INTERNATIONAL DESIGN CONFERENCE - DESIGN 2012
Dubrovnik - Croatia, May 21 - 24, 2012.

DESIGN 2012

A FRAMEWORK FOR MODEL-BASED SAFETY ANALYSIS OF COMPLEX ENGINEERED SYSTEMS

H. Mehrpouyan, T. Kurtoglu and P. Bunus

Keywords: hazard analysis, risk-based design, safety analysis

1. Introduction

The complexity of modern engineered systems is growing constantly. These systems contain a larger number of components that interact with each other in non-linear and often unpredictable ways. Unintended interactions lead to unexpected behaviors and consequences, some of which have proven to be catastrophic. One example of such an accident is the failure in landing of the Mars Polar Lander [Albee et al. 2000], which was attributed to the spurious signals generated by magnetic sensors in the landing legs to indicate the occurrence of the touchdown. While the Mars 2001 lander was connected to the parachute, tests illustrated that the spurious signals were generated in two consecutive steps becauseof the deployment of the landing legs. The Lander's controller software incorrectly accepts these signal noises as an indication of touchdown, eventhough it persisted for two consecutive readings of the sensors and shuts the engines down precipitately. The result of this unwanted interaction caused the spacecraft to crash, even though the software and the landing legs were functioning as expected. The crash occurred as a result of designers not accounting for all the interactions between the control software and the leg deployment component.

A key technical challenge in developing such complex systems is to ensure that catastrophic subsystem and component interactions are well understood and contained prior to full-scale development. Unfortunately, traditional system engineering methodologies are not capable of addressing the ambiguity and uncertainty that naturally exists in complex systems. This paper describes a model-based framework for safety analysis of complex engineered systems. The framework is aimed at safety analysis of cyber-electro-mechanical systems. It is envisioned to assist designers and systems engineers in early identification of undesirable interactions between subsystems and components as well as in the analysis of anomalies and potential faults due to environmental interactions.

The paper is structured as follows. Section 2 presents the background and related research on safety analysis of undesirable interactions and vulnerabilities in complex systems. Section 3 provides an overview of the proposed model-based safety analysis framework. Section 4 specifies the hazard types to be considered for construction of hazard ontology. Section 5, outlines the application of the proposed methodology in analyzing the safety issues for an electrical power subsystem of a sports utility vehicle. Conclusion and future work are presented in Section 6.

2. Related work

It is widely recognized that designing highly complex systems without any associated risks is a challenging task. As observed in [Keating et al. 2003], the subs-systems in complex systems are required to interact directly or indirectly with many other systems which results in a very large number of interactions. Leveson and Dulac [Leveson and Dulac 2005] argue that traditional hazard analysis techniques are based on assumptions that are only valid for specific domains such as simple

mechanical and automotive systems. The hazard analysis in such designs is based on the main assumption that an accident in the system is the result of component failures. Therefore, it is based on a new model which is called systems-theoretic accident modeling and processes (STAMP) [Leveson 2003]. In systematic models such as STAMP, accidents result from several causal factors that occur unexpectedly in a specific time and space. Therefore, the system under consideration is not viewed as a static entity but as a dynamic process that is constantly adapting to achieve its goals and reacting to internal and environmental changes. Consequently, hazards are viewed as complex interactions between system components and their intended environment. The STAMP models are designed based on safety-related constraints and hazards are identified by violation of these safety constraints.

There are many benefits in using the STAMP models as the basis for hazard analysis of a complex system. However, [Johnson and Holloway 2003] state that the STAMP approach has two fundamental weaknesses: 1. It lacks a methodological guideline in implementing the constraint flaw taxonomy, the knowledge require to implement these types of models. 2. Its approach of constructing control models of a complex system are complicated. In addition, [Johnson and Holloway 2003] presents two independent studies for implementing STAMP hazard analysis techniques on the result of accident occurred on the joint project between European Space Agency (ESA) and National Aeronautics and Space Administration (NASA) solar and heliocentric observatory (SOHO). The hazard analysis from each study resulted in significantly different conclusions regarding the cause of failure in the system under study. Another technique for safety analysis is hazard and operability studies (HAZOP) [CISHEC 1977] which is based on modeling the interaction flow between components and recognizing a hazard if components deviate from the operation that was intended for the component during the design. Using HAZOP a set of guide words are used to assist with the identification of such deviations. However, from the context of safety analysis based on interaction between components and their intended environments, HAZOP is unable to produce repeatable hazard analysis of the same accident due to the highly dynamic and unpredictable nature of the interactions between different subsystems and their operational environment. Moreover, depending on the expertise and skills of the safety engineers the deviations can be identified and interpreted erroneously.

Other safety analysis techniques for complex systems include FMEA [MIL-STD 1980] which is a tool for failure analysis in a complex system by connecting the potential failure modes and the resulting effects of the failure to each components to help the designers to evaluate the overall risk levels of the system. FTA [Vesely 1981] is another method to investigate the cause of accidents in a complex system and works bottom up, starting from the undesirable system event tracking the contributing failures that would lead to a high-level failure in the system under consideration. FTA combines all the potential failures and uses boolean logic to identify the failed state. Finally, another technique, called probabilistic risk assessment (PRA) [Henry and Kumamoto 1992] constructs a sequence diagram representing combinations of all failures and fault trees to construct a stochastic model of the system under consideration.

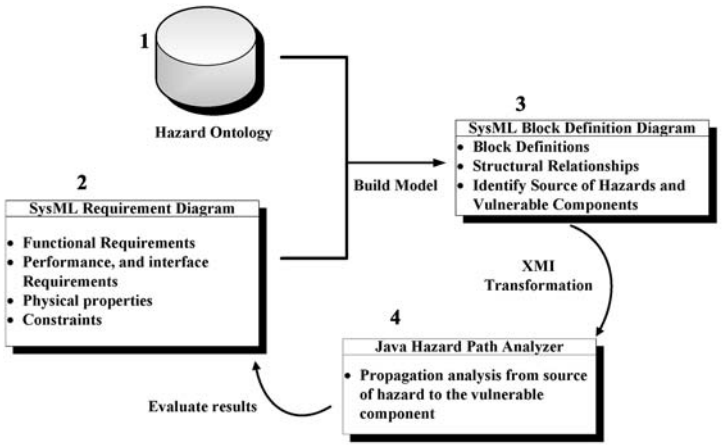

Figure 1. Overview of the model-based hazard analysis process

As discussed in this section existing works on hazard analysis lack accuracy in identification of potential safety issues caused by unexpected environmental factors and subsystem interactions. In addition, the algorithms in the literature do not attempt to identify the hazards within the system in the early stages of the conceptual design process. The proposed model-based safety analysis framework in this paper improves the safety analysis process by emphasizing the importance of precision in hazard definitions and integration at the early stages of system design by using an hazard ontology and requirement definition diagrams.

3. Framework overview

In order to identify the potential safety issues an effective safety analysis methodology must be conducted as early as possible in the system development process, ideally at conceptual design level. Therefore, in this paper a framework based on the evaluation of the design architecture, identifying the hazards, and modifying the design to mitigate these safety issues is proposed. The process is an iterative approach, where each cycle is repeated until no hazard is detected by the algorithm. An overview of the process followed by the framework is shown in Figure 1.

4. Hazard types and identification

In recent years, the development of design repositories and ontology-based frameworks has gained extensive attention. These frameworks are applied to manage the complexity of the design information in highly integrated system. A knowledge based ontology is used to specify a structured information model for organizing design knowledge, map requirements, and aid integration of subsystems. However, these ontologies do not provide any hazard information, even though the designers need hazard type information for each component and connection in order to analyze their threats and effects on the overall system. Therefore, a hazard ontology need to be constructed for each system design based on the hazard and vulnerability associated with each component in the system. In this context, hazard is the potential source that causes harm and constitutes deviation from intended design or operation. These hazards can be caused by the interactions between the components or environmental impact on the system. An example of such a common source of unsuspected hazard is sources and propagation paths of stored energy in electrical, chemical, or mechanical form. For the purpose of this work, the hierarchical hazard types in [Malin and Fleming 2006] are used as a reference to create a general hazard ontology for these types of hazard sources. Note that each category of energy source outlined in Table 1, is required to be methodically traced from the perspective of the conceptual design components and across subsystem interfaces to locate possible hazardous deviations. Creating an ontology for each design problem requires identification of the source of hazard in almost any circumstance which is only possible if detail knowledge of the system and its operation is known.

5. Model-based automated safety analysis example: SUV power subsystem

The proposed design and safety analysis process for early identification of the unexpected hazard sources and propagation paths is based on the conceptual design information. Conceptual design is a preliminary stage of the design process that describes the requirements comprehensively and abstractly, while identifying the optimized principle and solution to be used for the design. To initiate the conceptual design process, it is strongly recommended to proceed with the development of product architecture which is based on the functional model of the product. However, most existing functional models are difficult to translate into functional architectures for early hazard analysis. This transformation is challenging since the construction of a complex system with integrated hazard information requires designers to map the design requirements, the components' hazard-vulnerability properties, and hazard ontology models using a unified modelling environment. Therefore, a modeling language that provides a simple but powerful approach for modeling a wide range of engineering processes is required. The System Modeling Language (SysML) [Friedenthal et al. 2004] is a graphical modeling language for systems engineering applications. SysML is particularly an effective

tool to be used during specification and design of system engineering for specifying safety requirements, structure, and functional behaviour of the system under consideration [Weilkiens 2008]. SysML in our framework is used to capture and integrate design and safety information during the conceptual design process with particular focus on system functions and structure.
More specifically, two main categories of requirement and structural diagrams are used to provide ontalogies and component connection models for identifying and investigating system functions, treats, and safeguards. A requirement diagram enables designers to construct a system and safety requirement model from a text-based specification document and identify the relationship between these constraints. In addition, this diagram is used to trace specifications to model elements, track model elements that satisfy a particular specification, and verify whether the requirement is fulfilled by each model element. Block definition diagram is a sub-category of structure diagram and is used to connect components and define their properties, operations, relationships, hazards, vulnerabilities, and transmitted entities. The block definition diagram is derived from the requirement diagram which in turn is derived from the system specification document. In the block definition diagram, the default hazard, vulnerability, and transmitted risks are associated with each component by the use of hazard ontology, which provides a structure for matching hazard and vulnerability types with each component in the system.

Table 1. Hierarchical hazard type [Malin and Fleming 2006]

Cause of Hazardous Source	Energy	
Internal Interaction	Electrical	
	Mass/Gravity/Height	falls and drops
	Rotational Kinetic	
	Pressure/Volume	container ruptures
	Linear Kinetic	projectiles
	Chemical Reactions	corrosion
	Thermal	heat, cold
	Etiologic	viral
	Ionizing radiation	gamma
	Noise and Vibration	
External Interaction	Radiation	
	Explosion	
	Projectiles	
	Noise	
	Vibration	
	Fire	
	Atmospheric	

5.1 SUV power subsystem

The proposed model-based hazard methodology is applied to the SUV power subsystem. The SUV power subsystem is designed to deliver power to select loads in the engine. Figure 2 displays the existing design of the SUV power subsystem, containing a brake pedal, battery pack, power control unit, electrical power control unit, accelerator, and electric motor generator.

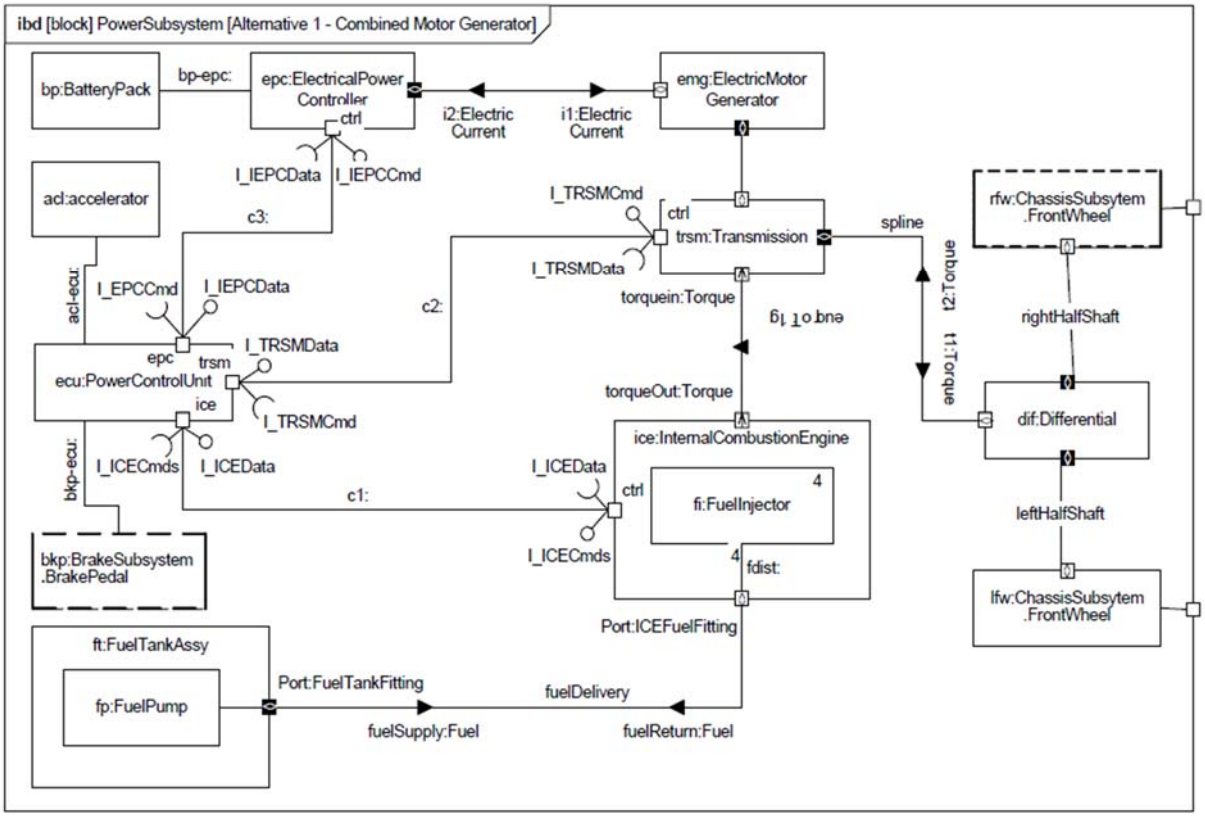

Figure 2. Internal structure of the power subsystem

5.2 Identifying hazard-vulnerability pairs

The first step in identifying the hazardous scenarios is to construct a hazard ontology for the SUV power subsystem design problem. Table 2 illustrates the developed hazard ontology and libraries of types of components, hazards, vulnerabilities, and transmitted entities for hazard analysis of the power subsystem under consideration.

Table 2. Hazard ontology-integral interaction: EMI

Components	Source of Hazard	Vulnerability	Hazard Transmission
Battery Pack	Electromagnetic interference(EMI)		
ransmission		EMI	
Power Control Unit		EMI	
All Components			EMI
All Connection			EMI

Next, a SysML requirement diagram for the specified SUV power subsystem is created using the subsystem design requirements. Figure 3 depicts the corresponding SysML requirement diagram derived from subsystem constraint. In this scenario the SUV power subsystem requirement diagram plays an important role in the system modeling by illustrating how the outlined constraint is satisfied by the system elements in the block definition diagram. The SUV power subsystem block definition diagram describes the internal system structure of the subsystem design using a block as its basic unit. Each block in the block definition diagram defines a collection of specifications such as properties, operations, relationships, hazards, vulnerabilities, and transmitted risks. In addition, each operational mode has a function and side effect action associated with it.

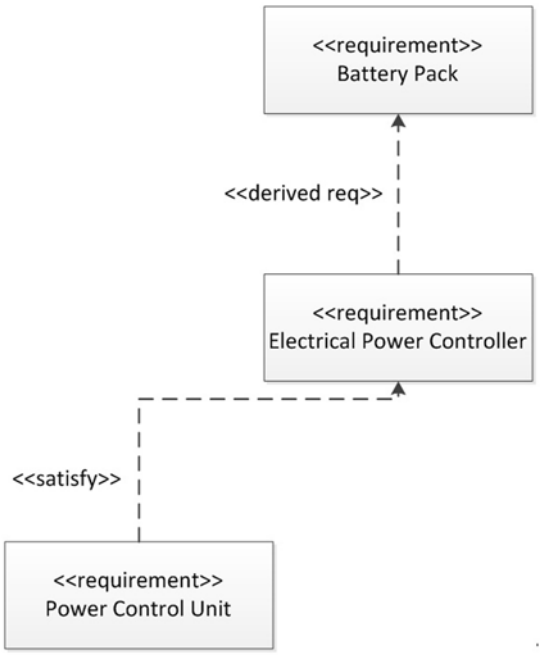

Figure 3. Requirement transformation to SysML requirement diagram

Battery pack component may have the operational modes on and off. The on-mode has the functional action of generating power and a side effect action of generating EMI. As illustrated in Figure 5, two hazard paths are identified for the battery pack block. On the other hand, the power controller unit, and transmission are vulnerable to the generated EMI hazard. These types of information are provided by the hazard ontology database constructed as part of the first step. As depicted in Figure 4, block definition diagram models the causal relationship between the hazard source in this case the battery pack and the impacted targets which are the power controller unit and transmission.

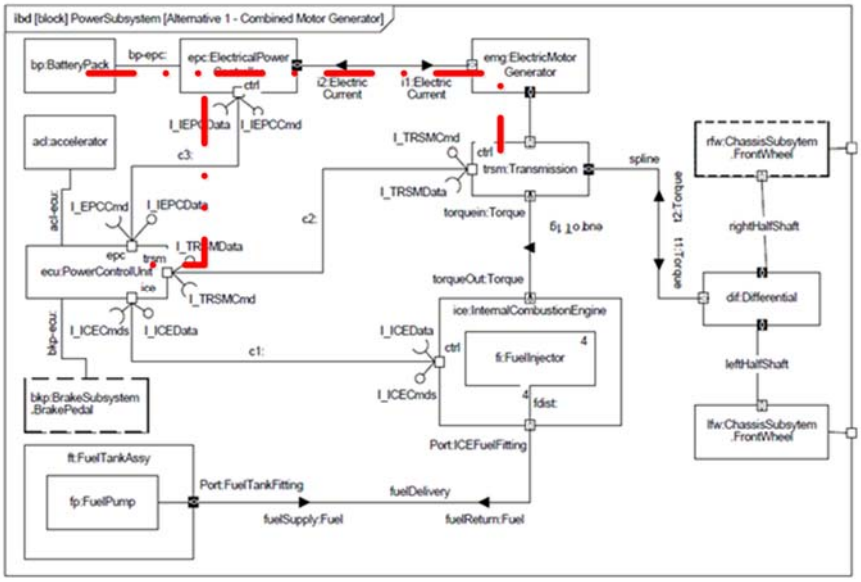

Figure 4. SysML block definition diagram including hazard parameters

5.3 Hazard path analysis

Although, the analysis of the constructed block definition diagram identifies the source of hazards and susceptible components in the system design, it does not verify safety violations. Since the threats

introduced to the system by a hazard source may propagate from the hazard source to the vulnerable components via other components and connections, they might be mitigated or eliminated.
Given that in the block definition diagram all the components and connections are associated with the hazard carrier type, in this paper the path analyzer procedure is proposed to compare the hazard type with the specification of each component. If the component cannot mitigate the effect of the hazard, it is propagated to the next component or connection while if the component can eliminate the threat caused by the hazard, the proposed path analyzer deems the specific hazard as resolved. The proposed path analyzer is based on the block definition diagram that is further transformed to a XML Metadata Interchange (XMI) file to enable quick and easy hazard path analysis through a javabased application called XMISearch. In the first step, the java-based hazard path analyzer searches for hazardous components, in this case the battery pack with the hazard type of EMI. This thread maybe propagated in all direction through conducting wires. In the second step, the process searches for potentially vulnerable components that are susceptible to the identified hazard in the previous step.
The susceptibility of component is recognized by comparing the type of vulnerability of the component with the type of identified hazard. For the SUV power subsystem under consideration, the simple depth-first search is implemented. As illustrated in Figure 4, there are two hazard paths to be examined by the hazard path analyzer: from the battery pack to the power control unit, and transmission. In order to analyze the path from battery pack to the power control unit, the path analyser inspects all the connections and components between the identified components for matching hazard transmitter types. This allows the algorithm to determine whether the hazard traverses from the source to the potentially vulnerable components. For the SUV power subsystem under consideration all the connections and components are carrier of EMI hazard. Therefore, the examined path is recognized as hazardous. Figure 5 illustrates the input and output of the proposed hazard path analyzer.

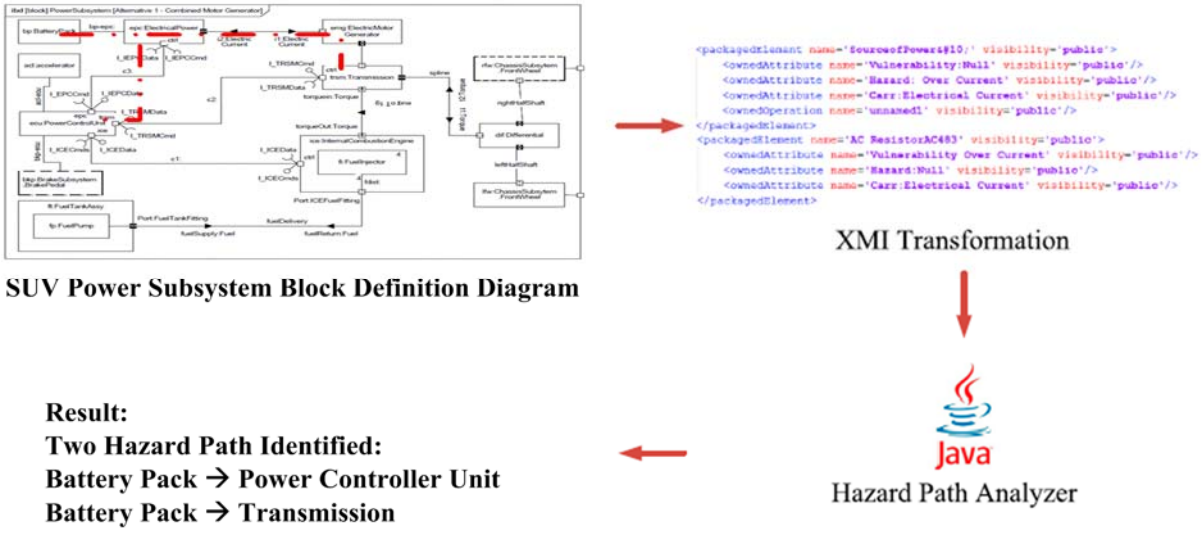

Figure 5. Input and output of hazard path analyzer

Note that the outcome of the model-based hazard analysis for the SUV power subsystem allows the designers to modify the requirement specification document by including additional constrains that prevent the detected hazard from propagating from the battery pack to the vulnerable components.

6. Conclusions

Conventional safety-analysis approaches are not adequate enough to predict and prevent types of system accidents, where the cause of accident is not the result of an individual element failure or human error. The key to a safe and reliable design of complex systems is to ensure that not only the

individual components and technologies but also their integrations are reliable and effective, resulting in safe and reliable systems.

In our approach, to ensure safety and reliability, hazards and vulnerabilities information of components and subsystems are incorporated into the design process of the system as early as possible. At the early stages of design, where firm decisions about the use of specific components and connections have not been made yet, system designers can apply the proposed hazard detection methodology to avoid erroneous designs. The proposed methodology transforms requirement and hazard information and enables the investigation of system interactions and identification of hazard scenarios. In future work, more complex systems or sub-systems with combinations of hazards and vulnerabilities associated with each component can be evaluated.

References

Albee, A., Battel, S., Brace, R., Burdick, G., "Report on the loss of the mars polar lander and deep space 2 missions." NASA STI/ Recon Technical Report N, March 2000.

CISHEC, "A guide to hazard and operability studies." The Chemical Industry Safety and Health Council of the Chemical Industries Association Ltd,, 1977

Friedenthal, S., Moore, A., Steiner, R., "A Practical Guide to SysML: The Systems Modeling Language". Addison-Wesley Professional, 2004.

Henley, E. J., Kumamoto, H., 1992. Probabilistic Risk Assessment. IEEE Press

Johnson, C. W., Holloway, C. M., "The esa/nasa soho mission interruption: Using the stamp accident analysis technique for a software related mishap," Software: Practice and Experience, vol. 33, p. 11771198, 2003.

Keating, C., Rogers, R., Unal, R., Dryer, D., Sousa-Poza, A., Safford, R.,"System of systems engineering," Engineering Management Journal, vol. 15, no. 3, pp. 36–45, Sept. 2003.

Leveson, N. G., "A New Accident Model for Engineering Safer Systems", Safety Science, 2003.

Leveson, N., Dulac, N., "Safety and risk driven design in complex systems of systems," in Proceedings of the 1st NASA/AIAA Space Exploration Conference,Orlando, Florida,, Feb. 2005.

Malin, J. T., Fleming, L., "Vulnerabilities, influences and interaction paths: Failure data for integrated system risk analysis," Aerospace Conference, 2006 IEEE, 2006.

MIL-STD-1629A, 1980. "Military Standard: Procedures for Performing A failure Mode, Effects and Criticality Analysis". MIL-STD-1629A, Department of Defense Washing- ton DC.

Vesely, W. E., 1981. "Fault Tree Handbook". Division of the System Safety Office of Nuclear Reactor Regulation, US Nuclear Regulatory Commission, Washington DC, DeparT ment of Defense Washington DC.

Weilkiens, T., "Systems engineering with SysML/UML: modeling, analysis, design" Morgan Kaufmann, 2008.

Dr. Tolga Kurtoglu
Area Manager
Palo Alto Research Center
3333 Coyote Hill Rd, 94304, Palo Alto, CA, USA
Telephone: +1 – 650 – 812 4714
Email: kurtoglu@parc.com