco is a member of INCOSE and of the Lifecycle Modeling Language Steering Committee, and currently serves as the Joint Executive Systems Engineering Management (SEM-PD21) Program Academic Associate. From NPS, Dr. Giammarco has earned a Ph.D. in Software Engineering, an M.S. in Systems Engineering Management, and a Certificate in Advanced Systems Engineering. She holds a B.E. in Electrical Engineering from Stevens Institute of Technology.

Douglas L. Van Bossuyt, Ph.D. is a partner at KTM Research, LLC in Tualatin, Oregon. KTM Research specializes in machine vision for manufacturing systems and vision-guided robotics, and has machines deployed in manufacturing facilities throughout North America and Asia. His research focuses on the intersection of design, system modeling, and risk analysis. Dr. Van Bossuyt received his PhD from the Complex Engineered Systems Design Laboratory at Oregon State University in 2012.