Engineering Safety and Security Related Requirements for Software Intensive Systems

Donald G. Firesmith
Carnegie Mellon Software Engineering Institute

Many software-intensive systems have significant safety and security ramifications and need to have their associated safety- and security-related requirements properly engineered. It has been observed by several consultants, researchers, and authors that inadequate requirements are a major cause of accidents involving software-intensives systems, and poor security requirements prevent the early incorporation of security concerns into the architecture. Yet in practice, there is very little interaction between the requirements, safety, and security disciplines and little collaboration between their respective communities. Most requirements engineers, safety engineers, and security engineers know little about their respective disciplines. Also, safety and security engineering typically concentrates on architectures and designs rather than requirements because hazard and threat analysis typically depends on the identification of hardware and software components, the failure of which can cause accidents and vulnerabilities which can enable successful attacks. This leads to safety- and security-related requirements that are often ambiguous, incomplete, unverifiable, and even missing. This tutorial begins with a single common realistic example of a safety- and security-critical system that will be used throughout to provide good examples of safety- and security-related requirements. The tutorial provides a consistent ontology of safety, security, and requirements concepts and terminology, provides clear definitions and descriptions of the different kinds of safety- and security-related requirements, and finishes with a practical consistent combined process for engineering them.

29th International Conference on Software Engineering (ICSE'07 Companion)
0-7695-2892-9/07 $20.00 © 2007 IEEE