Engineering Safety-Related Requirements For Software-Intensive Systems

Donald Firesmith
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213 USA
+1 (412) 268-6874
dgf@sei.cmu.edu

ABSTRACT

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

Categories and Subject Descriptors

D.2.1 [**Requirements/Specifications**]: Elicitation methods and methodologies

General Terms: Management

Keywords

Requirements Engineering, Safety, Safety Requirements

1. GOALS AND OBJECTIVES

The overall goal of this one-day tutorial is to teach the attendees how to engineer safety-related requirements for software-intensive systems. Specific objectives include learning the:

- Different types of safety-related requirements including their purpose and composition.
- Basic tasks of safety engineering that are related to engineering safety-related requirements.
- Relationship between safety quality subfactors and the quality criteria of safety requirements.

2. Audiences

The intended audience for this tutorial includes:

- Requirements engineers who must collaborate with safety engineers to engineer the safety-related requirements.
- Safety engineers who must perform the hazard and risk analysis that drives the safety-related requirements and who must collaborate with requirements engineers to engineer these requirements.
- Stakeholders in safety-related requirements including subject matter experts, customer representatives, architects, software engineers, testers, and certifiers.

3. SUMMARY OF CONTENTS

The tutorial starts out with an overview of a realistic safety-critical system that will be used as an ongoing example, specifically an automated people mover to be used by patrons of a very large zoo. The tutorial provides sufficient information about the example to enable the attendees to practice engineering the system's different kinds of safety-related requirements

The second section of the tutorial provides an overview of requirements engineering for safety engineers so that they will understand the characteristics of good safety-related requirements and where they should be documented.

The third section of the tutorial provides an overview of safety engineering for requirements engineers. This includes the basic safety concepts such as valuable assets that can be accidentally harmed; safety incidents such as accidents and near misses (close calls); hazards; safety risks based on harm severities and likelihood of hazards/accidents; safety integrity levels (SILs) of requirements and safety assurance evidence levels (SEALs) of architectural components; safety goals, policies, and requirements; safety vulnerabilities; and safety mechanisms / safeguards.

The fourth section of the tutorial identifies, defines, and discusses the four major kinds of safety-related requirements: (1) safety requirements (a form of quality requirement), (2) safety-significant requirements (including safety-critical functional, data, interface, and non-safety quality requirements), (3) safety subsystem requirements, and (4) safety constraints. Techniques for engineering

ICSE'06, May 20-28, 2006, Shanghai, China.
ACM 1-59593-085-X/06/0005.

these different kinds of requirements as well as examples of these requirements will be provided.

The fifth and final section of the tutorial covers a subset of safety engineering and provides a generic process for producing safety-related requirements. After providing an overview, it covers safety program planning during which safety goals are included in ConOps documents or vision statements. Next covered is safety analysis consisting of asset analysis, safety incident analysis, hazard analysis, safety risk analysis, safety significance analysis, and safety control analysis during which the four kinds of safety-related requirements are identified, analyzed, and specified. The last topics covered are the requirements-related aspects of the remaining safety tasks including safety monitoring, safety incidence investigation, safety compliance assessment, and safety

4. STRUCTURE OF CONTENTS

4.1 Common Example

This section provides an overview of a realistic safety critical system that will be used as an ongoing example. The example is an automated people mover to be used by patrons of a very large zoo. This section describes the motivation for the system. It also covers the relevant main concepts the attendees need to understand in order to practice engineering the system's different kinds of safety-related requirements.

4.2 Requirements Engineering Concepts

This section provides an overview of requirements engineering for safety engineers. It addresses the:

- Importance of requirements engineering to project success.
- Definition of the basic concepts of requirements engineering.
- Major tasks comprising requirements engineering
- Major work products produced by requirements engineering
- Critical characteristics of good requirements so that safety engineers will know the necessary characteristics of good safety-related requirements.
- Different kinds of requirements such as functional, data, interface, and quality requirements as well as constraints.

4.3 Safety-Engineering Concepts

This section provides an overview of safety engineering for requirements engineers. It addresses the following basic safety concepts:

- Safety as a Quality Factor of a Quality Model
- Safety Quality Subfactors
- Valuable Assets
- Accidental Harm to Valuable Assets
- Safety Incidents (Accidents & Near Misses)
- Hazards
- Safety Risks
- Safety Goals, Policies, and Requirements
- Safeguards (Safety Mechanisms)
- Vulnerabilities (system-internal sources of hazards)

4.4 Safety-Related Requirements

This section describes the following four main types of safety-related requirements including examples of such requirements:

- Safety Requirements, which are a type of quality requirement
- Safety-Significant Requirements (including safety-critical functional, data, interface, and non-safety quality requirements)
- Safety Subsystem Requirements
- Safety Constraints

4.5 Safety-Engineering Process

This subsection describes a safety-engineering process with emphasis on the engineering of safety-related requirements. It addresses:

- Safety Program Planning
- Safety Analysis including Asset Analysis, Safety Incidence Analysis, Hazard Analysis, Safety Risk Analysis, Safety Significance Analysis, and Safety Control Analysis
- Safety Monitoring
- Safety Incidence Investigation
- Safety Compliance Assessment
- Safety Certification

5. ACKNOWLEDGMENTS

This tutorial has been built based on the following sources:

Donald G. Firesmith, *OPEN Process Framework Repository Organization Website*, 2001-2006, <http://www.opfro.org>.

Donald G. Firesmith, "Engineering Safety Requirements, Safety Constraints, and Safety-Critical Requirements," *Journal of Object Technology (JOT)*, 3(3), Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, pp. 27-42, March/April 2004.

Donald G. Firesmith, *Common Concepts Underlying Safety, Security, and Survivability Engineering*, Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute, Pittsburgh, Pennsylvania, December 2003.

Donald G. Firesmith, "Using Quality Models to Engineer Quality Requirements," *Journal of Object Technology (JOT)*, 2(5), Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, pp. 67-75, September/October 2003.

Donald G. Firesmith, "A Taxonomy of Safety-Related Requirements," *Requirements Engineering'2004 Requirements for High Assurance Systems (RHAS) Workshop*, in Kyoto, Japan, IEEE Computer Society, Washington, D.C., 6 September 2003.

Donald G. Firesmith, "Specifying Good Requirements," *Journal of Object Technology (JOT)*, 2(4), Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, pp. 77-87, July/August 2003