Addressing Uniqueness and Unison of Reliability and Safety for a Better Integration

Zhaofeng Huang, Ph.D., Aerojet Rocketdyne
Fayssal Safie, Ph.D., NASA

Key Words: Reliability, System Safety, Failure Mode and Effects Analysis (FMEA), Hazard Analysis, Fault Tree Analysis (FTA), Probabilistic Risk Assessment (PRA), Reliability Allocation and Prediction

SUMMARY & CONCLUSIONS

Over time, it has been observed that Safety and Reliability have not been clearly differentiated, which leads to confusion, inefficiency, and, sometimes, counter-productive practices in executing each of these two disciplines. It is imperative to address this situation to help Reliability and Safety disciplines improve their effectiveness and efficiency.

The paper poses an important question to address, "*Safety and Reliability – Are they unique or unisonous?"* To answer the question, the paper reviewed several most commonly used analyses from each of the disciplines, namely, FMEA, reliability allocation and prediction, reliability design involvement, system safety hazard analysis, Fault Tree Analysis, and Probabilistic Risk Assessment. The paper pointed out uniqueness and unison of Safety and Reliability in their respective roles, requirements, approaches, and tools, and presented some suggestions for enhancing and improving the individual disciplines, as well as promoting the integration of the two.

The paper concludes that Safety and Reliability are unique, but compensating each other in many aspects, and need to be integrated. Particularly, the individual roles of Safety and Reliability need to be differentiated, that is, Safety is to ensure and assure the product meets safety requirements, goals, or desires, and Reliability is to ensure and assure maximum achievability of intended design functions. With the integration of Safety and Reliability, personnel can be shared, tools and analyses have to be integrated, and skill sets can be possessed by the same person with the purpose of providing the best value to a product development.

1 INTRODUCTION

Reliability, by definition, is the probability that a system or component performs its intended functions under specified operating conditions for a specified period of time [1-3]. More broadly, Reliability Engineering is an engineering discipline that deals with how to design, produce, ensure, and assure reliable products to meet pre-defined product functional requirements [1-3].

Safety is defined as the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [4-5]. System Safety is defined as the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the product life cycle [4].

It is obvious that from their definitions, Reliability and Safety serve different, though related, purposes. However, it has been observed that, both in theory and in practice, Reliability and Safety often have not been clearly differentiated in terms of their roles, objectives, and approaches. This creates some confusion, inefficiency, and, sometimes, counter-productive practices in executing these two disciplines. There is a need to address this issue for clarification, and also to define and develop methods and tools to integrate these two disciplines for better support of a product development.

In this paper, we first review key objectives and tasks of Reliability and Safety, respectively, in Sections 2 and 3, which set the tone for the follow-on discussions of the uniqueness and unison of Reliability and Safety in Section 4. In Section 5, we present some ideas and approaches to enhance and improve the two disciplines with distinctive and focused roles, better integration, and unique sets of skills and tools.

2 RELIABILITY OVERVIEW

Reliability, by its definition, is primarily addressing the achievability of a set of ***given*** design functions. Therefore, by nature, reliability tasks are design-centric, that is, all reliability tasks start with design information at hand and finish with an evaluation about reliability of the design being analyzed. Typical reliability tasks include Failure Mode and Effects Analysis (FMEA), or Failure Mode, Effects and Criticality Analysis (FMECA), Critical Item List (CIL), reliability allocation and prediction, reliability involvement in design and development. The following is a brief overview of these tasks.

2.1 FMEA/FMECA/FMEA/CIL

FMEA [6-7] is a bottom-up, inductive reliability analysis tool. It systematically analyzes a product's design, element-by-element, in terms of its failure definition (failure mode), the failure causes, and failure effects. It starts from the basic product design definition which, during conceptual design, is a set of function designs, and during detailed design, is the list of the hardware or software components. It inductively infers the system failures from the design presented. The FMEA also addresses the failure cause control and requires mitigations in place to reduce the severity or the likelihood of the failure mode. The FMEA evolves to be a FMECA when the probability of occurrence of each failure mode is estimated, allowing risk levels to be identified, ranked, and prioritized. Sometimes, RPN (risk prioritization number, which is the

product of likelihood, severity and detection scores of the failure mode) is used for failure mode ranking and prioritization. Critical Items List (CIL) is an analysis that is performed on the high severity failure modes identified by FMEA. It lists the measures that are required to eliminate or to reduce the likelihood of failure mode occurrence. Some typical CIL measures include design requirements, test requirements, manufacturing and quality requirements, and operation and field support requirements.

One of the key ground rules of the FMEA or FMECA is "one basic element at a time," that is, when analyzing Function or Component or Piece Part A, we assume all other interacting functions, components, piece parts, and interface conditions are per specifications (or we call "as-designed and as-built condition"). This assumption is in line with design practice. For example, we don't design a turbopump to accommodate an out-of-specification inlet condition. This assumption greatly simplifies the FMEA thought process and makes the FMEA approach viable. Otherwise, it would drastically grow in complexity if all combinations of failures were examined. But this simplification also leads to the limitation of the FMEA; that is, simultaneous and multiple failure mode causes and effects, and system interactions are usually not addressed in FMEA.

2.2 Reliability Allocation and Prediction (RAP)

RAP brings reliability analysis from qualitative, such as failure mode identification, to quantitative, such as quantifying the probability of the failure modes and failure scenarios. There are many RAP modeling techniques and methods defined by military standards, reliability text books, and literature articles [9-11]. The primary purposes of RAP are to derive numerical reliability requirements to guide the product Design-For-Reliability effort, assess the product's reliability and provide reliability data to assist design trades and design optimization, and document RAP results to assure compliance with customer requirements or realization of program reliability goals.

The key task of RAP is the quantification of reliability, defined as the probability that a system or component performs the intended functions under a set of specified operational conditions for a specified period of time. The most widely used reliability prediction method is reliability block diagram (RBD). Each block in the RBD can be a function block or a component/piece part block. Therefore, an RBD is primarily a simplified design representation of the system being analyzed. Since the prediction is based on RBD, which is an inductive reliability approach, the system interaction and function dependency are usually not explicitly addressed. The other RAP methods include stress-strength interference approach and industry standard failure rate databases [9-12]. All these methods start from components or sub-systems being designed and usually do not explicitly address system interactions and interfaces.

2.3 Reliability Involvement in Design and Development

Reliability involvement in design and development includes the activities of reviewing and incorporating lessons learned into design, addressing failure modes and failure causes associated with the designs, and using qualitative and quantitative reliability data to support design trades, design optimization, and risk mitigation and controls [1-3, 10, 12]. For lessons learned activity, Reliability Engineers gather and summarize lessons learned from past failure analysis reports from similar programs and products and present the data to integrated product teams (IPTs) throughout all design phases to make sure the design will address identified failure modes and causes. Reliability Engineers discuss failure mode and cause concerns, and lead or facilitate IPT to develop failure mode and cause elimination, prevention, and mitigation. For design trade activity, Reliability Engineers provide reliability analyses that summarize reliability pros and cons, and rank reliability deltas among various candidate/alternative design options to support design decisions.

2.4 Summary of Reliability Tasks

Besides the reliability tasks discussed above, there are other reliability activities and tasks, including reliability program plan development, reliability testing and analysis, reliability verification, failure analysis and prevention, and reliability participation in design reviews. There are some activities and tasks branching out from reliability to support safety, maintainability, availability, and warranty analysis. In summary, the reliability tasks are centered around designs, and bottom-up and inductive in nature from the design information at hand to assess system reliability performance that supports designed function achievability.

3 SAFETY OVERVIEW

Safety, by its definition, is primarily addressing hazardous conditions that may cause personal injury, illness or death, damage to the environment, the product, or facilities. The ultimate concerns of safety may not be specific to the product design. Therefore, by nature, safety analyses are top-down, starting from a top level hazard event such as fire, explosion, personal injury, toxicity, or environment pollution, and trace down and link the top level hazard to product design details. Typical System Safety tasks include hazard analysis and Fault Tree Analysis. Probabilistic Risk Assessment (PRA), under the context of addressing an undesirable system hazard event, is also part of a safety analysis. The following is a brief overview of these tasks.

3.1 Hazard Analysis and Fault Tree Analysis (FTA)

A Hazard Analysis [4] is a systematic analysis of potential hazards associated with the system, their causes, and measures taken to mitigate the hazards. The Hazard Analysis is a top-down and deductive analysis method. It is initiated early in the design phase by identifying a set of top level system hazards and forming hazard list based on customer and regulatory requirements, public safety concerns, or previous history of similar products, and engineering knowledge and judgment. The Hazard List is then developed into a Preliminary Hazard Analysis (PHA), which helps to identify safety critical areas associated with the system being developed, and establish safety design criteria for eliminating, mitigating, and controlling the potential hazard causes. As the design matures, the PHA is evolved into the Subsystem Hazard Analysis

(SSHA) and System Hazard Analysis (SHA), which further analyze hazard events and their interactions within the system that can produce undesired outcomes, and identify the hazard controls and mitigation.

Fault Tree Analysis [13] is a graphical representation of the top level hazards traced down to the intermediate failure events, then down to the hazard cause as the fault tree basic events. Fault Tree Analysis is also a top-down and deductive analysis tool. Fault Tree relationships are described by the fault tree Boolean logic with the typical Boolean gates of AND and OR.

3.2 Probabilistic Risk Assessment (PRA)

PRA is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance [14-15]. PRA is failure scenario based and takes a phenomenological approach to address failure risk from its initiating events to an undesirable end state, such as loss of a launch vehicle or loss of mission. Key elements of PRA include Master Logic Diagram, Event Trees or Event Sequence diagrams, and Fault Trees. The result of the PRA is a set of failure scenarios that lead to a set of end states, the probability of the end states, as well as uncertainty associated with the probability estimates. PRA helps identify the areas where mitigating controls are needed to reduce the risk of the undesirable end states.

3.3 Summary of Safety Tasks

There are other safety activities and tasks, including safety program plan development, safety hazard caution and hazard prevention development, safety testing and verification, safety participation in design reviews and independent safety review, and mishap reporting and investigation. In summary, safety analyses are flowed down from top level hazard concerns and undesirable events, taking a top-down approach to link top level hazards to the product design details for hazard cause control and mitigation. Safety analysis also addresses sub-system or component interactions, interfaces and compounded hazard causes.

4 UNIQUENESS AND UNISON

4.1 Uniqueness of Reliability and Safety

4.1.1 Uniqueness in Their Roles

The role of reliability is to ensure and to assure the achievability of functionality of the product. The role of safety is to ensure and assure the system is safe. Here the word "ensure" represents actions to make it happen. The word "assure" represents making claims and stating confidently that it is true. Reliability addresses the realization of the functional requirements of the components or systems, while Safety addresses the identification of system hazard events and their controls and mitigations. It is misleading to equate unreliable to unsafe since a top level hazard may or may not be related to the component, sub-system, or system design functions. Similarly, a failure-to-function may or may not lead to a hazard event. As an example of this distinction, let's consider a consumer product such as ice cream. The functional requirements of an ice cream product can be flavor, taste, color and nutritional ingredients, while the safety concern is toxicity. Toxicity is not directly affected by the functional requirements such as color or flavor of the ice cream. The role of Reliability is to ensure, through design and production, that flavor, taste, color, and nutritional ingredients of the ice cream meet their specifications. The role of Safety is to minimize the risk of toxicity through a set of hazard cause controls and mitigation during the ice cream production and consuming.

For aerospace products such as rocket engines, reliability concerns and safety concerns overlap greatly, yet still have their own distinct purposes. In one aspect, the function of a rocket engine is to realize a "controlled explosion," as depicted by a Shuttle flight in Figure 1. Here Reliability is concerned with ensuring controllability while Safety is addressing the prevention of that explosion becoming uncontrolled. Another example is in the trade-off of single engine design versus multiple engine design on a launch vehicle, illustrated in Fig. 2. From a reliability viewpoint, the overall function of the engine system is to provide adequate thrust to enable mission success. A single engine is generally more reliable than multiple engines because the single engine has fewer parts, fewer items to fail, less integration complexity, and, therefore, a higher probability of achieving mission success. From a safety viewpoint, a key objective is to ensure the crew is not harmed during the mission, the public is not endangered, and the environment is not damaged. While the proper functioning (i.e. reliability) of individual components plays a role in overall safe function of the system, a vehicle with multiple engines that allows for single engine-out capability will likely have a better safety than a single-engine configuration that does not have that capability. In many industry applications, safety devices are designed and implemented to mitigate hazardous conditions. However, components of safety devices, themselves, introduce failure modes and failure causes which adversely affect reliability.

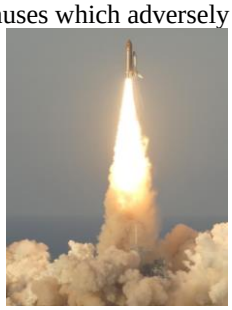

Figure 1 Illustration of a "Controlled Explosion" – A Shuttle Flight

Figure 2 Reliability versus Safety in a Single or Multiple Engine Launch Vehicle System

4.1.2 Uniqueness in Their Requirements

The role reliability requirements are closed-ended, product function specific within the boundary of the design functions. All reliability requirements are internally imposed, mirroring the functional requirements within the design space. For example, a requirement for a turbopump of a rocket engine is to deliver a required delta pressure with a desired probability. In contrast to reliability requirements, safety requirements are open-ended, non-function specific such as the statements "no fire or explosion," "no harm to the human being." Reliability requirements are mostly driven by product functional requirements, while safety requirements are driven either by the desire to avoid negative customer, user, and societal impacts, or by externally imposed constraints, such as regulatory and legal policies, and restrictions.

4.1.3 Uniqueness in Their Approaches

The reliability approach is primarily bottoms up, starting from function statements, or the component or the piece part that is designed to realize the intended functions. The reliability tools such as Failure Mode and Effects Analysis (FMEA) and Reliability Block Diagrams (RBD) all start from individual component or sub-systems. The FMEA examines, function-by-function or component-by-component or piece part-by-piece part, all credible failure modes and their effects that may impair the intended functions. In contrast to the reliability approach, the safety approach is primarily top-down. Hazard analysis and fault tree analysis are typical examples of the safety approach, which start from identifying top level hazard events and traces down to the lower level triggering events until the bottom basic events are exhaustively listed, and controls and mitigations for these basic events are established to ensure and to assure safety. While the reliability approach is typically looking for component failures that lead to an inability to function, the safety investigates all conditions that can result in a hazard.

4.1.4 Uniqueness in the Analysis Boundaries

Safety analysis considers sub-system and component interactions and common causes from multiple components and sub-systems, while reliability analysis usually only focuses on the component or sub-system or the functional element being analyzed and assumes all other interacting components are at an as-designed and as-built condition. As such, external system vulnerability and uncertainty are often not explicitly considered in reliability analysis, but may be required to be addressed as part of the safety analysis. History has also shown that there were some system accidents [5] where none of the components or individual functions within the system failed. In general, the analysis boundary of safety is broader than reliability's.

4.2 Unisons of Reliability and Safety

4.2.1 Unisons in Their Roles

One common aspect of Safety and Reliability is that both are addressing some anomalous and undesirable conditions. But the criteria of anomaly or undesirability can be different, although unreliability may often lead to an unsafe condition or vice versa. Both disciplines examine the system and component design, development, and operation for their possible failures or undesirable events, develop measures to gage its success, and propose implementations to achieve its respective objectives. Depending on the product types, the roles of Safety and Reliability can be more or less overlapping, or can be closely or sometimes directly related, where a failure-to-function leads to an unsafe condition. For rocket engine products, it is observed that the majority of hazard causes are functional failures of certain components or sub-systems. Therefore, the roles of Reliability and Safety are heavily overlapping.

4.2.2 Unison in Requirements

There is more overlap between reliability and safety requirements in aerospace products than in consumer products. For example, for rocket engines, a loss of mission due to lack of thrust is a direct violation of reliability requirement, but it is also a safety hazard event since it immediately imposes a higher threat to the astronauts' safety. For consumer products, such as ice cream, as we discussed earlier, reliability and safety requirements can be very much non-overlapping.

4.2.3 Unison in Analysis Methodology, Tools, and Techniques

There is a central theme in both reliability and safety analysis methodology, tools and techniques. That is to ask "*what can go wrong*?" and "*how can we prevent and mitigate that*?" As we discussed earlier, reliability analysis is primarily bottoms-up, while safety analysis is primarily top-down. Where they meet in the middle can be common and overlapping. For example, for rocket engine products, safety hazard analysis identifies top level hazard events, then traces these hazard events down to the hazard causes through fault trees. Often, those hazard causes are the failure modes or associated causes identified in FMEA. It is this overlapping and connection that provides opportunity for integration and efficiency improvement. Next section will discuss linkage of reliability and safety tools, and how safety and reliability tools play together to address reliability and safety issues.

4.2.4 The Link of Safety and Reliability – A Space Shuttle Case Study

Given the safety and the reliability discussions above, it is clear that safety and reliability engineering are two different areas serving different functions in supporting the design and operation of launch vehicles. However, safety and reliability tools and techniques, in many cases, play together in a complementary manner [15]. A good example is the Space

Shuttle External Tank (ET) Thermal Protection System (TPS) safety assessment, shown in Fig. 3, using probabilistic risk assessment process to assess the risk of foam debris hitting the Orbiter and leading to a loss of crew (LOC) [16]. Starting from the top, the risk assessment, which is simulation based, used the ET TPS void distributions derived from the dissection data of the ET components under consideration as the initial input. The void distributions were then used in a fracture mechanics model to generate divots. The divots generated were then transported to evaluate the damage impact on the Orbiter. The output of the model was the probability of Orbiter damage exceeding a specified tolerance limit set for the Orbiter. The risk assessment model, although limited in scope, was very critical in understanding and communicating the safety/risk of the ET TPS in flight. The results of the risk assessment were used as part of the rationale to Return-to-Flight (RTF) after the Columbia accident [17]. It is important to note that the reliability of the foam generation using fracture mechanics was a key input to the probabilistic risk assessment. This application represents a good illustration of the complementary nature of safety and reliability analyses.

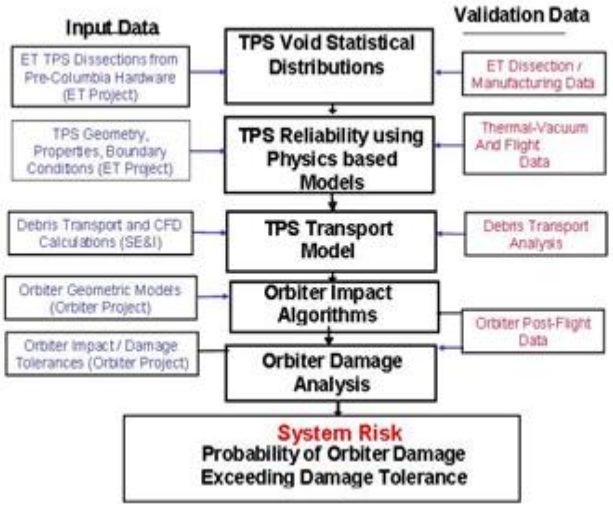

Figure 3 Shuttle ET TPS Foam Risk Assessment Logic

5 ENHANCEMENTS AND IMPROVEMENTS

5.1 Enhancing the Roles

For Safety, the objective is to identify system hazards and ensure their causes are controlled. An enhanced role would be achieved by determining all of the top level safety requirements of the system, directly from customer requirements or derived, and establishing clear linkages between the requirements, their associated system hazards, and the features of the design or process that control the hazards and their causes. For Reliability, the objective is to ensure that a design maximizes its probability of performing its intended function. Enhancement of reliability role is to focus on a better linkage between the function(s) that are needed to be performed by the system and its components, and the design solutions being incorporated into the design to help maximize functional success.

5.2 Enhancing the Integration

As we have pointed out, there are opportunities for enhancing the integration between Safety and Reliability. As discussed in Section 4, there is an overlap in analysis and data elements among the FMEA, reliability prediction, hazard analysis, and fault tree analysis. Reliability and Safety disciplines need to define best practices for integrating these analyses to provide the best value to the customers, ensuring the analysis results are useful, consistent, cohesive, mutually-compensating, and non-redundant. Figure 4 is a concept from the Society of Automotive Engineers (SAE) [18] that attempted to integrate reliability analysis and safety analysis. Figure 5 presents an integrated reliability and safety modeling approach.

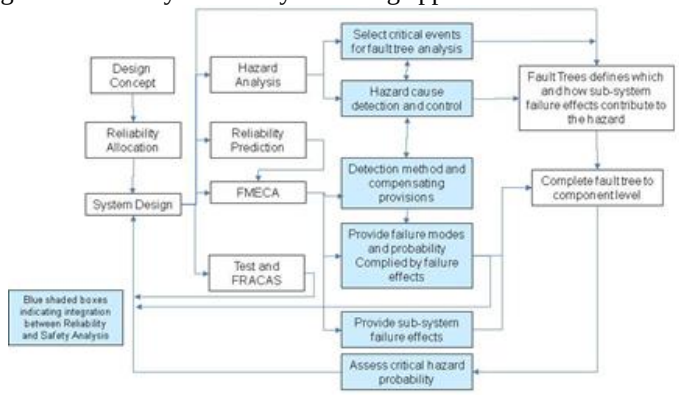

Figure 4 SAE Recommended Reliability and Safety Analysis Integration Flow [18]

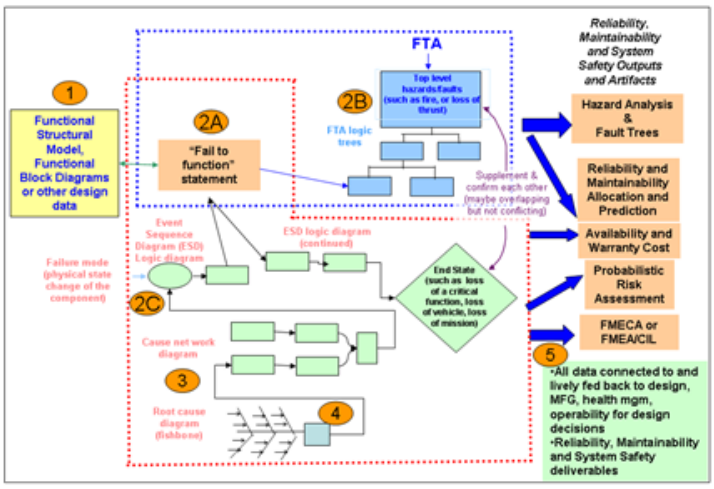

Figure 5 An Integrated Reliability and Safety Modeling Approach

5.3 Improving Tools

As part of the integrated reliability and safety approach described above, the reliability and safety analysis toolsets also need to support this integration. While the individual disciplines will still perform their respective analyses, the tools being used need to allow for integration of shared information among the FMEA, hazard analysis, reliability modeling and prediction, and PRA. Additionally, the tools should be integrated with other engineering discipline tools from Design, Systems Engineering, Structural Engineering, Quality, and Configuration Management for improved efficiency.

5.4 Improving Technical and Personal Skills

As unique roles Reliability and Safety play, the skill set and skill levels of Reliability and Safety Engineers need to be enhanced in the reliability and safety discipline areas, as well as in an IPT environment. For example, for a Reliability Engineer to be successful within an IPT environment to help maximize the product functional achievability, the Reliability Engineer needs to be knowledgeable about the product designs and be familiar with other disciplines' analyses in order to help implement solutions for failure prevention and mitigation. Reliability Engineers also need to be open-minded about failures. The definition of the failure can be in a general sense, such as failure to assemble, failure to achieve test objectives, and failure to meet schedule, etc. Reliability Engineers need to look for opportunities to help IPTs and programs identify, prevent, and mitigate the failures with applicable reliability tools and techniques.

Safety discipline also needs to cultivate safety experts with specialized knowledge on the products your company is producing. The objective is for safety engineers to master the knowledge and hands-on skills on the system hazards and undesirable events on the product relevant to the appropriate regulatory or customer requirements, safety certification processes, insurance implications, legal and society ramifications, and typical hazard cause controls and mitigation methods. Safety engineers need to address system and component interactions, external threats on safety, such as vulnerability and uncertainty in operating environments, and user application specifics.

REFERENCES

1. Department of Defense, *MIL-STD-785 Reliability Program for System and Equipment Development and Production*, Washington, D.C., 1980
2. G.W. Ireson, C.F. Commbs, and R. Moss, R., *Handbook of Reliability Engineering and Management*, John Wiley and Sons, New York, New York, 1995
3. D.T. O'Connor, *Practical Reliability Engineering*, John Wiley & Sons, New York, 2002
4. Department of Defense, *MIL-STD-882E Standard Practice for System Safety*, Washington, D.C., 2012
5. N. Leveson,, *Engineering a Safe World: Systems Thinking Applied to Safety*, The MIT Press, 2011
6. Department of Defense, *MIL-STD-1629A Procedures For Performing A Failure Mode, Effects and Criticality Analysis*, Washington D.C., 1980
7. D.H. Stamatis, *Failure Mode and Effect Analysis: FMEA From Theory to Execution*, American Society for Quality, Milwaukee, 2003
8. Department of Defense, *MIL-STD-756 Reliability Modeling and Prediction*, Washington D.C., 1982
9. Department of Defense, *MIL-HDBK-217F Reliability Prediction of Electronic Equipment*, Washington, DC., 1991
10. E. Nikolaidis, D.M. Ghiocel, and S. Singhal, *Engineering Design Reliability Handbook*, CPC Press, London, 2005
11. Z. Huang, Y. Jin, "Reliability Prediction Method: A Survey and Selection for Mechanical Design-for-Reliability," ASME Design Engineering Technical Conference, 2009-87103, San Diego, California, 2009
12. E.B. Haugen, *Probabilistic Mechanical Design*, John Wiley & Sons, 1980
13. NASA, *Fault Tree Handbook with Aerospace Applications*, Washington, DC. 2002
14. NASA, *Probabilistic Risk Assessment Procedure Guide*, Washington, DC., 2002
15. F.M. Safie, R. Stutts, Z. Huang, "Reliability and Probabilistic Risk Assessment – How They Play Together," Proc. Ann. Reliability & Maintainability Symp., January 2015
16. F. M. Safie and R. L. Belyeu, "NASA New Approach for Evaluating Risk Reductions Due to Space Shuttle Upgrades," Proc. Ann. Reliability & Maintainability Symp., January 2000, pp. 288-291.
17. NASA, "Report of Columbia Accident Investigation Board," NASA 2003
18. Society of Automotive Engineers, "Reliability and Safety Process Integration," AIR 5022, Warrendale, PA, 1996

BIOGRAPHIES

Zhaofeng Huang, Ph.D.
Aerojet Rocketdyne
P.O. Box 7922, RFA45, 8900 De Soto Ave.
Canoga Park, CA 91309, USA

e-mail: Zhaofeng.huang@rocket.com

Dr. Zhaofeng Huang is a Technical Fellow at Aerojet Rocketdyne in the areas of Reliability Engineering and Probabilistic analysis under Systems Engineering. Zhao has been working at Aerojet Rocketdyne for 28 years and supported (is supporting) many past and on-going propulsion and energy programs in developing and implementing advanced reliability methods, design-for-reliability approaches, and probabilistic risk assessment for reliability and safety enhancement. Zhao holds a Ph.D. and MS in Mechanical Engineering from University of Southern California, MS in Statistics from Iowa State University, MA in Math from Temple University, and BS in Computational Math from Shanghai University of Science & Technology. Zhao is a Certified Reliability Engineer and Certified Quality Engineer from American Society for Quality, and has Manufacturing Engineering Certificates from UCLA and Society of Manufacturing Engineers.

Fayssal M. Safie, Ph.D., CRE
NASA Marshall Space Flight Center/QD30
Huntsville, Alabama 35812, USA

e-mail: fayssal.safie@msfc.nasa.gov

Dr. Faysal Safie is currently serving as The NASA Reliability and Maintainability (R&M) Technical Fellow. He joined NASA in 1986 as a reliability and quality engineer at Marshall Space Flight Center (MSFC). He received over 50 honors and awards, including the NASA Exceptional Engineering

Achievement Medal, the NASA Flight Safety Award, the NASA Quality Assurance Special Achievement Recognition (QASAR) Award, and the NASA Silver Snoopy Award. He published over 40 papers in R&M Engineering, Probabilistic Risk Assessment, System Safety, Quality Engineering, and Computer Simulation. Besides his responsibility as a NASA Tech Fellow, Dr. Safie is serving as an Adjunct Professor in the Systems Engineering Department at the University of Alabama in Huntsville (UAH). He has a Bachelor degree in science and a Bachelor, a Master, and a Doctorate in engineering.