Engineering
Safety- and Security-Related Requirements for Software-Intensive Systems

Presented at SSTC 2010

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Donald Firesmith, Terry Roberts & Stephen Blanchette, Jr.

27 April 2010
### Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 APR 2010</td>
<td></td>
<td>00-00-2010 to 00-00-2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Safety- and Security-Related Requirements for Software-Intensive Systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5a. CONTRACT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5b. GRANT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5c. PROGRAM ELEMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5d. PROJECT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5e. TASK NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. DISTRIBUTION/AVAILABILITY STATEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release; distribution unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT unclassified</td>
</tr>
<tr>
<td>b. ABSTRACT unclassified</td>
</tr>
<tr>
<td>c. THIS PAGE unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. LIMITATION OF ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same as Report (SAR)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18. NUMBER OF PAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Form Approved
OMB No. 0704-0188

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.
Contents

Three Disciplines
Challenges
Fundamental Concepts
Safety- and Security-Related Requirements
Collaboratively Engineering Safety- & Security-Related Requirements
Conclusion
Three Disciplines: Requirements, Safety, and Security Engineering
Three Related Disciplines

Safety Engineering

the engineering discipline within systems engineering concerned with lowering the risk of *unintentional unauthorized* harm to valuable assets to a level that is acceptable to the system’s stakeholders by preventing, detecting, and reacting to such harm, mishaps (i.e., accidents and incidents), hazards, vulnerabilities, and safety risks

Security Engineering

the engineering discipline within systems engineering concerned with lowering the risk of *intentional unauthorized* harm to valuable assets to a level that is acceptable to the system’s stakeholders by preventing, detecting, and reacting to such harm, misuses (i.e., attacks and incidents), threats, vulnerabilities, and security risks

Requirements Engineering

the engineering discipline within systems/software engineering concerned with identifying, analyzing, reusing, specifying, managing, verifying, and validating goals and requirements (including safety- and security-related requirements)
Challenges:
Combining Requirements, Safety, and Security Engineering
Challenges

Requirements engineering, safety engineering, and security engineering have different:

• Communities
• Disciplines with different training, books, journals, and conferences
• Professions with different job titles
• Fundamental underlying concepts and terminologies
• Tasks, techniques, and tools

Safety and security engineering are:

• Typically treated as secondary specialty engineering disciplines
• Performed separately from, largely independently of, and lagging behind the primary engineering workflow: (requirements, architecture, design, etc.)
Challenges

Current separate methods for performing requirements, safety, and security engineering are inefficient and ineffective.

Separation of requirements engineering, safety engineering, and security engineering:

- Causes poor safety- and security-related requirements that are often:
  - Vague/unverifiable/unfeasible architectural and design constraints
  - Capabilities or goals rather than requirements
  - Inadequate and too late to drive architecture development and test planning
- Makes it unnecessarily difficult to achieve certification and accreditation for safe/secure operations
Challenges

Poor requirements are a primary cause of more than half of all project failures (defined in terms of):

- Major Cost Overruns
- Major Schedule Overruns
- Major Functionality not delivered
- Cancelled Projects
- Delivered Systems that are never used

Poor requirements are a major root cause of many (or most) accidents involving software-intensive systems.

Security ‘requirements’ often mandated (e.g., Industry Best Practices, Security Functions)

- Often, these are not derived into meaningful requirements at the engineering level
Challenges

Constant tension: How safe and secure is safe and secure enough?

What is needed:

- Better consistency between safety and security engineering
  - More consistent concepts and terminology
  - Reuse of techniques across disciplines
  - Less unnecessary overlap and avoidance of redundant work
- Better collaboration:
  - Between safety and security engineering
  - With requirements engineering
- Better safety- and security-related requirements
Fundamental Concepts: 
A Foundation for Understanding
Quality Model

Architectural Components

System

defines the meaning of the quality of a

Quality Model

Quality Characteristics

Quality Attributes

are measured along

Quality Measurement Scales

Quality Measurement Methods

are measured using

Internal Quality Characteristics

External Quality Characteristics

12

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Quality Characteristics (External)
Defensibility

Defensibility

the quality characteristic capturing the degree to which the system:

- Properly prevents, detects, reacts to, and adapts to:
  - Unintended and unauthorized harm to valuable assets due to the occurrence of
  - Abuses enabled by the existence of
  - Dangers

- Has defensibility risks that are acceptably low to its stakeholders

- Valuable Assets may be people, organizations, property, services, or environments

- Harm may be direct or indirect, intentional or unintentional, authorized or unauthorized
Defensibility$_2$

Safety and security aspects of defensibility are defined in a similar manner by replacing:

- Abuse with either mishap (safety) or misuse (security)
- Danger with either hazard (safety) or threat (security)
- Defensibility risks with safety risks and security risks
Safety- and Security-Related Requirements
There’s More Than One Type

Too often, only a single type of requirements is considered when there are many types that need consideration:

- Special non-functional requirements:
  - Safety and security requirements are quality requirements
- Safety- and security-significant requirements (functional, data, and interface)
- Safety and security functions/subsystems requirements
- Safety and security constraints:
  - Architectural and design constraints
  - Mandated defensibility controls (i.e., safeguards and countermeasures)

Separation of safety/security/requirements engineering almost assures gaps in requirements

Gaps in Requirements Lead to Shortcomings in Delivered Systems
Four Types of Defensibility-Related Requirements

- Safety Requirements
- Security Requirements
- Functional Requirements
- Quality Requirements
- Data Requirements
- Interface Requirements

Defensibility Function / Subsystem Requirements

Intolerable Risk Requirements SAL = 4
High Risk Requirements SAL = 3
Moderate Risk Requirements SAL = 2
Low Risk Requirements SAL = 1

Safety/Security Assurance Level (SAL)

Defensibility-Independent Requirements SAL = 0
Defensibility-Significant Requirements SAL = 1 - 4

System Requirements

Primary Mission Requirements
Supporting Requirements

Safety Function / Subsystem Requirements
Security Function / Subsystem Requirements

Safety Constraints
Security Constraints
Defensibility Constraints

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Example Safety- and Security-Related Requirements

Safety / Security Requirement

“When in mode V, the system shall limit the occurrence of accidental harm of type W to valuable assets of type X to an average rate of no more than Y asset value per Z time duration.”

“When in mode X, the system shall detect misuses of type Y an average of at least Z percent of the time.”

Safety / Security Significant Requirement

“The system shall automatically transport passengers between stations.”

“The system shall enable users to update their personal information.”

Safety / Security Function / Subsystem Requirement

“The system shall include a fire detection and suppression subsystem.”

“The system shall support the encryption/decryption of sensitive data.”

Safety / Security Constraint

“The system shall not contain any of the hazardous materials in Table X.”

“The system shall use passwords for user authentication.”
Collaboratively Engineering Safety- & Security-Related Requirements
Stovepipes are Typical...

To Requirements Engineering
A Better Way

Ensure close collaboration among Safety, Security, and Requirements Teams

Better Integrate Safety and Security Methods:

- Concepts and Terminology
- Techniques and Work Products
- Provide Cross Training

Better Integrate Safety and Security Methods with Requirements Methods:

- Early during Development Cycle
- Clearly define Team Responsibilities
- Provide Cross Training

Develop all types of Safety- and Security-related Requirements

Ensure that these Requirements have appropriate Properties
An Overall Defensibility Engineering Method

- Defensibility Program Planning
- Defensibility Analysis
- Defensibility Monitoring
- Abuse Investigation
- Compliance Assessment
- Defensibility Policy Development
- Defensibility Certification & Accreditation
Defensibility Analysis ➔ Reqts Engineering

Safety Team collaborates with Security Team

Safety Team performs Defensibility Analysis

Safety and Security Engineering

Stakeholder Analysis

Asset Analysis

Abuse Analysis

Abuser Analysis

Vulnerability Analysis

Danger Analysis

Risk Analysis

Significance Analysis

Defense Analysis

Requirements Team performs

Requirements Identification

Requirements Analysis

Requirements Validation

Requirements Verification

Requirements Engineering

Defensibility-Related Requirements

Stakeholders Subject Matter Experts Safety Team Security Team
Conclusion
Summary

Engineering safety- and security-related requirements requires appropriate Concepts / Methods / Techniques & Tools / Expertise

These must come from the respective experts in:

- Requirements engineering (safety- and security-related requirements)
- Safety engineering (analysis and safety goals)
- Security engineering (analysis and security goals)

BUT, Requirements/Safety/Security Engineering need to be:

- Properly interwoven.
- Consistent with each other.
- Performed collaboratively and in parallel (i.e., overlapping in time).

A collaborative process will advance Safety and Security Engineering to 1st class efforts

Ultimately, collaboration will improve the safety and security aspects of delivered systems
Contact Information

Donald Firesmith
Senior Member of the Tech. Staff Acquisition Support Program
Telephone: +1 412-268-6874
Email: dgf@sei.cmu.edu

U.S. mail:
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

World Wide Web:
www.sei.cmu.edu
www.sei.cmu.edu/contact.html

Customer Relations
Email: customer-relations@sei.cmu.edu
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257
Backup
Defensibility Quality Attributes

- Occurrence of Unauthorized Harm
  - Occurrence of Abuse (Mishap, Misuse, or Incident)
  - Existence of External Abuser
  - Existence of Internal Vulnerability
  - Existence of Danger (Hazard or Threat)
  - Existence of Defensibility Risk

- Problem Type Defensibility Attribute

- Solution Type Defensibility Attribute
  - Problem Prevention
  - Problem Detection
  - Problem Reaction
  - Problem Adaptation
  - Harm Arrest
  - Mitigation
  - Recovery
  - Analysis
  - Counterattack (Security)

- Robustness
- Safety
- Occupational Health
- Security
- Survivability

- Defensibility

- Quality Characteristic

- Quality Attribute

- Quality Measurement Scale

- Quality Measurement Method

- Quality Model

- System
Unauthorized Harm to Valuable Assets

Stakeholders

value

have an interest in the

System

must defend

Unauthorized Harm

may occur to

Valuable Assets

People

Organizations

Property

Environment

Services

Human Beings

Roles Played

Development

Owner

Supplier

User

Tangible Property

Intangible Property

Private Property

Public Property

Commercial Property

© 2010 Carnegie Mellon University
Types of Harm

- **Safety**
- **Security**
- **Survivability**

**Unintentional (Accidental) Harm**

- **Attacker-Caused (Malicious) Harm**

**Authorized Harm**

**Unauthorized Harm**

Valuable Assets may occur to Harm

- **Direct Harm**
- **Indirect Harm**

**Harm to People**
- Death
- Injury
- Illness
- Kidnap
- Corruption (bribery or extortion)
- Hardship

**Harm to Organizations**
- Bankruptcy
- Lost Market Share
- Loss of Profits
- Loss of Reputation

**Harm to Property**
- Destruction
- Damage
- Corrupt
- Theft
- Unauthorized Access
- Unauthorized Disclosure

**Harm to the Environment**
- Destruction
- Damage
- Loss of Use

**Harm to a Service**
- Corruption
- Unauthorized Usage (Theft)
- Accidental Loss of Service
- Denial of Service (DOS)
- Repudiation of Transaction

- © 2010 Carnegie Mellon University
Types of Abuses

- **Mishaps (Safety)**
  - Accidents
  - Safety Incidents
  - Unintended Harm

- **Misuses (Security)**
  - Successful Civilian Attacks
  - Security Incidents
  - Unauthorized Attacks

- **Survivability Abuses**
  - Military Attacks
  - Survivability Incidents

- **Defensibility Events**
  - Probes
Types of Abusers

- System Maintainer
- User

- System Developer
- System Operator

- Non-malicious Human Abuser
- Non-malicious External System
- Aspect of the Natural Environment

- Non-malicious Abuser (Safety)
- Malicious Abuser (Security)

- Attack
- Malware

- Arsonist
- Disgruntled Employee
- Identity Thief
- Mugger
- Rapist
- Cracker
- Foreign Government
- Industrial Spy
- Professional Criminal
- Terrorist

- Software Malware
- Hardware Malware
- Malware System

- Backdoor
- Spyware
- Trojan
- Worm
- Virus

Abuser

- System-External Condition
- System-Internal Condition
- Vulnerability

- Condition
- Danger
- Hazard (Safety)
- Threat (Security)

Defensibility Event

- Accident (Safety)
- Safety Incident
- Attack (Security)
- Security Incident

Danger is the ultimate cause of a

May include existence of

Malicious Abuser creates and uses

May result in exploits

Hazard (Safety) and Threat (Security)

Vulnerability are partially defined in terms of the existence of system-external

System-External Condition

Software Engineering Institute | Carnegie Mellon

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Vulnerabilities

- **Dangers**
  - are partially defined in terms of the existence of system-internal vulnerabilities

- **Defenses**
  - eliminate or mitigate vulnerabilities

- **Abusers**
  - exploit vulnerabilities
  - typically cause abuses
    - may cause unauthorized harm
      - may occur to valuable assets

- **Nonmalicious Abusers**
  - desire

- **Malicious Abusers**
  - may cause abuses

- **Stakeholders**
  - have interest in the system
  - have stakeholder needs
  - must meet stakeholder needs

- **System**
  - must defend
  - must defend valuable assets

- **Valuable Assets**
  - value

- **Defensibility**
  - define types of 'quality' of the system
  - stakeholder needs
  - system requirements
  - stakeholder needs

- **Quality Factors**
  - engineering safety & security-related requirements
  - firesmith/roberts/blanchette, 27 april 2010
  - © 2010 carnegie mellon university
Dangers

Defensibility Risks is the expected amount of can be estimated using the probability of are partially defined in terms of the existence of system-external

Abusers typically cause

Nonmalicious Abusers may enable the occurrence of system-internal

Malicious Abusers may cause or enable

Vulnerabilities are partially defined in terms of the existence of system-internal

Abuses may enable the occurrence of

Stakeholders exist in the

have an interest in the

have

must meet

must defend

Stakeholder Needs

System may occur to define types of ‘quality’ of the

Unauthorized Harm may cause

Valuable Assets

Stakeholder Needs have value

Defensibility

Quality Factors

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Defensibility Risks

- Defensibility Risk is due to:
  - Harm Likelihood can be estimated in terms of:
  - Harm Severity are estimated in terms of:

- Harm Likelihood is the likelihood of the occurrence of:
  - Hazard Likelihood
  - Threat Likelihood
  - Accident Likelihood
  - Successful Attack Likelihood

- Hazard Likelihood may result in:
  - Abuses may cause:
    - Unauthorized Harm may occur to:
      - Valuable Assets

- Successful Attack Likelihood corresponds to the “expected” amount of:
Risk in terms of Software Degree of Control

Risk is due to Harm may result in Dangers Software Degree of Control can be estimated in terms of Dangers software’s control over occurrence of Abuses may cause Unauthorized Harm categorizes amount of corresponds to the “expected” amount of Valuable Assets is estimated in terms of Harm Severity

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Types of Requirements
Types of Defensibility-Related Requirements

- **Safety**
  - Safety Requirements
  - Safety-Significant Requirements
  - System Requirements

- **Security**
  - Security Requirements
  - Security-Significant Requirements
  - Defensibility Requirements

- **Defensibility**
  - Defensibility-Related Requirements
  - Defensibility Function/Subsystem Requirements

- **Constraints**
  - Safety-Related Requirements
  - Security-Related Requirements
  - Defensibility Constraints
Abuse (Misuse and Mishap) Analysis

Abuse Analysis

Safety and Security Engineering

Requirements Engineering

Abuse Identification
Abuse Tree Analysis
Abuse Case Analysis
Abuse Goal Identification

Abuse Table
Abuse Trees
Abuse Cases
Abuse Goals

Preparation

Requirements Identification
Requirements Analysis
Requirements Validation

Stakeholders
Subject Matter Experts
Safety Team
Security Team

Project Documentation (RFP, Contract, ConOps)
Asset Table
Asset Value and Harm Table
Generic / Reusable Abuse Type Lists
Generic / Reusable Abuse Table
Generic / Reusable Abuse Likelihood Categories
Generic / Reusable Abuse Goals

Defensibility Compliance Repository

Standard / Reusable Abuse Likelihood Categories

Safety Team collaborates with Security Team

Software Engineering Institute | Carnegie Mellon

Engineering Safety- & Security-Related Requirements
Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Abuser Analysis

Safety Team collaborates with Security Team

Abuser Analysis

Preparation
Abuser Identification
Abuser Profiling
Abuser Occurrence Analysis
Abuser Goal Development
Requirements Team Support

Defensibility Compliance Repository

Requirements Identification
Requirements Analysis
Requirements Validation

Potential Abuser List
Abuser Profiles
Abuser Occurrence Table
Abuser-Related Goals

Abuser Protection Requirements
Abuser Detection Requirements
Abuser Reaction Requirements
Safety Abuser Requirements
Security Abuser Requirements

Abuser-Related Requirements

Stakeholders provide input during
Subject Matter Experts provide input during

Stakeholders

Project Documentation (RFP, Contract, ConOps)
Generic / Reusable Abuser Lists
Generic / Reusable Abuser Profiles
Generic / Reusable Abuser-Related Goals

Safety and Security Engineering

Requirements Engineering
Danger Analysis

Subject Matter Experts collaborate with Safety Team and Security Team.

- Requirements Team performs Generic / Reusable Hazard and Threat Requirements Analysis.
- Stakeholders provide input during Danger Profiling.
- Stakeholders provide input during Danger Identification.
- Stakeholders provide input during Danger Profiling.
- Danger Identification performs Danger (Hazard & Threat) Profiles.
- Danger Profiling performs Cause Analysis.
- Danger Cause Analysis performs Root Cause Analysis.
- Danger Effects Analysis performs Common Cause Analysis.
- Danger Likelihood Analysis performs Cause and Effects Diagrams.
- Danger Goal Identification performs Danger Goals.
- Requirements Team Support provides input during Danger Identification.

Danger Analysis

System Safety and Security Documentation, Other System Documentation, Non-System Documentation, Generic / Reusable Danger Lists, Generic / Reusable Danger Profiles, Generic / Reusable Danger Likelihoods, Defensibility Compliance Repository, and Requirements Team Support are used in the process.

Requirements Engineering

Requirements Team performs Defensibility Compliance Repository, Subject Matter Experts, Safety Team, and Security Team.

Danger Goals are validated by Requirements Validation.

Danger Effects Analysis, Danger Likelihood Analysis, Danger Goal Identification, Requirements Team Support, and Defensibility Compliance Repository are inputs to Requirement Identification.

Requirements Analysis performs Requirements Validation.

Requirements Validation performs Requirements Analysis.

Hazard Requirements and Threat Requirements are inputs to Requirement Identification.

Requirements Engineering performs Generic / Reusable Hazard and Threat Requirements Analysis.

Software Engineering Institute | Carnegie Mellon
Defensibility Risk Analysis

Safety Team collaborates with Security Team

Risk Analysis

Requirements Team

Asset Risk Table

Harm Risk Table

Abuse Risk Table

Danger Risk Table

Requirements Identification

Requirements Analysis

Requirements Validation

Risk Goals

Defensibility Risk Goals

Defensibility Compliance Repository

Generic / Reusable Risk Tables

Abuse Table

Abuse Trees

Abuse Cases

Danger Profiles

Danger Cause and Effects Diagrams

Safety and Security Engineering

Stakeholders

Subject Matter Experts

Subject Matter Experts

Stakeholders

Safety Team

Security Team

Requirements Engineering

Standard / Reusable Defensibility Risk Requirements

Safety Risk Requirements

Security Risk Requirements

Risk Requirements

Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University
Defense Analysis

Safety Team collaborates with Security Team performs Defense Analysis.

Safety and Security Engineering

Defense Type Identification

Countermeasure and Safeguard Type Lists

List of Defense Functions / Subsystems

Vendor Trade Studies

Requirements Identification

Requirements Analysis

Requirements Validation

Defense Functionality Identification

Defensibility Compliance Repository

Defense Adequacy Analysis

Countermeasure and Safeguard Selection Reports

Defense Constraints

Generic / Reusable Safeguard and Countermeasure Lists

Stakeholders provide input during Defense Analysis.

Safety and Security Requirements

Generic / Reusable Safeguard and Countermeasure Lists

Standard Defense Functionality and Constraint Requirements

Safety and Security Risks

Architecture Team collaborate in the performance of Architecting.

Stakeholders

Subject Matter Experts

Security Team

Subject Matter Experts

Safety Team

Security Team

Requirements Engineering

Safety and Security-Related Requirements

Firesmith/Roberts/Blanchette, 27 April 2010
© 2010 Carnegie Mellon University