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

ICCBSS’2007 Conference Tutorial

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Donald Firesmith
27 February 2007
Tutorial Goals

Familiarize Members of:

- **Safety** and Security Teams with:
  - Foundations of *Requirements Engineering*
  - *Common Concepts and Techniques from Both Disciplines*
- **Requirements** Teams with the Foundations of:
  - **Safety Engineering**
  - **Security Engineering**

Familiarize Members of all three Disciplines with:

- Different Types of **Safety- and Security-related Requirements**
- Common *Process* for Engineering these Requirements
Contents

Challenges
Common Example
Requirements Engineering Overview
Safety and Security Engineering Overview
Types of Safety- and Security-related Requirements
Common Consistent Collaborative Process
Conclusion
Challenges:
Combining Requirements, Safety, and Security Engineering
Challenges

Requirements Engineering, Safety Engineering, and Security Engineering:

• Different Communities
• Different Disciplines with different Training, Books, Journals, and Conferences
• Different Professions with different Job Titles
• Different fundamental underlying Concepts and Terminologies
• Different Tasks, Techniques, and Tools

Safety and Security Engineering are:

• Typically treated as Specialty Engineering Disciplines
• Performed separately and largely independently of the primary Engineering Workflow (Requirements, Architecture, Design, Implementation, Integration, Testing.)
Challenges

Current separate Processes for Requirements, Safety, and Security are Inefficient and Ineffective.

Separation of Requirements Engineering, Safety Engineering, and Security Engineering:

- Causes poor Safety- and Security-related Requirements.
  - Goals rather than Requirements
  - Vague, unverifiable, unfeasible, architectural and design constraints
- Inadequate and too late to drive architecture and testing
- Difficult to achieve Certification and Accreditation
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:

- Industry Best Practices
- Security Functions
Challenges

How Safe and Secure is Safe and Secure *enough*?

Situation Cries out for Process Improvement:

- Better Consistency between Safety and Security Engineering
  - More consistent Concepts and Terminology
  - Reuse of Techniques
  - Less Unnecessary Overlap and Avoidance of Redundant Work
- Better Collaboration:
  - Between Safety and Security Engineering
  - With Requirements Engineering
- Better Safety- and Security-related Requirements
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, 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, 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)
Common Example:
An Automated People Mover System
Desired Characteristics

Common Ongoing Example throughout the Tutorial

Should Not Need Special Domain Knowledge

Example System should be:

- Safety-Critical
- Realistic
- SW-Intensive

Understandable in terms of:

- Requirements
- Technology
- Hazards
Example Overview

*Very Large* New Zoo

Zoo Automated Taxi System (ZATS)

Example Zoo Habitat Guideway Layout

ZATS Context Diagram

Proposed ZATS:

- Taxis
- Elevated Concrete Guideway
- Taxi Stations
Very Large New Zoo
Zoo Automated Taxi System (ZATS)
Example Habitat Layout
ZATS Context Diagram

- **Zoo Automated Taxi System (ZATS)**
  - **Passengers** rides the
  - **Maintainers** maintain and monitor the
  - **Operators** notifies and alerts the
  - **Managers** views the status and reports of the
  - **Internet** alerts the
  - **Zoo Nurse** view status of the
  - **Emergency Responders** requests emergency services from the
  - **Emergency Medical Technicians** obtains bank card approval to pay for zoo taxi travel cards from the
  - **Fire Fighters** obtains employee and membership information from the
  - **Police**

- **Zoo Information System**

- **Bank Card Processing Gateway**
Proposed Taxi Architecture

Front Door Panel

C Speaker

Display (Information, Location)

M Speaker

Back Door Panel

Front Window (Emergency Exit)

Radios

Computer Subsystem

Place for strollers or wheelchair

Front Bench Seat (Electric Batteries)

Back Bench Seat (Electric Batteries)

PS

HMSW

Steering Mechanism

GlS

Electrical Subsystem

DS DL DLS

Door Motor

GlS

Electric PBS

BS SS

Drive Wheel

PS

HMSW

Steered Wheel
Automated Taxis On Elevated Guideways

- Maintenance and Emergency Walkway
- Back of Taxi
- Best View
- Wheels
- Ground Level
- Habitat with Animals
- Power and Communications Cables
- Guideway
Proposed Taxi Station
Proposed Taxi Station Network Diagram
Example Collision Hazard
Requirements Engineering:
An Overview
Requirements Engineering Topics

Definition of Requirements Engineering

Requirements Engineering:
• Tasks
• Work Products

Importance and Difficulty of Requirements Engineering

Goals vs. Scenarios vs. Requirements

Types of Requirements

Characteristics of Good Requirements
Requirements Engineering

Definition

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)

the cohesive collection of all tasks that are primarily performed to produce the requirements and other related requirements work products for an endeavor

Today, these RE tasks are typically performed in an iterative, incremental, parallel, and time-boxed manner rather than according to the traditional Waterfall development cycle, whereby parallel means with the:

Primary work flow disciplines such as architecting, design, and testing

Specialty engineering disciplines such as safety and security engineering
RE Tasks and Work Products

Business Analysis (i.e., Customer, Competitor, Market, Technology, and User Analysis as well as Stakeholder Identification and Profiling)

Visioning

Requirements Identification (a.k.a., Elicitation)

Requirements Reuse

Requirements Prototyping

Requirements Analysis

Requirements Specification

Requirements Management

Requirements Validation

Scope Management (Management)

Change Control (Configuration Management)

Quality Control (Quality Engineering)
Requirements Engineering Work Products

Business Analyses

Stakeholder Profiles

Vision Statement
  • Goals

Operational Concept Document (OCD)
  • Usage Scenarios

Requirements Repository and published Specifications
  • Requirements

Requirements Prototypes

Domain Model

Glossary
Importance and Difficulty of Requirements Eng.

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
- Hazards and associated Mishaps (Accidents and Safety Incidents)
- Vulnerabilities
Difficult of Requirements Engineering

“The hardest single part of building a software system is deciding precisely what to build. No other part of the conceptual work is as difficult as establishing the detailed technical requirements, including all the interfaces to people, to machines, and to other software systems. No other part of the work so cripples the resulting system if done wrong. No other part is more difficult to rectify later.”

Goals

A goal is an *informally documented perceived need of a legitimate stakeholder*.

- Goals are typically documented in a vision statement.
- Goals drive the analysis and formal specification of the requirements.
- Examples:
  - The system shall support user activity X.
  - The system shall be efficient.
  - The system shall be easy to use.
  - The system shall be safe to use.
- Goals are typically not verifiable.
- Goals may not be feasible.
Example ZATS Goals

Functional Goals:

• ZATS must rapidly transport patrons between the parking lots and the zoo.
• ZATS must rapidly transport patrons between habitats within the zoo.
• ZATS must allow patrons to take leisurely tours of the habitats.

Data Goal:

• ZATS must record and report appropriate system usage statistics.

Capacity Goal:

• ZATS must include sufficient taxis so that patrons need not wait long for a free taxi.

Usability Goal:

• ZATS must be very easy and intuitive for patrons to use, including those who are not very good with technology.
Usage Scenarios

A usage scenario is a specific functionally cohesive sequence of interactions between user(s), the system, and potentially other actors that provides value to a stakeholder.

Usage scenarios:

- Are instances of use cases.
- Can be either “sunny day” or “rainy day” scenarios.
- Have preconditions, triggers, and postconditions.
- Are typically documented in an Operational Concept Document (OCD).
- Drive the analysis and formal specification of the [primarily functional] requirements.
- Often include potential design information.
- Can be written in either list or paragraph form.
Example ZATS Scenario

Ride Zoo Loop Line To Restaurants for Lunch:

After the family enters a waiting taxi, Mr. Smith looks at the zoo map on its ceiling. A light representing their taxi is glowing at the Tropical Rainforest Habitat outer taxi station. He uses the control panel to select the inner taxi station at the habitat, which is the central taxi station near the restaurants and shops as a destination. He then swipes his zoo taxi debit card, and the display shows the remaining balance of $9.00 on the card. The taxi warns them to set down and thirty seconds later, the station and taxi exit doors close. Their taxi accelerates out of the taxi station and turns to the left onto the Zoo Loop Line.

Shortly after leaving the taxi station, they see a spur the angles off to their left towards a large building containing the taxi control center and maintenance facility. They continue around the outside of the zoo, passing other the Great Cats, the Wolves and Other Dogs, and the Bears habitats. Just before they reach the outer African Savanna taxi station, the guideway makes a sweeping turn to the right and they can see the parking lot on their left. Everyone looks to see if they can see the family van, but the parking lot is too big and they can only see the parking lot taxi station near where it is parked.

Soon, they pass the zoo entrance on their left and turn right to follow the main street to where the main restaurants and shops are. Their taxi passes the inner African Savanna taxi station on their right, circles around the central area, and soon pulls off the Zoo Loop Line to enter the inner Great Apes and Monkeys taxi station. Exiting the taxi when the doors open, they head down the elevator and outside for an early lunch at one of the many restaurants.
Requirements

A (product) requirement is a mandatory characteristic (behavior or attribute) of a product (e.g., system, subsystem, software application, or component).

- Requirements are documented in requirements specifications.
- Requirements are driven by goals.
- Example: “At each taxi station while under normal operating conditions, ZATS shall provide a taxi to passengers within an average of 5 minutes of the passengers’ request.”
- Requirements must have certain characteristics (e.g., verifiable and feasible).
Types of Requirements

- Process Requirements
- Product Requirements
  - Functional Requirements
  - Non-Functional Requirements
    - Data Requirements
    - Interface Requirements
    - Quality Requirements
    - Constraints
  - Stakeholder (Business) Requirements
  - Software Requirements
  - System/Subsystem Requirements
  - Main Mission Requirements
  - Specialty Engineering Subsystem Requirements
  - Hardware Requirements
Types of Requirements

- Product Requirements
  - Functional Requirements
  - Non-Functional Requirements
  - Constraints
    - Data Requirements
    - Interface Requirements
    - Quality Requirements
    - Defensibility Requirements
      - Safety Requirements
      - Security Requirements
      - Survivability Requirements
- Development Method Requirements
- Stakeholder (Business) Requirements
- Derived Requirements
- Primary Mission Requirements
- Supporting Requirements
- System/Subsystem Requirements
- Software Requirements
- Hardware Requirements
- Manual Procedure Requirements
- Safety Function/Subsystem Requirements
- Security Function/Subsystem Requirements
- Defensibility Constraints
- Safety Constraints
- Security Constraints
- Survivability Constraints

Software Engineering Institute
Carnegie Mellon
Characteristics of Good Requirements

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Consistent</td>
</tr>
<tr>
<td>Cohesive</td>
<td>Usable by Stakeholders</td>
</tr>
<tr>
<td>Feasible</td>
<td>Uniquely Identified</td>
</tr>
<tr>
<td>Relevant</td>
<td>Traced</td>
</tr>
<tr>
<td>Unique</td>
<td>Externally Observable</td>
</tr>
<tr>
<td>Unambiguous</td>
<td>Stakeholder-Centric</td>
</tr>
<tr>
<td>Validatable</td>
<td>Properly Specified</td>
</tr>
<tr>
<td>Verifiable</td>
<td>Prioritized</td>
</tr>
<tr>
<td>What or How Well, not How</td>
<td>Scheduled</td>
</tr>
<tr>
<td></td>
<td>Managed</td>
</tr>
<tr>
<td></td>
<td>Controlled</td>
</tr>
</tbody>
</table>

http://www.jot.fm/issues/issue_2003_07/column7
Safety and Security Engineering: An Overview
Similar Definitions

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, 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, and security risks
Fundamental Concepts:
A Foundation for Understanding
Fundamental Concepts

Quality Model
Safety and Security as a Quality Factors with associated Quality Subfactors
Systems responsible for Valuable Assets
Stakeholders
Accidental and Malicious Harm to Valuable Assets
Defensibility Occurrences (Accidents, Attacks, and Incidents)
Agents (External and Internal, Malicious and Non-malicious)
Vulnerabilities (system-internal sources of dangers)
Dangers (Hazards and Threats)
Defensibility Risks (Safety and Security)
Goals, Policies, and Requirements
Defenses (Safeguards and Counter Measures)
Quality Model

- Quality Model
  - Quality Factor
    - defines the meaning of quality for the System
  - Quality Subfactor
    - defines a type of the quality of the System
    - is measured using a Quality Measure (Measurement Scale)
  - Quality Measure (Measurement Scale)
    - defines a part of a type of the quality of the System

Quality Model

Quality Factor

Quality Subfactor

Quality Measure (Measurement Scale)
Quality Factors

Quality Model

Quality Factor

Development-Oriented Quality Factor

Usage-Oriented Quality Factor

Quality Subfactor

is measured using a

Quality Measure (Measurement Scale)

Quality Subfactor

Capacity Configurability Dependability Efficiency Interoperability Performance Utility

Quality Subfactor

Defensibility Security Correctness Predictability

Defensibility

Soundness

Safety Survivability Operational Availability Reliability Stability

Correctness

Predictability

Robustness
Safety as a Quality Factor

Safety is the Quality Factor capturing the Degree to which:

- Accidental Harm to Valuable Assets is eliminated or mitigated
- Safety Occurrences and Events (Accidents, Safety Incidents, and Hazardous Events) are eliminated or their negative consequence mitigated
- Hazards (i.e., Hazardous Conditions) are eliminated or mitigated:
  - System Vulnerabilities
  - Non-malicious Agents (humans, systems, and the environment)
- Safety Risks are kept acceptably low
- The preceding Problems are Prevented, Detected, Reacted to, and possibly Adapted to
Security as a Quality Factor

Security is the Quality Factor capturing the Degree to which:

- *Malicious Harm* to Valuable Assets is eliminated or mitigated
- *Security Occurrences and Events (Attacks, Security Incidents, and Threatening Events)* are eliminated or their negative consequence mitigated
- *Threats* (i.e., Threatening Conditions) are eliminated or mitigated:
  - System Vulnerabilities
  - Malicious Agents (humans, systems, and malware)
- *Security Risks* are kept acceptably low
- The preceding Problems are *Prevented, Detected, Reacted to*, and possibly *Adapted to*
Defensibility Quality Subfactors

- Occurrence of Unauthorized Harm
- Occurrence of Defensibility Event
- Existence of External Agent
- Existence of Internal Vulnerability
- Existence of Danger
- Existence of Defensibility Risk

Defensibility Problem Type
- Safety
- Security

Defensibility Subfactor
- Quality Factor

Defensibility Solution Type
- Prevention
- Detection
- Reaction
- Adaptation

Quality Subfactor
- is measured using a

Quality Measure (Measurement Scale)

Quality Model
Valuable Assets

Stakeholders

have an interest in the

value

System

must defend

Unauthenticated Harm

may occur to

Valuable Assets

People

Property

Environment

Services

Human Beings

Roles Played

Organizations

Tangible Property

Intangible Property

Private Property

Public Property

Commercial Property
Some ZATS Valuable Assets

People:
- Passengers
- Operators
- Maintainers

Property:
- Animals
- Passenger Bank Card Information
- Taxis
- Taxi Stations

Environment:
- Habitat

Services:
- Taxi Service
Types of Harm

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

- **Authorized Harm**
- **Unauthorized Harm**

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

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

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

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

- **Harm to a Service**

**Valuable Assets** may occur to Harm
Stakeholders

Person → Person Role → Organization → Organization Role

Stakeholder

- has legitimate interest in the values
- is responsible for an Asset

System
Some ZATS Stakeholders

People:

• Emergency Responders
• Passengers
• Operators
• Maintainers
• ZATS Developers
• Zoo Employees
• Zoo Management

Organizations:

• Bank Card Processing Gateway
• Safety and Security Certification/Accreditation Bodies
• Zoo Regulatory Bodies
Accidents and Attacks

Agents typically cause Vulnerabilities which may cause Dangers that may enable the occurrence of Defensibility Risks which can be estimated using the probability of Defensibility Occurrences.

Stakeholders have an interest in the value of Stakeholder Needs which must be defended. The System must meet the Stakeholder Needs to ensure the value of Valuable Assets.

Unauthorized Harm may occur to Valuable Assets, defining types of 'quality' of the System.
Types of Defense Occurrences

- Defensibility Occurrences
  - Mishaps
    - Accidents
    - Safety Incidents
      - Successful Attacks
      - Unsuccessful Attacks
    - Probes
  - Misuses
    - Civilian Attacks
    - Security Incidents
  - Survivability Incidents
    - Military Attacks
    - Survivability Incidents

- Defensibility Events
- Cause
- Unauthorized Harm
Example ZATS Defensibility Occurrences

Accidents:

• Natural Disasters
• Taxi Accidents
• Taxi Station Accidents

Safety Incidents:

• Inadequate Headway
• Overspeed

Attacks:

• Arson
• Cyber-attacks

Security Incidents:

• Antivirus Software Works
Agents

System Maintainer  User
System Developer  System Operator

Non-malicious Human Agent  Non-malicious External System  Aspect of the Natural Environment  Attacker  Malware

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

Agent

may include existence of

System-External Condition  System-Internal Condition

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

Condition  Danger

Vulnerability  Hazard (Safety)  Threat (Security)

Defensibility Occurrence

Defensibility Event

may result in

exploits

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

Backdoor  Spyware  Trojan  Worm  Virus

Cracker  Professional Criminal  Foreign Government

Malicious Agent  Disgruntled Employee  Industrial Spy  Terrorist

Malware  Hardware Malware  Malware System

Non-malicious Human Agent  Non-malicious External System  Aspect of the Natural Environment  Attacker  Malware

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

Agent

may include existence of

System-External Condition  System-Internal Condition

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

Condition  Danger

Vulnerability  Hazard (Safety)  Threat (Security)

Defensibility Occurrence

Defensibility Event

may result in

exploits

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

Backdoor  Spyware  Trojan  Worm  Virus

Cracker  Professional Criminal  Foreign Government

Malicious Agent  Disgruntled Employee  Industrial Spy  Terrorist

Malware  Hardware Malware  Malware System

Non-malicious Human Agent  Non-malicious External System  Aspect of the Natural Environment  Attacker  Malware

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

Agent

may include existence of

System-External Condition  System-Internal Condition

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

Condition  Danger

Vulnerability  Hazard (Safety)  Threat (Security)

Defensibility Occurrence

Defensibility Event

may result in

exploits

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

Backdoor  Spyware  Trojan  Worm  Virus

Cracker  Professional Criminal  Foreign Government

Malicious Agent  Disgruntled Employee  Industrial Spy  Terrorist

Malware  Hardware Malware  Malware System
Example ZATS Agents

Non-Malicious Agents:

- Human Agents (e.g., Developer, Maintainer, Operator, Passenger)
- External Systems (e.g., Communications Network, Electrical Power Grid)
- Natural Environment (e.g., River or Weather)

Malicious Agents:

- Attackers (e.g., Arsonists, Crackers, Terrorists, Thieves)
- Malware (e.g., virus, Trojan horse, Worm)
Vulnerabilities

- Defenses
  - eliminate or mitigate
  - are partially defined in terms of the existence of system-internal

- Stakeholders
  - have
  - have an interest in the
  - must meet
  - must defend
  - Stakeholder Needs
    - value

- Valuable Assets
  - System
    - Defensibility
      - Defensibility Occurrences
        - may cause
          - Unauthorized Harm
            - define types of ‘quality’ of the

- Agents
  - typically cause
    - exploit
      - Nonmalicious Agents
      - Malicious Agents
        - desire

- Dangers
  - may cause
    - Stakeholder Needs
      - have
        - an interest in the
    - System
      - must defend
        - may occur to
Mishaps and Misuses vs. Hazards and Threats

- **Mishaps**
  - Nonmalicious Agents
    - Mishaps
      - Accidents
        - Harm Events
          - Safety Incidents
            - Conditions
              - Dangers
                - Hazards

- **Misuses**
  - Malicious Agents
    - Misuses
      - Security Incidents
        - Threatening Events
          - Attack Triggers
            - Harm Events
              - Security Events

- **Harms and Hazards**
  - Unauthorized Harm
    - Valuable Assets
      - may occur to
        - Dangers
          - Hazards
            - may cause the occurrence of
              - Security Events
                - Exploit Vulnerabilities

- **Events**
  - Events
    - Defensibility Events
      - Causes
        - Security Incidents
          - Threatening Events
            - Security Events
              - Expose Vulnerabilities
Defensibility Risks

- Defensibility Risks are due to
- Harm Likelihood can be estimated in terms of
- Software Control
- Harm Severity

Danger Likelihood
- Is the likelihood of the occurrence of
- Dangers

Harm Event Conditional Likelihood
- Can be estimated in terms of
- Hazard Likelihood
- Threat Likelihood
- Accident Likelihood
- Successful Attack Likelihood

May result in

Networks of Dangerous Events
- May cause

Unauthorized Harm
- May occur to

Valuable Assets

Categorizes amount of
Types of Risks

- Safety Risks
- Security Risks
- Survivability Risks

Defensibility Risks

Risks

Risks of Unauthorized Harm
- Expected Amount of Specific, Specific Types of, or All Unauthorized Harm (Regardless of Asset, Accident, Attack, Hazard, or Threat)

Risks to Valuable Assets
- Expected Amount of Specific, Specific Types of, or All Unauthorized Harm to Specific or Specific Types of Valuable Assets

Risks due to Accidents or Attacks
- Expected Amount of Specific, Specific Types of, or All Unauthorized Harm due to Specific or Specific Types of Accidents or Attacks

Risks due to Hazards or Threats
- Expected Amount of Specific, Specific Types of, or All Unauthorized Harm due to Specific or Specific Types of Hazards or Threats
Safety and Security Goals and Policies

- Quality Requirements
- Defensibility Requirements
- Stakeholders
  - have an interest in the System
  - must meet Stakeholder Needs
  - value
- Valuable Assets
- Stakeholder Needs
  - have interests in the System
  - must meet
- System
- Vulnerabilities
  - may cause Defensibility Occurrences
- Dangers
  - may enable the occurrence of Defensibility Occurrences
- Agents
  - typically cause
  - Non-malicious Agents
  - Malicious Agents
  - exploit
- Unauthorized Harm
  - define types of 'quality' of the System
- Defensibility Goals
  - are partially defined in terms of system-external state
  - are partially defined in terms of system-internal state
- Quality Factors
  - state desired end results regarding state rules to achieve
- Defensibility Policies
  - mandate minimum amounts of Defensibility Requirements
- Survivability
  - Safety Security
- Quality Requirements
  - mandate minimum amounts of Defensibility Requirements
Types of Defensibility Goals

- Safety Goals
- Security Goals
- Survivability Goals

- Goals involving Harm to Valuable Assets
- Goals involving Accidents, Attacks, and Incidents
- Goals involving Agents
- Goals involving Vulnerabilities
- Goals involving Dangers (Hazards and Threats)
- Goals involving Safety and Security Risks

- Stakeholder Goals
- Quality Goals
- Defensibility Goals

- Prevention Goals
- Detection Goals
- Reaction Goals
- Adaptation Goals
Safety- and Security-Related Requirements
Types of Safety- and Security-Related Requirements

Too often only a Single Type of Requirements is considered. Not just:

• Special Non-Functional Requirements (NFRs):
  — Safety and Security Requirements are Quality Requirements are NFRs
• Safety- and Security-Significant Functional, Data, and Interface Requirements
• Constraints on Functional Requirements
• Architecture and Design Constraints
• Safety and Security Functions/Subsystems
• Software Requirements

Reason for Presentation Title

Safety- and Security-Related Requirements for Software-Intensive Systems
Types of Safety- and Security-Related Requirements

- Product Requirements
  - Functional Requirements
  - Non-Functional Requirements
    - Quality Requirements
      - Defensibility Requirements
        - Safety Requirements
        - Security Requirements
        - Survivability Requirements
    - Data Requirements
    - Interface Requirements
    - Constraints
      - Defensibility Constraints
    - Primary Mission Requirements
  - Derived Requirements
- Stakeholder (Business) Requirements
- Development Method Requirements
- Supporting Requirements
  - Manual Procedure Requirements
  - System/Subsystem Requirements
    - Software Requirements
    - Hardware Requirements
  - Safety Function/Subsystem Requirements
  - Security Function/Subsystem Requirements
  - Survivability Constraints
  - Safety Constraints
  - Security Constraints
  - Survivability Requirements
Types of Defensibility-Related Requirements

- Safety Requirements
  - Safety Requirements
  - Safety-Significant Requirements
  - Safety Function/Subsystem Requirements
  - Safety Constraints

- Security Requirements
  - 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
Types of Safety-Related Requirements

- **Asset / Harm Requirements**
- **Safety Incident Requirements**
- **Hazard Requirements**
- **Safety Risk Requirements**

**Types of Safety Requirements**

- **Safety-Independent Requirements**
  - SIL = 0
- **Safety-Significant Requirements**
  - SIL = 1 - 5
- **Safety-Moderate Requirements**
  - SIL = 2
- **Safety-Critical Requirements**
  - SIL = 4
- **Safety-Intolerable Requirements**
  - SIL = 5

**Safety Integrity Level (SIL)**

- **Safety - Intolerable**
  - SIL = 5
- **Safety - Critical**
  - SIL = 4
- **Safety - Major**
  - SIL = 3
- **Safety - Moderate**
  - SIL = 2
- **Safety - Minor**
  - SIL = 1

**Protect Valuable Assets Requirements**
**Detect Safety Incidents Requirements**
**React to Safety Incidents Requirements**

**Non-Safety Quality Requirements**
**Safety Requirements**

**System Requirements**
**Main Mission Requirements**
**Safety System Requirements**

**Constraints**
Safety and Security Requirements

Safety and Security Requirements are Quality Requirements. Quality Requirements are Product Requirements that specify a mandatory amount of a type of product quality (i.e., quality factor or quality subfactor).

Quality Requirements should be:

• Scalar (How Well or How Much)
• Based on a Quality Model
• Specified in Requirements Specifications
• Critically Important Drivers of the Architecture
Components of a Quality Requirement

- **Quality Requirement**
  - specifies a minimum level of quality of the
  - restricts applicability of
  - provides evidence of existence of
  - is measured against

- **Condition**
  - describes aspect of quality of

- **System-Specific Quality Criterion**
  - must meet or exceed
  - is measured using a

- **Quality Factor**
  - defines the meaning of quality for the

- **Quality Subfactor**
  - is measured against

- **Measurement Threshold**
  - 1..*

- **Quality Measure (Measurement Scale)**
  - 1..*

- **Quality Model**
  - 0..*

- **System**
  - 1..*
Safety- and Security-Significant Requirements

Are identified based on Safety or Security (e.g., hazard or threat) Analysis

Subset of non-Safety and non-Security Requirements:

- Functional Requirements
- Data Requirements
- Interface Requirements
- Other Quality Requirements
- Constraints

Safety/Security Integrity Level (SIL) is not 0:

- May have minor Safety/Security Ramifications
- May be Safety- or Security-Critical
- May have intolerable Safety or Security Risk
SILs and SEALs

Safety/Security Integrity Level (SIL)

a category of required safety or security for safety- or security-significant requirements.

Safety/Security Evidence Assurance Level (SEAL)

a category of required evidence needed to assure stakeholders (e.g., safety or security certifiers) that the system is sufficiently safe or security (i.e., that it has achieved its required SIL).

SILs are for requirements

SEALs are for components that collaborate to fulfill requirements (e.g., architecture, design, coding, testing)
Safety and Security Function/Subsystem Rqmts.

Defensibility Function/Subsystem Requirements are requirements for functions or subsystems that exist strictly to improve defensibility (as opposed to support the primary mission requirements).

• Safety Function or Subsystem Requirements are requirements for safety functions or subsystems.

• Security Function or Subsystem Requirements are requirements for security functions or subsystems.
Safety Function/Subsystem Requirements

Functions or subsystems strictly added for safety:

- Aircraft Safety Subsystems:
  - Collision Avoidance System
  - Engine Fire Detection and Suppression
  - Ground Proximity Warning System (GPWS)
  - Minimum Safe Altitude Warning (MSAW)
  - Wind Shear Alert

- Nuclear Power Plant:
  - Emergency Core Coolant System

All requirements for such functions/subsystems are safety-related.
Example Safety Function/Subsystem Requirements

“Except when the weapons bay doors are open or have been open within the previous 30 seconds, the weapons bay cooling subsystem shall maintain the temperature of the weapons bay below X° C.”

“The Fire Detection and Suppression Subsystem (FDSS) shall detect smoke above X ppm in the weapons bay within 2 seconds at least 99.9% of the time.”

“The FDSS shall detect temperatures above X° C in the weapons bay within 2 seconds at least 99% of the time.”

“Upon detection of smoke or excess temperature, the FDSS shall begin fire suppression within 1 second at least 99.9% of the time.”
Security Function/Subsystem Requirements

Functions or subsystems strictly added for security:

- Access Control Function
- Encryption/Decryption Subsystem
- Firewalls
- Intrusion Detection System
- Virus Protection Application

All requirements for such functions/subsystems are security-related.

Look in the Common Criteria for many reusable example security function requirements.
Safety and Security Constraints

A **Constraint** is any Engineering Decision that has been chosen to be mandated as a Requirement. For example:

- Architecture Constraints
- Design Constraints
- Implementation Constraints (e.g., coding standards or safe language subset)
- Testing Constraints

A **safety constraint** is any constraint primarily intended to ensure a minimum level of safety (e.g., a mandated safeguard).

Safety and Security Standards often mandate Industry Best Practices as Constraints.
Example ZATS Safety Constraints

“When the vehicle is stopped in a station with the doors open for boarding, the horizontal gap between the station platform and the vehicle door threshold shall be no greater than 25 mm (1.0 in.) and the height of the vehicle floor shall be within plus/minus 12 mm (0.5 in.) of the platform height under all normal static load conditions…”

Automated People Mover Standards – Part 2: Vehicles, Propulsion, and Braking (ASCE 21-98)

“Oils and hydraulic fluids shall be flame retardant, except as required for normal lubrication.”

Note need to define flame retardant and normal lubrication.
Common Process:
A Basis for Effective Collaboration
Defensibility & Requirements Engineering

Defensibility-Related Requirements

Defensibility Analysis

- System Analysis
- Stakeholder Analysis
- Asset Analysis
- Vulnerability Analysis
- Event Analysis
- Agent Analysis
- Danger Analysis
- Risk Analysis
- Significance Analysis
- Defense Analysis

Defensibility-Work Products

- Requirements Identification
- Requirements Analysis
- Requirements Validation

Defensibility-Related Requirements

Requirements Team

Stakeholders, Subject Matter Experts, Safety Team, Security Team

Safety Team

Security Team

collaborates with

performs
Systems Analysis

Safety Team

Security Team

collaborates with

performs

System Analysis

Understand Requirements

Safety and Security Engineering

Vision Statement

Context Diagram

Goals

ConOps

Scenarios

Use Cases

Requirements Models

Requirements Specifications

Requirements

Architecture Model

Architecture Documentation

Requirements Engineering

Requirements Team

Architecture Team
Asset Analysis

Safety Team collaborates with Security Team

Project Documentation (RFP, Contract, ConOps)
Generic / Reusable Asset Tables
Standard / Reusable Asset Value and Harm Severity Categories
Generic / Reusable Asset Value and Harm Severity Tables
Standard / Reusable Asset-Harm Goals

Asset Value and Harm Severity Categories
Generic / Reusable Asset Tables

Requirements Team

Asset Identification
Stakeholder Analysis
Asset Use Analysis
Value Analysis
Harm Analysis

Safety and Security Engineering

Safety Team
Security Team

Subject Matter Experts
Stakeholders

Value and Harm Table
Asset Table
Asset Stakeholder Table
Asset Usage Table
Asset-Harm Goals

Requirements Identification
Requirements Analysis
Requirements Validation

Asset-Harm Requirements

Requirements Team

Stakeholders
Subject Matter Experts
Safety Team
Security Team

Subject Matter Experts
Stakeholders

Stakeholder Table

Engineering Safety- & Security-Related Requirements ICCBSS Tutorial
Donald Firesmith, 27 February 2007
© 2007 Carnegie Mellon University
Defensibility Occurrence Analysis

- Subject Matter Experts
- Stakeholders
- Project Documentation (RFP, Contract, ConOps)
- Asset Table
- Asset Value and Harm Table
- Generic / Reusable Attack Type Lists
- Generic / Reusable Defensibility Occurrence Table
- Standard / Reusable Occurrence Likelihood Categories
- Generic / Reusable Occurrence Goals

Safety Team collaborates with Security Team to perform Occurrence Analysis.

Safety and Security Engineering:
- Occurrence Identification
- Abuse Tree Analysis
- Abuse Case Analysis
- Goal Identification
- Defensibility Event Goals

Requirements Engineering:
- Requirement Identification
- Requirement Analysis
- Requirement Validation

Abuse Cases
- Abuse Trees
- Defensibility Occurrence Table

Requirements Team performs Abuse Requirements.

Abuse Trees
- Goal Identification
- Defensibility Occurrence Table

Stakeholders, Subject Matter Experts, Safety Team, Security Team collaborate.
Example Abuse (Attack) Tree
Example Abuse (Mishap and Attack) Tree

- **Defensibility Occurrence**
  - **Attack (A)**
  - **Mishap (M)**

- **ZATS Control Facility Attack or Mishap**
  - **Fire**
    - **Explosion**
      - **Explosive (A)**
      - **Propane (M)**
    - **Arson (A)**
    - **Electrical Fire (M)**
    - **Furnace Fire (M)**
    - **Lightning Fire (M)**
    - **Wild Fire (M)**
  - **Fire Suppression (M)**
  - **River Flooding (M)**
  - **Sprinkler System (M)**
  - **Storm Surge (M)**
  - **Water Pipe Leak (M)**

- **Flooding**
- **Roof**
  - **Snow Load (M)**
  - **Volcanic Ash (M)**
  - **Wind Damage (M)**
  - **Hurricane (M)**
  - **Thunderstorm (M)**
  - **Tornado (M)**

- **Building Collapse**
  - **Earthquake (M)**
  - **Sinkhole (M)**
  - **Tornado (M)**

- **Data Center**
  - **Cooling Loss (M)**
  - **Hardware Failure (M)**
  - **Malware (A)**
  - **Sabotage (A)**
  - **Theft (A)**
  - **Vandalism (A)**

- **Explosion**
  - **Explosive (A)**
  - **Propane (M)**

- **Fire**
  - **Explosive (A)**
  - **Propane (M)**

- **Defensibility Occurrence**
  - **ZATS Control Facility Attack or Mishap**

Legend:
- Inheritance
- Association
Example Abuse (Mishap and Misuse) Cases

- **Storm**
  - **Snow Storm**
  - **Ice Storm**
    - **Tornado**
    - **Hurricane**

- **Thunder Storm**
  - **Strike With Lightning**
    - **Damage Taxis**

- **Rain on Guideways**
  - **Coat Guideways With Ice**
    - **Make Guideways Unsafe**

- **Snow on Guideways**
  - **Drop Debris On Guideways**
    - **Blow Down Building**
      - **Blow Down Control Facility**
      - **Blow Down Maintenance Facility**
      - **Blow Down Taxi Station**

- **Start Fire**

---

Engineering Safety- & Security-Related Requirements ICCBSS Tutorial
Donald Firesmith, 27 February 2007
© 2007 Carnegie Mellon University
Vulnerability Analysis

Requirements Team

- Performs Requirements Identification
- Performs Requirements Analysis
- Performs Requirements Validation

Requirements Engineering

- Vulnerability Requirements
- Vulnerability Constraints

Safety and Security Engineering

- System Vulnerability Analysis
- Organization Vulnerability Analysis
- Vulnerability Identification
- Vulnerability Table
- Defensibility Compliance Repository

Vulnerability Analysis

- Safety Team
- Security Team
- Collaborates with

Vulnerability Identification

- System Vulnerability Analysis
- Organization Vulnerability Analysis

Safety Team

- Safety Team
- Provides input during

Security Team

- Security Team
- Provides input during

Actual / Proposed System Architecture

- Actual / Proposed System Architecture
- Provides input during

Actual / Proposed System Design

- Actual / Proposed System Design
- Provides input during

Actual / Proposed System Implementation

- Actual / Proposed System Implementation
- Provides input during

Asset Value and Harm Table

- Asset Value and Harm Table
- Provides input during

Safety Team

- Safety Team
- Performs

Security Team

- Security Team
- Performs

Software Engineering Institute

Carnegie Mellon
Agent Analysis

Safety and Security Engineering

Stakeholders
- Subject Matter Experts
- Project Documentation (RFP, Contract, ConOps)
- Generic / Reusable Agent Lists
- Generic / Reusable Agent Profiles
- Generic / Reusable Agent-Related Goals

Agent Analysis
- performs
- collaborates with
  - Safety Team
  - Security Team

Agent-Related Requirements
  - Generic / Reusable
  - Standard / Reusable

Agent-Related Goals
  - perfroms

Agent Identification
- Potential Agent List

Agent Profiling
- Agent Profiles

Agent Occurrence Analysis
- Agent Occurrence Table

Agent Goal Development
- Agent-Related Goals

Support Requirements Engineering

Requirements Team
- standard / Reusable Agent-Related Requirements
- Requirements Identification
- Requirements Analysis
- Requirements Validation

Stakeholders
- Subject Matter Experts
- Safety Team
- Security Team
Danger Analysis

Danger Identification

Danger Profiling

DANGER CAUSE ANALYSIS

DANGER EFFECTS ANALYSIS

DANGER LIKELIHOOD ANALYSIS

CAUSE ANALYSIS

ROOT CAUSE ANALYSIS

COMMON CAUSE ANALYSIS

DANGER (Hazard & Threat) Profiles

Requirements Team

Generic / Reusable Hazard and Threat Requirements

Requirements Identification

Requirements Analysis

Requirements Validation

Stakeholders

Other System Documentation

System Safety and Security Documentation

Non-System Documentation

Generic / Reusable Danger Lists

Generic / Reusable Danger Profiles

Generic / Reusable Danger Likelihoods

Safety Team

Security Team

Danger Analysis

Subject Matter Experts

Defensibility Compliance Repository

Stakeholders

Subject Matter Experts

Safety Team

Security Team

Engineering Safety- & Security-Related Requirements ICCBSS Tutorial
Donald Firesmith, 27 February 2007
© 2007 Carnegie Mellon University
Example Fault Tree

Passenger falls out of open door of moving taxi

- Passenger inattentive and near taxi door

- Door opens on moving taxi
  - Taxi door is unlocked
    - Taxi door lock fails unlocked
    - Taxi computer fails
    - Taxi door motor fails open
    - Taxi computer fails

- Train starts moving with open door
  - Taxi door fails to close
  - Taxi starts to move
    - Taxi computer fails
    - Taxi motor fails on
    - Taxi computer fails

- Warning is ineffective
  - A

- Taxi door motor fails open
  - Taxi computer fails
Example Event Tree

- Passenger near open door on moving taxi
  - Taxi Speed Sensor
  - Door Position Sensor
  - Door Motor
  - Taxi Brakes
  - Warning Speaker

- Passenger protected
  - Passenger may fall out of stopped taxi
  - Passenger likely to fall out of stopped taxi
  - Passenger may fall out of moving taxi
  - Passenger likely to fall out of moving taxi
  - Passenger likely to fall out of moving taxi
Example Cause and Effect Tree

Legend

- **Event**
- **Hazardous Event**
- **Accident**
- **State**
  - **Hazard**
  - **Harm**

Two taxis approach point where their individual guideways merge

- **Guideway location identifier** has failed
- **Taxi 2 location sensor** has failed
- **Right-of-way not requested**
- **Lack of right-of-way ignored**
- **Taxi 2 computer has failed**
- **Taxi 2 power fails on**
- **Taxi 2 brakes fail off**
- **No warning sent**
- **Failure to yield not observed**

Taxi (1) with right-of-way fails to yield once taxi (2) without right-of-way fails to yield

- **Taxi 1 transmitter has failed**
- **Taxi 1 computer has failed**
- **Taxi 1 power fails on**
- **Warning ignored**

Two taxis moving too fast to stop

- **Warning ignored**
- **No warning received**

Merging taxis collide

- **Guideway is damaged**
- **Taxi(s) are harmed**
- **Taxi(s) crash off guideway into habitat**
- **Taxi(s) crash off guideway into parking lot**

Passenger(s) are harmed

- **Passenger(s) are killed**
- **Passenger(s) are injured**

Animal(s) are harmed

- **Animals are harmed**

Patrons’ vehicles are harmed

- **Patrons’ vehicles are harmed**
- **Taxi(s) are destroyed**
- **Taxi(s) are damaged**
Defense Analysis

Defense Analysis performs the following tasks:

1. Countermeasure and Safeguard Type Lists
2. List of Defense Functions / Subsystems
3. Vendor Trade Studies
4. Countermeasure and Safeguard Selection Reports

Requirements Team performs the following tasks:

1. Defense Functionality Requirements
2. Requirements Validation
3. Requirements Identification
4. Defense Constraints

Safety and Security Engineering performs the following tasks:

1. Countermeasure and Safeguard Type Lists
2. List of Defense Functions / Subsystems
3. Vendor Trade Studies
4. Countermeasure and Safeguard Selection Reports

Requirements Team collaborates with Safety Team and Security Team.

Defence Analysis collaborates with Subject Matter Experts and Stakeholders.

Defence Analysis provides input during Safety and Security Engineering.

Defence Analysis provides input during Requirements Engineering.

Defence Analysis collaborates with Market Research.

Defence Analysis performs Defense Type Identification.

Defence Analysis performs Defense Functionality Identification.

Defence Analysis performs Defense Selection.

Defence Analysis performs Defense Adequacy Analysis.

Defence Analysis collaborates in the performance of Architecture.

Defence Analysis collaborates with Architecture Team.

Defence Analysis collaborates with Requirements Team.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Standard Defense Functionality and Constraint Requirements.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Standard Defense Functionality and Constraint Requirements.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.

Defence Analysis collaborates with Generic / Reusable Safeguard and Countermeasure Lists.

Defence Analysis collaborates with Safety and Security Assurance Level (SAL) Allocations.

Defence Analysis collaborates with Stakeholders.

Defence Analysis collaborates with Subject Matter Experts.

Defence Analysis collaborates with Safety Team.

Defence Analysis collaborates with Security Team.
Defense Certification and Accreditation
Conclusion:

Process Improvement Recommendations
Conclusion

Engineering safety-significant requirements requires appropriate:

- Concepts
- Methods
- Techniques
- Tools
- Expertise

These must come from both:

- Requirements Engineering
- Safety Engineering
Conclusion

There are four types of Safety- and Security-related Requirements:

- Safety and Security Quality Requirements
- Safety- and Security-Significant Requirements
- Safety and Security Function/Subsystem Requirements
- Safety and Security Constraints

Different Types of Safety- and Security-related Requirements have different Structures.

These different Types of Requirements need to be identified, analyzed, and specified differently.
Conclusion

Processes for Requirements Engineering, Safety Engineering, and Security Engineering need to be:

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


Better Integrate Safety and Security Processes:

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

Better Integrate Safety and Security Processes with Requirements Process:

• 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 the proper Properties.