A multilevel framework of system safety: Technical failures, human factors, organizational behavior, and societal influence
Mark S. Avnet, Tonya L. Smith-Jackson

This paper provides an overview of a developing research program intended to advance the theory and practice of system safety by explicitly examining the causes of accidents from a multilevel perspective, including proximate technical causes, human error, organizational culture, and societal influences. A growing body of literature on systems approaches to safety has laid the foundation for an interdisciplinary effort examining the nature of the relationships across these levels. At each level, a distinct and rich set of methods, tools, and disciplinary knowledge exists and has been applied to a wide array of system contexts. Each of these disciplinary perspectives provides a unique lens to examine safety in complex engineered systems. The field of system safety has now advanced to a point at which both the disciplinary methods and the holistic systems perspective can be integrated to build a robust and comprehensive understanding of the depth, nuance, and complexity of system safety. The goals of the research are (1) to develop a robust framework for ensuring system safety that offers specific and practical guidelines for system development, management, accident investigation, and policymaking from a holistic, multilevel, and interdisciplinary perspective; (2) to create a universal repository of safety-related knowledge across disparate contexts, industries, and disciplines to serve as the engine for implementing and operationalizing the framework, and (3) to provide a platform for fundamental research focused on the theoretical foundations of each level of the framework. The repository, also called the System Safety Database, will provide a desperately-needed and long-overdue consolidated reference to the existing body of knowledge needed to implement the framework effectively. It will facilitate analysis across disciplines and contexts, allowing researchers and practitioners to use integrated mixed-methods approaches to conduct investigations, analyses, research, and development activities across multiple levels of a system. This work will lead to a fundamental understanding of the overall ecosystem of safety and will provide stakeholders at all levels, from individual operators to policymakers, with the tools and perspectives needed to improve safety in complex socio-technical systems.
Quantifying the ilities: A Literature Review of Resiliency, Flexibility, and Adaptability
Andrew J. Turner, Matt Cotter, William Monahan

This paper presents a literature review of the methods for quantifying system ilities. The ilities are non-functional system characteristics. The motivation for designing systems to express these ilities is in response to the ever increasing complexity of engineered systems, increasing requirements on budget and schedule, and the need to adapt to a rapidly changing world. The systems engineering community has increased its focus on defining and implementing the ilities for over a decade. Many works available in the literature have defined the ilities and their inter-relations. A subset have gone further to quantify the ilities; however, the literature is currently fragmented in its approach. This paper attempts to identify and summarize the various approaches in quantifying the ilities. A systematic literature review was conducted across eight conferences and journals from 2010 to 2015. This paper addresses the findings for resiliency, flexibility, and adaptability, which include definitions or quantifications in 166 documents. The definitions discovered for each of the ilities demonstrated relative agreement, however, many differed in the details. Resilience was found to have an acceptable number of quantified measures. Flexibility and adaptability were found to need further attention from the community to develop additional quantified measures.

Applying the Robustness (Broad Utility) Workflow to Assess Resiliency for Engineered Resilient Systems
Christina Rinaudo, Randy K. Buchanan, Shelia K. Barnett

The Engineered Resilient Systems (ERS) Community of Interest (COI) is one of 17 Science and Technology (S&T) strategic priorities of the Office of the Secretary of Defense. ERS research focuses on developing methods and processes to support model-based systems engineering analysis early in the Department of Defense (DoD) acquisition life cycle. ERS research efforts include defining, quantifying, and developing a methodology to determine platform-based system resiliency. An aspect of DoD resiliency was mapped to the term robustness (also known as broad utility). Through the application of a process described as Needs Context, robustness has been translated into a conceptual mathematical workflow. This study investigated the application of the robustness workflow. The goal was to achieve a mathematical robustness value for a system design alternative using the initial system requirements generated during the development of the Mine Resistant Ambush Protected (MRAP) vehicle.

The MRAP was considered a resilient system that served as a multifunctional platform for the U.S. Military in the Middle East. A secondary outcome was to provide feedback to the analytical community with regard to the workflow and to assist in determining any additional factors necessary for development of metrics to analyze resiliency. This paper will address the application of the robustness workflow and will support the next phase of efforts to quantify resiliency in systems engineering.