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

**Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213**

**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**

---

**1. REPORT DATE**

**27 APR 2010**

**3. DATES COVERED**

**00-00-2010 to 00-00-2010**

**4. TITLE AND SUBTITLE**

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

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**6. AUTHOR(S)**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR’S ACRONYM(S)**

**11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for public release; distribution unlimited

**13. SUPPLEMENTARY NOTES**

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

**14. ABSTRACT**

**15. SUBJECT TERMS**

**16. SECURITY CLASSIFICATION OF:**

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

**17. LIMITATION OF ABSTRACT**

Same as Report (SAR)

**18. NUMBER OF PAGES**

48

**19a. NAME OF RESPONSIBLE PERSON**

---

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

defines the meaning of a specific type of quality of a

Quality Characteristics

Quality Attributes

determine the measurement scales

Quality Measurement Scales

Quality Measurement Methods

Internal Quality Characteristics

External Quality Characteristics

are measured using

are measured along

are measured along

measure quality along
Quality Characteristics (External)

- Robustness
  - Safety
    - Occupational Health
  - Security
    - Survivability
- Defensibility
- Performance
- Soundness
  - Availability
  - Correctness
  - Predictability
    - Reliability
    - Stability
- Efficiency
- Functionality
- Interoperability
- Serviceability
- Configurability
- Environmental Compatibility
- Habitability
- Operability
- Usability

Quality Characteristic
Internal Quality Characteristic
External Quality Characteristic
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

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 Requirements**
- **Defensibility Constraints**
  - Defensibility-Independent Requirements
  - System Requirements
  - Defensibility Function / Subsystem Requirements
- **Defensibility Function / Subsystem Requirements**

**Safety/Security Assurance Level (SAL):**
- Intolerable Risk Requirements SAL = 4
- High Risk Requirements SAL = 3
- Moderate Risk Requirements SAL = 2
- Low Risk Requirements SAL = 1

**SAL Safety/Security Assurance Levels:**
- Safety/Security Assurance Level (SAL) = 0
- Safety/Security Assurance Level (SAL) = 1
- Safety/Security Assurance Level (SAL) = 2
- Safety/Security Assurance Level (SAL) = 3
- Safety/Security Assurance Level (SAL) = 4
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…

Safety Team performs Safety Analysis

Security Team performs Security Analysis

Safety Engineering

- Stakeholder Analysis
- Asset Analysis
- Abuse Analysis
- Abuser Analysis
- Vulnerability Analysis
- Danger Analysis
- Risk Analysis
- Significance Analysis
- Defense Analysis

Security Engineering

- Stakeholder Analysis
- Asset Analysis
- Abuse Analysis
- Abuser Analysis
- Vulnerability Analysis
- Danger Analysis
- Risk Analysis
- Significance Analysis
- Defense Analysis

To Requirements Engineering

Software Engineering Institute

Carnegie Mellon
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 Policy Development
- Defensibility Monitoring
- Compliance Assessment
- Abuse Investigation
- Defensibility Certification & Accreditation
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

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

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

Customer Relations
Email: customer-relationships@sei.cmu.edu
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257
Backup
Unauthorized Harm to Valuable Assets

Stakeholders

value

have an interest in the

must defend

System

Unauthorized Harm

may occur to

Valuable Assets

People

Organizations

Property

Environment

Services

Roles Played

Human Beings

Development

Owner

Supplier

User

Tangible Property

Intangible Property

Private Property

Public Property

Commercial Property
Types of Harm

- Safety
- Security
- Survivability

- Unintentional (Accidental) Harm
- Attacker-Caused (Malicious) Harm

- Authorized Harm
- Unauthorized Harm

- Valuable Assets may occur to:
  - Direct Harm
  - Indirect Harm

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

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

- Harm to Property:
  - Destruction
    - Damage
    - Corruption
    - 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
Types of Abuses

Abuses

- Defensibility Events
  - Mishaps (Safety)
    - Accidents
    - Safety Incidents
      - Unauthorized Harm
  - Misuses (Security)
    - Successful Civilian Attacks
    - Security Incidents
      - Unsuccessful Attacks
      - Probes
  - Survivability Abuses
    - Military Attacks
    - Survivability Incidents
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)
- Attacker
- Malware
  - Software Malware
  - Hardware Malware
  - Malware System
- Backdoor
- Spyware
- Trojan
- Worm
- Virus

Abuser
- may include existence of
- System-External Condition
- System-Internal Condition
- Vulnerability
- Condition
- Danger
- Hazard (Safety)
- Threat (Security)

Abuse
- are partially defined in terms of the existence of system-external
- may result in
- exploits
- may be the ultimate cause of a
- Defensibility Event

Danger
- System-External Condition

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

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

to exploit

desire

Nonmalicious Abusers

Malicious Abusers

Vulnerabilities

may enable the occurrence of

are partially defined in terms of system-internal

may cause or enable

Abuses

Stakeholders

exist in the

have an interest in the

have

Stakeholder Needs

must meet

must defend

System

may occur to

Unauthorized Harm

define types of ‘quality’ of the

Valuable Assets

have

value

Stakeholder Needs

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

Defensibility Risk is due to risk harm likelihood and severity can be estimated in terms of harm event danger is the likelihood of the occurrence of the conditional likelihood given danger may result in abuses which may cause unauthorized harm which may occur to valuable assets.

Harm Likelihood can be estimated in terms of hazard likelihood threat likelihood accident likelihood and successful attack likelihood.

Harm Severity can be estimated in terms of the expected amount of damage corresponds to the "expected" amount of harm that may occur to valuable assets.
Risk in terms of Software Degree of Control

Risk is due to Harm, which may result in Dangers. Dangers may cause Abuses, which may result in Unauthorized Harm. Unauthorized Harm may occur to Valuable Assets.

Defensibility Risk can be estimated in terms of Software Degree of Control, which is software’s control over occurrence of Harm Severity. Harm Severity is estimated in terms of Harm Severity.

The diagram illustrates the concept that risks are due to harms, which can lead to dangers. Dangers may result in abuses, which may cause unauthorized harm. Unauthorized harm may occur to valuable assets, and the overall risk can be estimated in terms of software’s degree of control over the occurrence of harm severity.
Types of Requirements

- Contractual (Stakeholder) Requirements
- Derived (Developer) Requirements
- Operational Requirements
- Maintenance Requirements
- Sustainment Requirements
- Training Requirements
- Retirement Requirements
- Positive (shall) Requirements
- Negative (shall not) Requirements
- Business Requirements
- Software Requirements
- Hardware Requirements
- People Requirements
- Facility Requirements
- Entity Requirements
- Procedure Requirements
- Documentation Requirements
- System/Subsystem Requirements
- Primary Mission Requirements
- Supporting Requirements
- Functional Requirements
- Non-Functional Requirements
- Quality Requirements
- Data Requirements
- Interface Requirements
- Constraints
- Data Requirements
- Object Requirements
- Material Requirements
- Architecture Constraints
- Design Constraints
- Implementation Constraints
- Integration Constraints
- Configuration Constraints
Types of Defensibility-Related Requirements

- Safety Requirements
  - Safety-Significant Requirements
  - Safety Function/Subsystem Requirements
  - Safety Constraints
- Security Requirements
  - Security-Significant Requirements
  - Security Function/Subsystem Requirements
  - Security Constraints
- Defensibility Requirements
  - Defensibility-Significant Requirements
  - Defensibility Function/Subsystem Requirements
  - Defensibility Constraints
- System Requirements
- Defensibility-Related Requirements
- Safety-Related Requirements
- Security-Related Requirements
Systems Analysis

Safety Team

 collaborates with

Security Team

performs

System Analysis

---

Safety and Security Engineering

Requirements Engineering

- Vision Statement
- Context Diagram
- Goals
- ConOps
- Scenarios
- Use Cases
- Requirements Models
- Requirements Specifications
- Requirements
- Architecture
- Model
- Architecture Documentation

- Understand Requirements
- Understand Architecture

- Requirements Team

- Architecture Team
Vulnerability Analysis

Safety and Security Engineering

Preparation
- Vulnerability Identification
- System Vulnerability Analysis
- Operational Vulnerability Analysis
- Vulnerability Goal Identification
- Requirements Table
- Vulnerability Goals
- Requirements Validation
- Requirements Analysis
- Requirements Identification

Vulnerability Requirements
- Safety Vulnerability Requirements
- Security Vulnerability Requirements
- Vulnerability Constraints
- Safety Vulnerability Constraints
- Security Vulnerability Constraints

Requirements Engineering

Requirements Team
- performs

Safety Team
- collaborates with Security Team

Security Team

Requirements Team Support
- Architects, Designers, and Implementers
- Quality Engineers, Testers, and Maintainers
- Safety Team
- Safety Team

Vulnerability Analysis
- Actual / Proposed System Architecture
- Actual / Proposed System Design
- Actual / Proposed System Implementation
- Asset Value and Harm Table
- Defensibility Compliance Repository
- Failure Mode Effect Criticality Analysis (FMECA) Table

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

Subject Matter Experts

Safety Team collaborates with Security Team

perform Abuser Analysis

Preparation

Abuser Identification

Abuser Profiling

Abuser Occurrence Analysis

Abuser Goal Development

Requirements Team Support

Potential Abuser List

Abuser Profiles

Abuser Occurrence Table

Abuser-Related Goals

Defensibility Compliance Repository

Safety and Security Engineering

Safety Protection Requirements

Abuser Detection Requirements

Abuser Reaction Requirements

Abuser-Related Requirements

Safety Abuser Requirements

Security Abuser Requirements

Requirements Engineering

Project Documentation (RFP, Contract, ConOps)

Generic / Reusable Abuser Lists

Generic / Reusable Abuser Profiles

Generic / Reusable Abuser-Related Goals

Stakeholders

provide input during

Software Engineering Institute | Carnegie Mellon

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

Safety and Security Engineering

Requirements Team

Generic / Reusable Hazard and Threat Requirements

Danger Goals

Requirements Validation

Danger Profiling

Danger Likelihood Analysis

Danger Goal Identification

Requirements Team Support

Defensibility Compliance Repository

Other System Documentation

Non-System Documentation

Danger Analysis

Danger Identification

Cause Analysis

Root Cause Analysis

Common Cause Analysis

Danger Effects Analysis

Danger Cause Analysis

Requirements Team

Stakeholders

Subject Matter Experts

Safety Team

Security Team

System Safety and Security Documentation

Generic / Reusable Danger Lists

Generic / Reusable Danger Profiles

Generic / Reusable Danger Likelihoods

Danger Analysis

Preparation

Danger Identification

Danger Profiling

Cause and Effects Diagrams

Danger (Hazard & Threat) Profiles

Non-System Documentation

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

- Safety Team collaborates with Security Team
- Stakeholders provide input during risk analysis
- Requirements Team performs risk analysis
- Generic / Reusable Risk Tables
- Abuse Table
- Abuse Trees
- Abuse Cases
- Danger Profiles
- Danger Cause and Effects Diagrams
- Requirement Team Support

Requirements Engineering
- Asset Risk Table
- Harm Risk Table
- Abuse Risk Table
- Danger Risk Table
- Requirements Identification
- Requirements Analysis
- Requirements Validation
- Standard / Reusable Defensibility Risk Requirements

Safety and Security Engineering
- Stakeholders
- Subject Matter Experts
- Safety Team
- Security Team

Subject Matter Experts

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

Safety and Security Goals

Project-Specific Safety and Security Assurance Level (SAL) Definitions

Project-Specific Safety and Security Evidence Assurance Level (SEAL) Definitions

Safety and Security Engineering

Architecture Engineering

Requirements Engineering

Requirements Identification

Requirements Analysis

Architecture Verification

Architecture Team

Stakeholders

Subject Matter Experts

Safety Team

Security Team

Requirements Team

Subject Matter Experts

Stakeholders

Defensibility Significance Analysis

Safety Team

Security Team

collaborates with

performs

provides input during

Defensibility Compliance Repository

SAL Categorization

SEAL Definition

SEAL Allocation

Architecture Representations

produces

collaborate in the performance of

Architecture Team

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

Safety and Security Engineering

- Defense Type Identification
- Defense Functionality Identification
- Market Research
- Defense Selection
- Countermeasure and Safeguard Selection Reports
- Countermeasure and Safeguard Type Lists
- List of Defense Functions / Subsystems
- Vendor Trade Studies
- Requirements Identification
- Requirements Analysis
- Requirements Validation
- Defense Constraints
- Safety Constraints
- Security Constraints

Requirements Team

- Countermeasure and Safeguard Type Lists
- List of Defense Functions / Subsystems
- Vendor Trade Studies
- Requirements Identification
- Requirements Analysis
- Requirements Validation
- Defense Constraints
- Safety Constraints
- Security Constraints

Safety and Security Requirements
- Safety and Security Risks
- Generic / Reusable Safeguard and Countermeasure Lists
- Standard Defense Functionality and Constraint Requirements

Stakeholders

- provide input during

Safety Team

- collaborates with

Security Team

- performs

Defense Analysis

Defensibility Compliance Repository

- collaborate in the performance of Architechting

Subject Matter Experts

- provide input during

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