

# Competing Failure Risk Analysis Using Dempster-Shafer Theory

William L. Oberkampf<sup>a</sup>, Jon C. Helton<sup>b</sup> and Jay D. Johnson<sup>c</sup>

<sup>a</sup>Validation and Uncertainty Quantification Department  
Sandia National Laboratories\*  
Albuquerque, NM 87185-0828  
wloberk@sandia.gov

<sup>b</sup>Jon C. Helton  
Environmental Decisions and WIPP Support Department  
Sandia National Laboratories\*  
Albuquerque, NM 87185-0779  
jchelto@sandia.gov

<sup>c</sup>Jay D. Johnson  
ProStat, Inc.  
2265 E. Fairview Circle  
Mesa, AZ 85204-5326  
jdjohns@aol.com

High-consequence systems, such as nuclear power reactors, missile systems, and weapon systems, commonly contain security and safety control systems that are closely coupled to enhance security and safety. For example, security systems which control the use or functioning of a system are typically very robust and resistant to unauthorized or unintended use. Similarly, safety systems are designed so that the complete system does not operate or function in any credible accident scenario. Control systems that combine use-control and safety assurance are sometimes referred to as surety systems.

This paper describes a risk analysis of a hypothetical surety system that is exposed to a fire accident scenario. The surety system is exposed to thermal heating such that the security component and the safety component of the system ultimately fail due to high temperature of each component. The security component is commonly referred to as a strong link, indicating that the component is very resistant to mechanical, electrical, or magnetic insults or attacks. The safety component is commonly referred to as a weak link, indicating that the component will fail more easily, relative to the strong link, during accident scenarios. These components are placed in close physical proximity so that they are exposed to similar environmental conditions during an accident scenario. The necessary condition for the high-consequence system to operate is the electrical functioning of the strong link. However, if the weak link has failed, the functioning of the strong link does not allow the high-consequence system to operate. As a result, the surety system is designed to operate in an accident scenario so that there is a competing failure race, with the weak link intended to fail before the strong link.

Risk analysis of the hypothetical surety system is described using Dempster-Shafer theory, which is sometimes referred to as random set theory or evidence theory. The thermal responses of the weak link and the strong link are specified as a functions of time with a simple algebraic model. For heating analyses of complex mechanical/electrical components in fires, there are large epistemic uncertainties in the thermal heating as well as in the thermal response. Epistemic uncertainty is also referred to as subjective uncertainty, reducible uncertainty, or uncertainty due to lack of knowledge. We represent the epistemic uncertainties in the thermal response as interval-valued parameters and alternate-plausible parameters in the algebraic temperature-time model. The failure temperatures of the weak-link and strong-link components are considered to be nondeterministic due to manufacturing variability. The failure temperatures of the population of each component are characterized by specified probability distributions. However, it is assumed that only a few components have been tested, so that epistemic uncertainty is present in the specification of the parameters of each distribution. The Dempster-Shafer analysis is compared with a traditional probabilistic analysis for the probability that the strong link fails before the weak link. It is found that the traditional probabilistic analysis does not fully represent the safety risk.

\*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U. S. Department of Energy under contract No. DE-AC04-94AL85000.