Systems Engineering

University of San Diego

Application to Information Security

Mark R. Heckman

University of San Diego

Align Security With Mission

- Security is typically not the mission of an organization
- It helps to enable the organization to achieve its mission
- How can we make sure to align security objectives with the organizational mission?
- Systems engineering concepts can help

Today's Outline

- What is a system?
- What is systems engineering?
- What is a "secure system"?
- How to apply systems engineering techniques to build secure systems

What is a System?

- A system is an arrangement of parts or elements
  - that together exhibit behavior or meaning
  - that the individual constituents do not.

- A system's properties emerge from
  - the parts or elements and their individual properties; AND
  - the relationships and interactions between and among the parts, the system and its environment.

INCOSE. 2019. *Systems Engineering and System Definitions*, version 1.0. International Council on Systems Engineering (INCOSE), INCOSE-TP-2020-002-06. (https://www.incose.org/docs/default-source/default-document-library/incose-se-definitions-tp-2020-002-06.pdf?sfvrsn=b1049bc6_0)

What is an Engineered System?

- An engineered system is a system
  - designed or adapted to interact with an anticipated operational environment
  - to achieve one or more intended purposes
  - while complying with applicable constraints.

What is Systems Engineering?

- Systems Engineering is a transdisciplinary and integrative approach
  - to enable the successful realization, use, and retirement of engineered systems,
  - using systems principles and concepts, and scientific, technological, and management methods

Example Systems for Cybersecurity

- Computers and computer-based devices
- Networks of computers
- People building and managing the systems, and the sensitive information they contain

- Each consists of
  - Software,
  - hardware,
  - information technology,
  - and the human element (e.g., designers, operators, users, attackers of these systems)

Engineered Systems for Cybersecurity

- Designed to interact with a defined operational environment to achieve intended purposes within applicable constraints

- I.e., to enforce security goals

What is a Secure System?

- Three essential characteristics of a secure system
  - It enables the delivery of the required system capability
    - despite intentional and unintentional forms of adversity.
  - It enforces constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized
    - while satisfying the first characteristic.
  - It enforces constraints based on a set of rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur
    - while satisfying the second characteristic.

I.e., A Secure System ...

- Does what it is supposed to do, despite intentional or unintentional disruptions
- Does only what it is supposed to do, and nothing else
- Enforces rule-based constraints on interactions with people and other systems

Systems Engineering for Cybersecurity

- Engineering trustworthy, secure systems requires
  - a transdisciplinary approach to protection,
  - a determination across all assets where loss could occur,
  - and an understanding of adversity, including how adversaries attack and compromise systems.
    - I.e., risk and threat assessment

NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems November 2022 (https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final)

Systems Engineering Reqs for Cybersec

- Substantial investment in the requirements, architecture, and design of systems, components, applications, and networks.
- Compelling evidence to support claims that it meets its requirements to deliver the protection and performance needed by stakeholders.
- A disciplined, structured, and standards-based set of systems security engineering activities and tasks

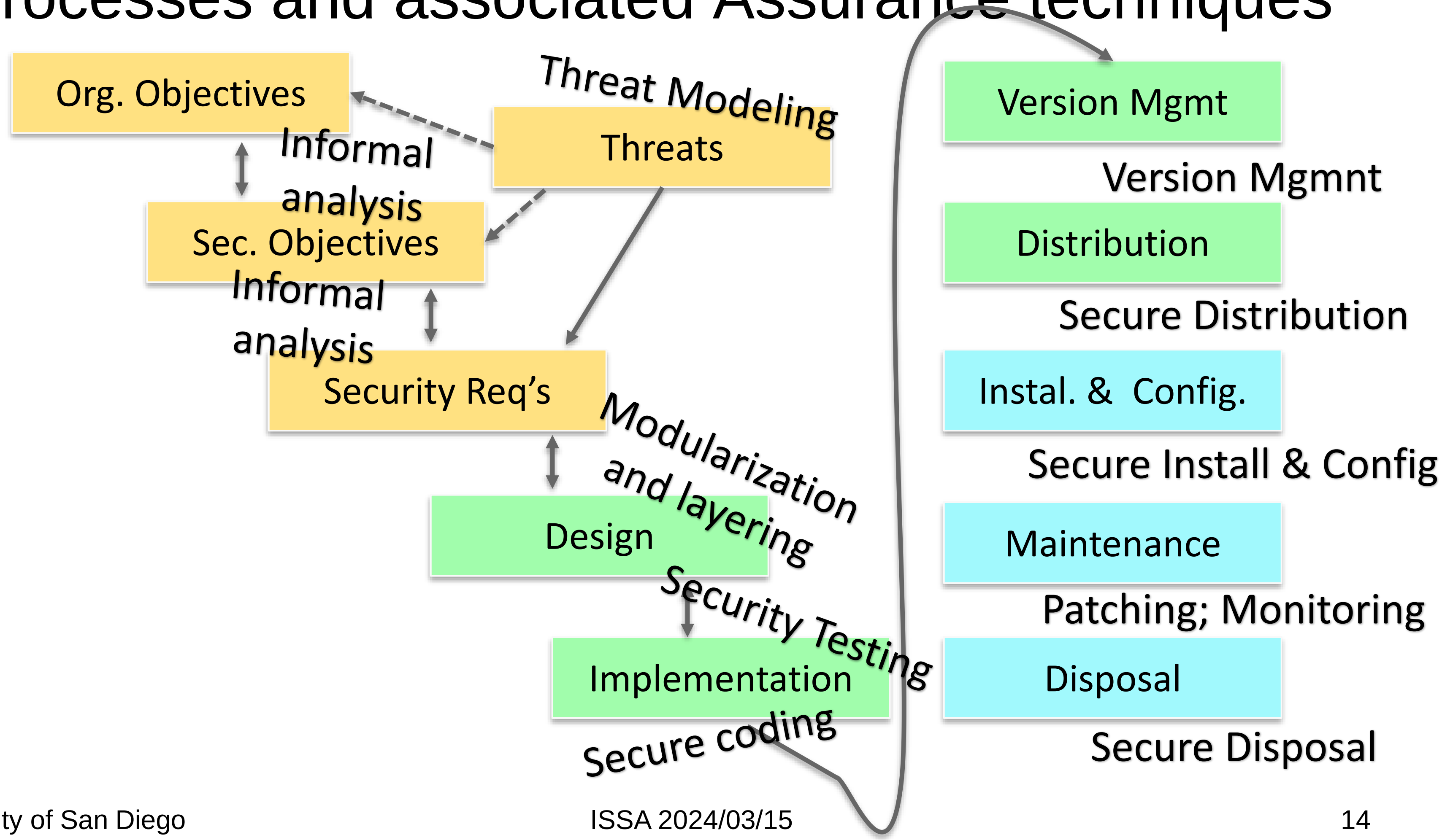
Technical Lifecycle Processes

- Business or Mission Analysis
- Stakeholder Needs and Requirements Definition
- System Requirements Definition
- System Architecture Definition
- Design Definition
- System Analysis
- Implementation
- Integration
- Verification
- Transition
- Validation
- Operation
- Maintenance
- Disposal

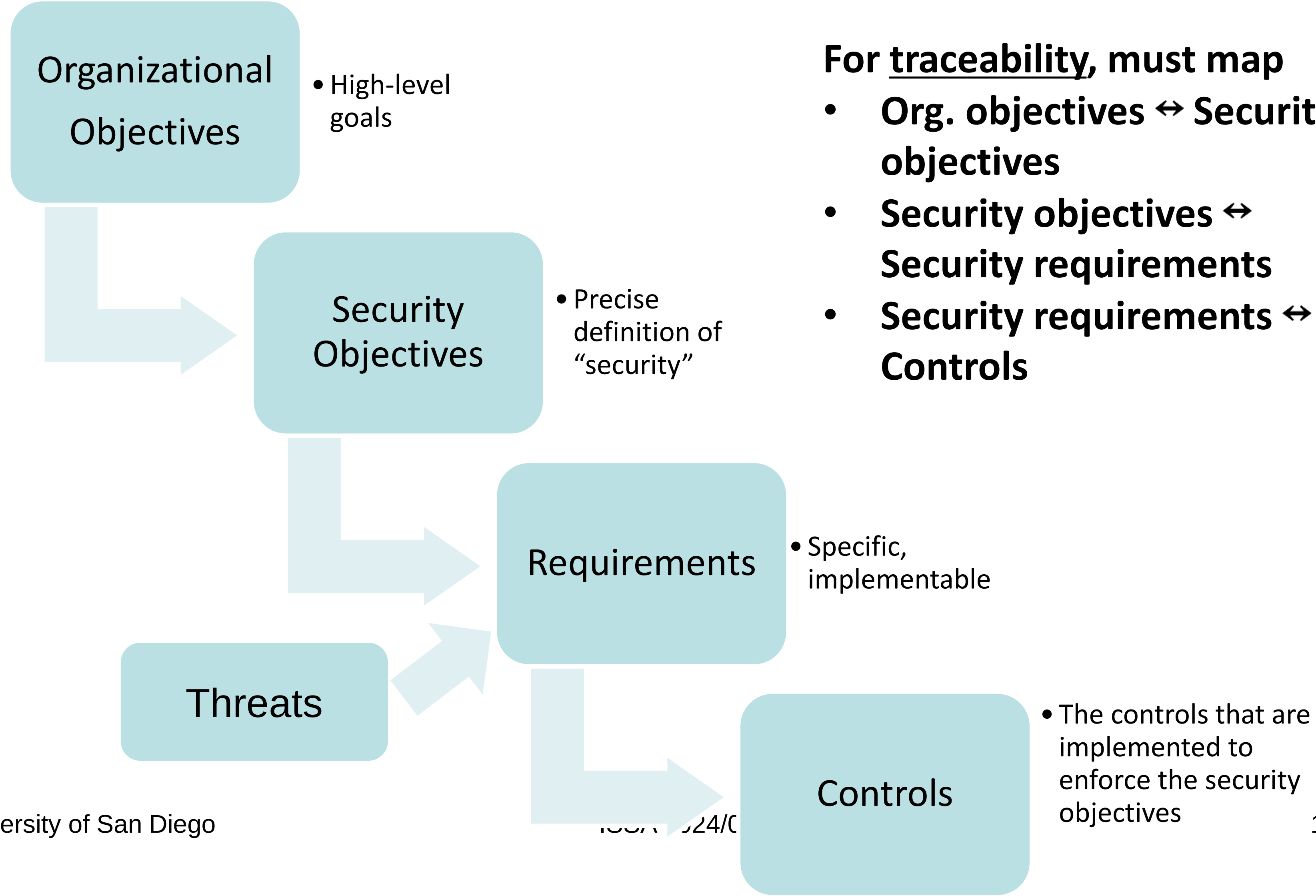
Appendix H of NIST SP 800-160v1r1

Simplified Process List

- Processes and associated Assurance techniques



Security Objectives, Policy, Requirements, and Specification of Controls



Organizational Objectives
• High-level goals
Security Objectives
• Precise definition of "security"
Requirements
• Specific, implementable
Threats
Controls
• The controls that are implemented to enforce the security objectives

For traceability, must map

- **Org. objectives ↔ Security objectives**
- **Security objectives ↔ Security requirements**
- **Security requirements ↔ Controls**

Traceability at All Levels

- For traceability, must map
  - Org. objectives ↔ Security objectives
  - Security objectives ↔ Security requirements
  - Security requirements ↔ Controls

- Usually not a formal (mathematical) process
- Use informal techniques to show traceability

- Gaps are not good – leaves a “hole” in security
- “Extras” are not good – wasted effort and resources

Organizational Objectives

- Sometimes called “business objectives” or “business drivers” or “mission”
  - E.g., “make money and stay in business”
- Typically NOT what you would call security objectives
  - They usually don’t mention security at all
- But security enables them

Sources of Organizational Objectives

- Laws and regulations (compliance)
- Client expectations
- Organizational “mission”
  - For commercial orgs: stay in business and make money
  - For the US DoD: national security
  - For a resistance radio station against an authoritarian government: to keep broadcasting resistance content
  - Goal: Maximize “value”, as defined by mission
- Organization’s own needs wrt security
  - E.g., protect intellectual property (IP)

Example: Organizational Objective

- An HMO needs to be compliant with laws and regulations concerning the security and privacy of personal health information
  - I.e., HIPAA
- Or else face penalties – financial or worse

- What is the HMO's objective?

- To comply with HIPAA

Example: Organizational Objective

- Amazon Web Services (AWS) wants to do business with the U.S. Department of Defense (DoD)
- DoD has very strict security standards
  - The DoD Cloud Computing Security Requirements Guide (SRG) provides a standardized assessment and authorization process so cloud service providers can serve DoD customers (https://iasecontent.disa.mil/cloud/SRG/index.html)

- What is Amazon's objective?
- To comply with the DoD SRG

Example: Organizational Objective

- Google Drive advertises that users can store personal files in their own private space, and share selected files with others so that only those given authorization will be able to access the files
- Customers expect and depend on the Google Drive service to protect their files, or they will go someplace else and Google will lose business

- What is Google's objective?
- To satisfy customers' expectations

Example: Organizational Objective

- Netflix provides streaming, but only allows customers to download streamed content under very controlled circumstances
- Netflix implements expensive Digital Rights Management (DRM), using such mechanisms as
  - Encrypted streaming
  - Backend authentication
  - IP/Geographic restrictions
- What is Netflix’s objective?
- Permit only paying customers to view content
- Prevent violations of Netflix’s contracts with content creators

Priorities and Resources

- An organization often must prioritize organizational objectives
  - E.g., What is the higher priority: serving customers or securing data?

- Also consider amount of resources the organization is willing or able to dedicate to security

- The priorities and available resources will necessarily constrain the security objectives

Org. Objectives are High Level

- Organizational objectives are usually high level
- And not expressed in security terms
- Can’t easily translate into system requirements

- E.g.:
  - **Organizational Objectives: *Protect IP***

- How to put that in terms that can be implemented?

Security Objectives

- Intermediate step: **Security objectives**

- Transition between high-level org objectives and implementable security requirements

- E.g.:
  - Organizational Objective: *Protect IP*
  - **Security Objective: *Only authorized employees shall be permitted to access confidential intellectual property***

The Definition of “Secure” for a System

- **Security objectives are the definition of “security” for the system**

- As in, “the system can be considered secure if ...”

- The complete set of security objectives are the list of necessary and sufficient conditions for “security” for the system

Types of Security Objectives

- Compliance with security laws and regulations
  - I.e., same as organizational objective
- Access control policy
  - In terms of protected assets
  - I.e., statements based on security concepts that you are familiar with: Confidentiality, Integrity, Availability, Authenticity, Non-repudiation
- System integrity objectives
- Security management objectives
  - E.g., to support auditing and effectiveness metrics
- Survivability

One-to-Many

- There may be many security objectives, even for a single organizational objective
- Consider the org. objective: *protect IP*
- What are the set of necessary and sufficient conditions that would enable us to say “this system is secure with respect to protecting IP”?

Necessary and Sufficient Objectives

- For each organizational objective, create necessary and sufficient security objectives
  - E.g., Org. objective: *Protect IP*
  - Security objectives:
    1. Only authorized employees can access the IP
    2. Only senior management, or administrators designated by senior management, shall be able to grant and revoke authorization to access IP
    3. Whenever an authorized person reads the IP, it must be possible for them to determine that the IP is authentic
    4. The IP must be available when needed by authorized people
    5. The identities of everyone who accesses the IP must be reliably recorded for auditing purposes
    6. All systems that store, process, and transmit the IP, or that control access, or that store, transmit, or process audit records, must be protected from compromise and tampering

How Do We Know We Have Them All?

- How do we know that we have found all of the necessary and sufficient security objectives to support the organizational objectives?

- Is there a formal process of finding them?
  - Something you can do by rote, or automatically?

We Don’t Know

- How do we know that we have found all of the necessary and sufficient security objectives to support the organizational objectives?

- Is there a formal process of finding them?
  - Something you can do by rote, or automatically?

- NO!
- Use informal methods and try your best
  - Repeat as necessary (e.g., after threat analysis)

Security Objectives, NOT Controls

- One of the security objectives above says “All systems that store, process, and transmit the IP, or that control access, or that store, transmit, or process audit records, must be secure from compromise and protected from tampering”

- Note that the objective does not say how to secure the systems from compromise or tampering
  - It does not specify security requirements, just objectives
    - Except, perhaps, when security objectives are simply statements of compliance that mention particular controls

Traceability

- For every organizational objective, there must be a sufficient set of security objectives
  - “forward traceability”
  - Any gaps means you have a hole in your security
  - It is possible for a security objective to support more than one organizational objective
- Every security objective must support one or more organizational objectives
  - “backward traceability”
  - Extraneous security objectives are wasteful

When Should You Discover Security Objectives?

- The time to discover the security objectives is
  - Before you begin the threat assessment
  - Before you determine the security requirements

- Threats are only dangerous because they could cause a failure to achieve the security objectives

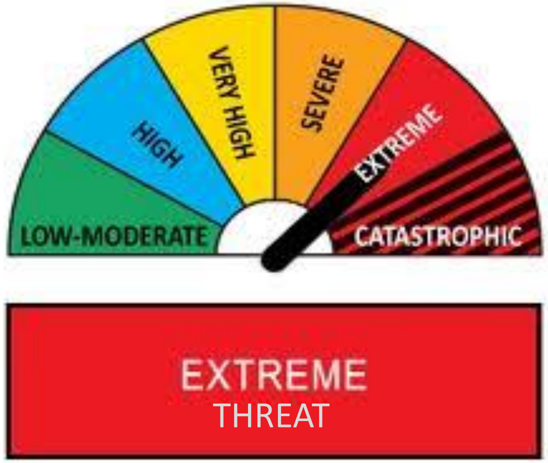
- Security requirements are specific controls implemented to block or mitigate threats so that security objectives can be achieved

Security Objectives Depend on Threats

- Use threat analysis to help discover security objectives that you hadn't already thought of
  - A threat is only a threat if it could violate the security objectives
  - If you identify what you think is a threat, but don't have a corresponding security objective that it would violate, you need to add that objective to your list

What is Threat Modeling?

- A process to
  - identify threats against a system
    - Viz., that would violate the system security objectives
  - determine appropriate countermeasures
  - And thereby increase system assurance
- Carried out early in the design process
  - To help identify security requirements



What are Requirements?

- Tell what the system is supposed to do
- “What”, not “how”
- What is the problem that needs to be solved?

More About Requirements

- May be high-level, abstract statements
  - Of a function or service
  - Of a system constraint
- Or may be highly detailed
  - E.g., mathematical specification of an algorithm
- Problem is that the term “requirements” is overloaded (has multiple meanings)

Need for Requirements

- Abstract requirements are sufficiently abstract that they do not pre-define an implementation
  - E.g., when the Government puts out a “request for proposal” (RFP) for contractors to bid on
  - To try to prevent confusion, I’ve used the term “objectives” to mean this high-level abstract statement of requirements
- System requirements define the system sufficiently well that the contractor and client can agree on the scope of work and the definition of “done”

Types of Requirements

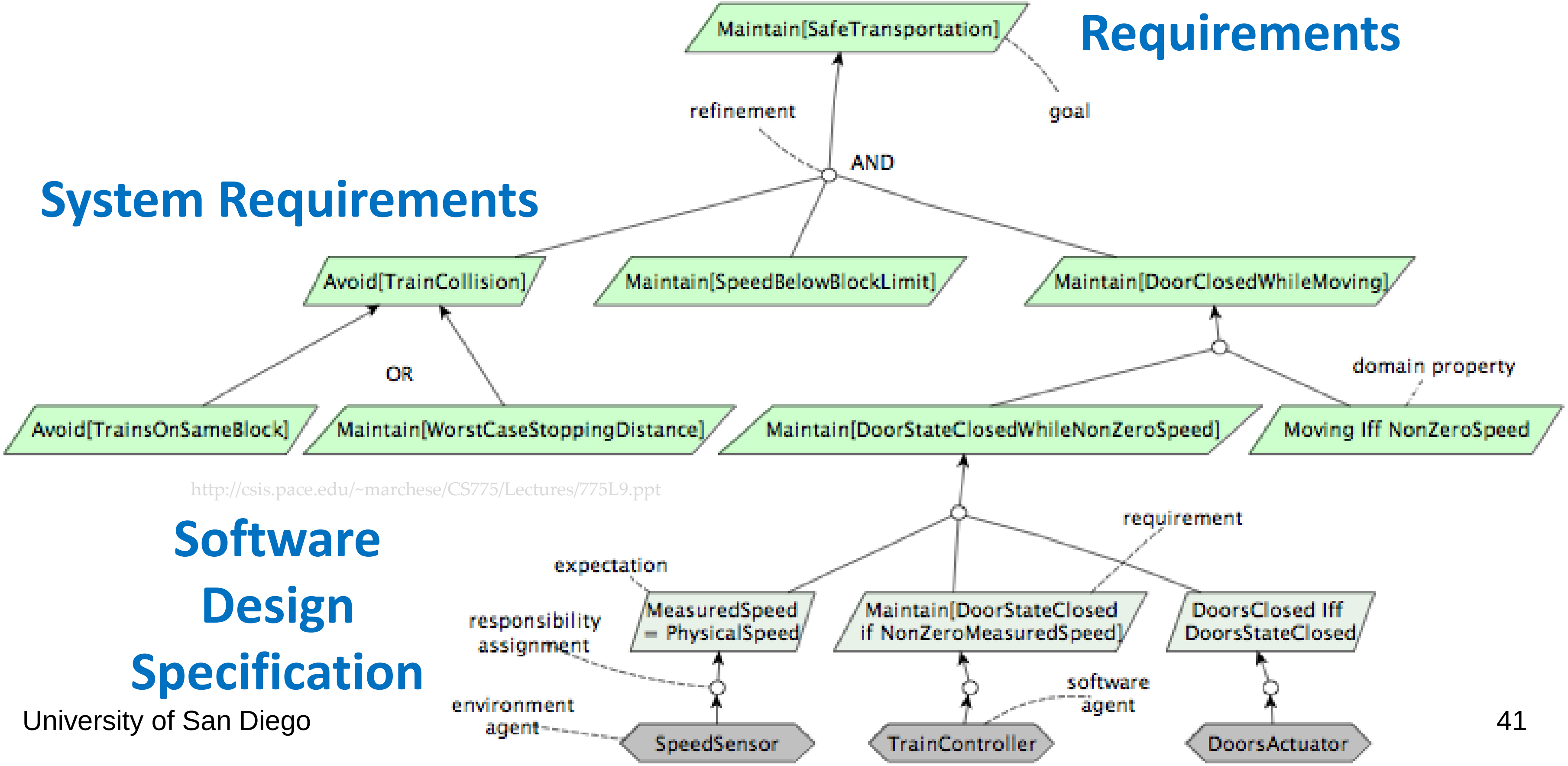
- User requirements
  - The high-level requirements – also called “definitions”
  - Describe the services that the system provides to users, plus any operational constraints on those services
- System requirements
  - More detailed than user requirements
  - Serve as the contract between the client and contractor
- Software specification
  - Highly-detailed document provided to developers as the basis for design and implementation
- There are security requirements of each type

Goal Decomposition and Contribution

- Goal decomposition (forward)
- Goal contribution (reverse)

User Requirements

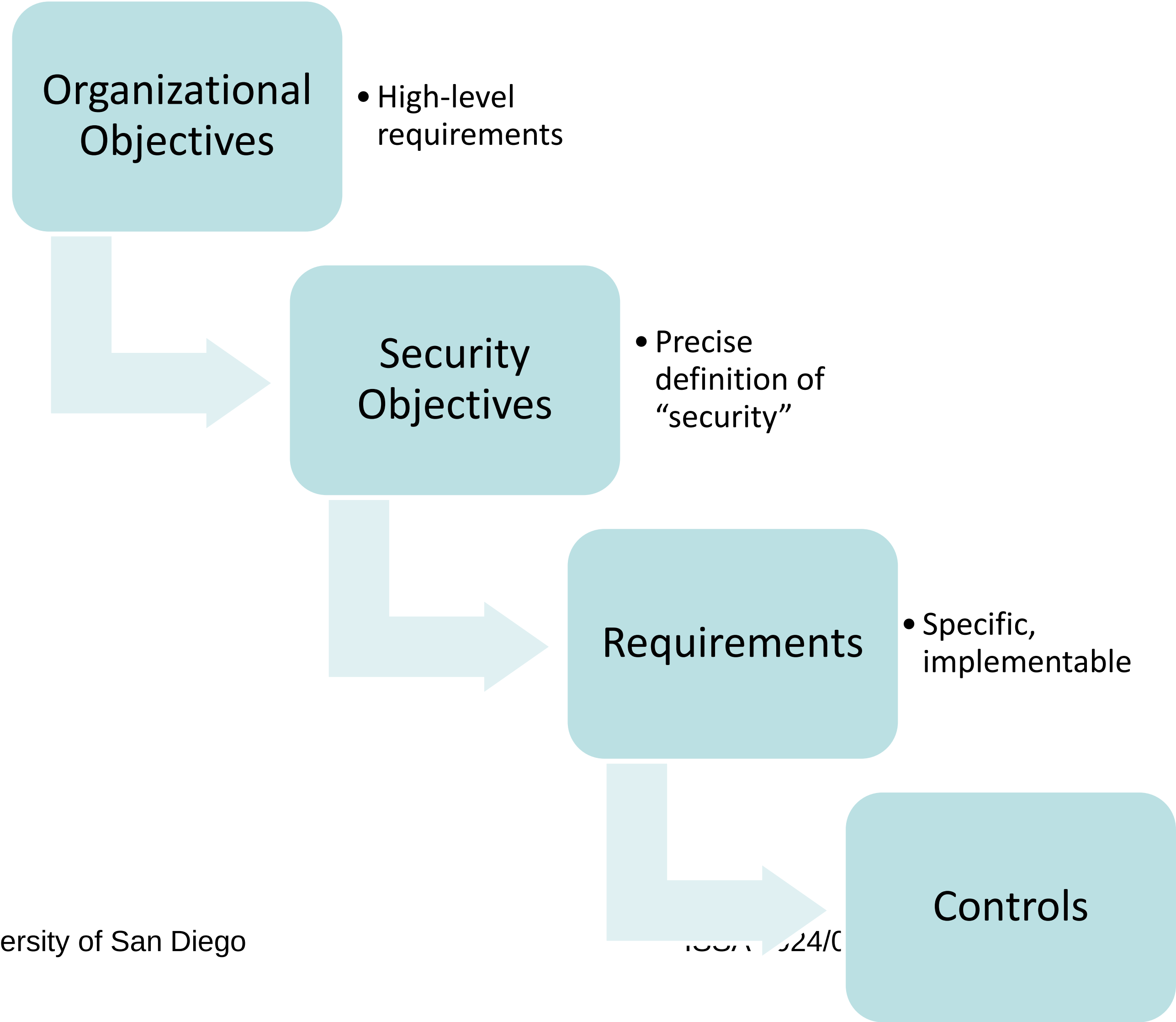
System Requirements


Maintain[SafeTransportation]
refinement
goal
AND
Avoid[TrainCollision]
Maintain[SpeedBelowBlockLimit]
Maintain[DoorClosedWhileMoving]
OR
domain property
Avoid[TrainsOnSameBlock]
Maintain[WorstCaseStoppingDistance]
Maintain[DoorStateClosedWhileNonZeroSpeed]
Moving Iff NonZeroSpeed
requirement
expectation
MeasuredSpeed = PhysicalSpeed
Maintain[DoorStateClosed if NonZeroMeasuredSpeed]
DoorsClosed Iff DoorsStateClosed
responsibility assignment
software agent
environment agent
SpeedSensor
TrainController
DoorsActuator

http://csis.pace.edu/~marchese/CS775/Lectures/775L9.ppt

Software Design Specification

Security Objectives, Policy, Requirements, and Specification of Mechanisms



Organizational Objectives

- High-level requirements

Security Objectives

- Precise definition of “security”

Requirements

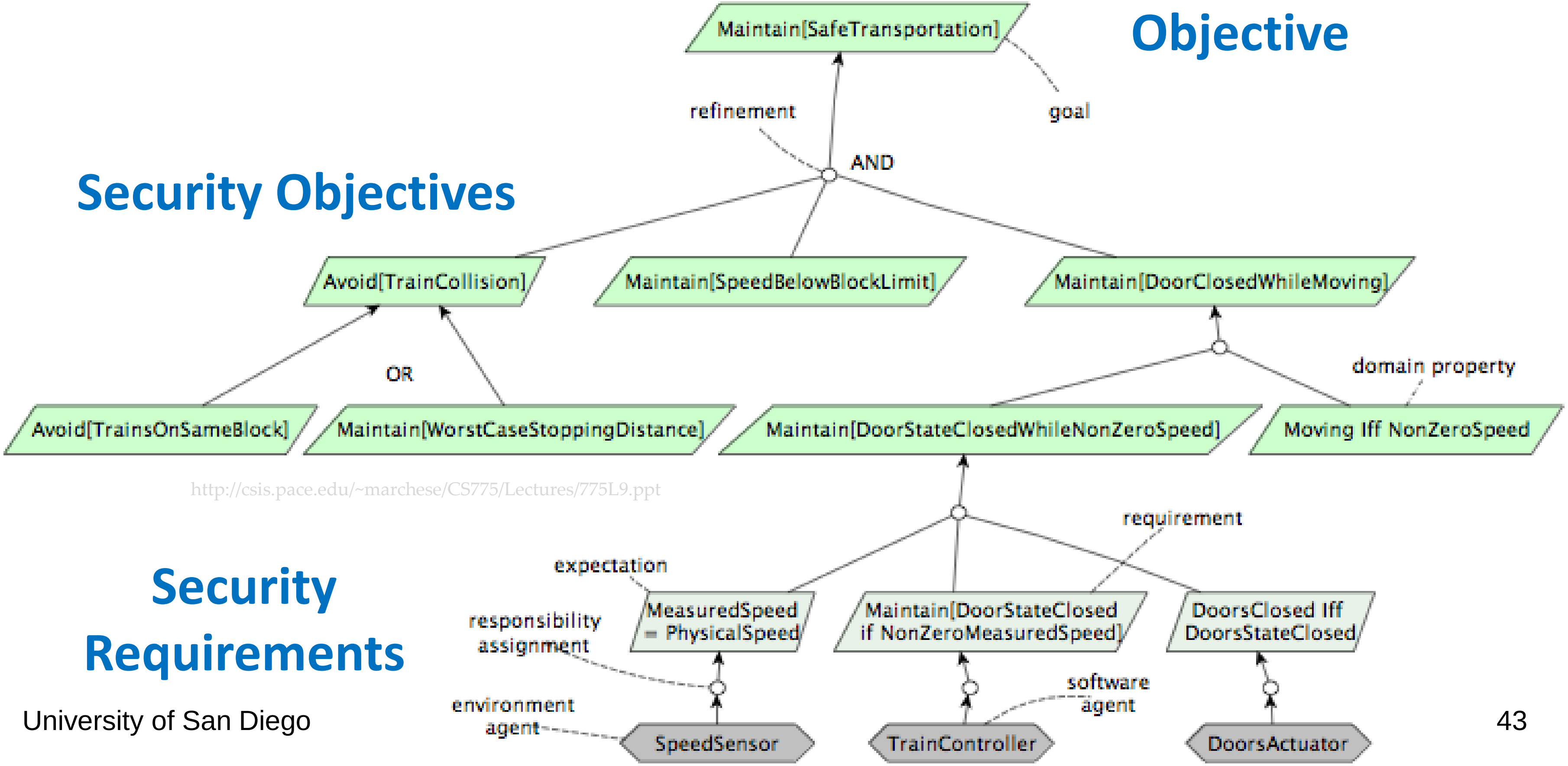
- Specific, implementable

Controls

- The controls that enforce the policy

Goal Decomposition and Contribution

- Goal decomposition (forward)
- Goal contribution (reverse)


Maintain[SafeTransportation]
goal
refinement
AND
Avoid[TrainCollision]
Maintain[SpeedBelowBlockLimit]
Maintain[DoorClosedWhileMoving]
OR
domain property
Avoid[TrainsOnSameBlock]
Maintain[WorstCaseStoppingDistance]
Maintain[DoorStateClosedWhileNonZeroSpeed]
Moving Iff NonZeroSpeed
requirement
expectation
responsibility assignment
MeasuredSpeed = PhysicalSpeed
Maintain[DoorStateClosed if NonZeroMeasuredSpeed]
DoorsClosed Iff DoorsStateClosed
software agent
environment agent
SpeedSensor
TrainController
DoorsActuator

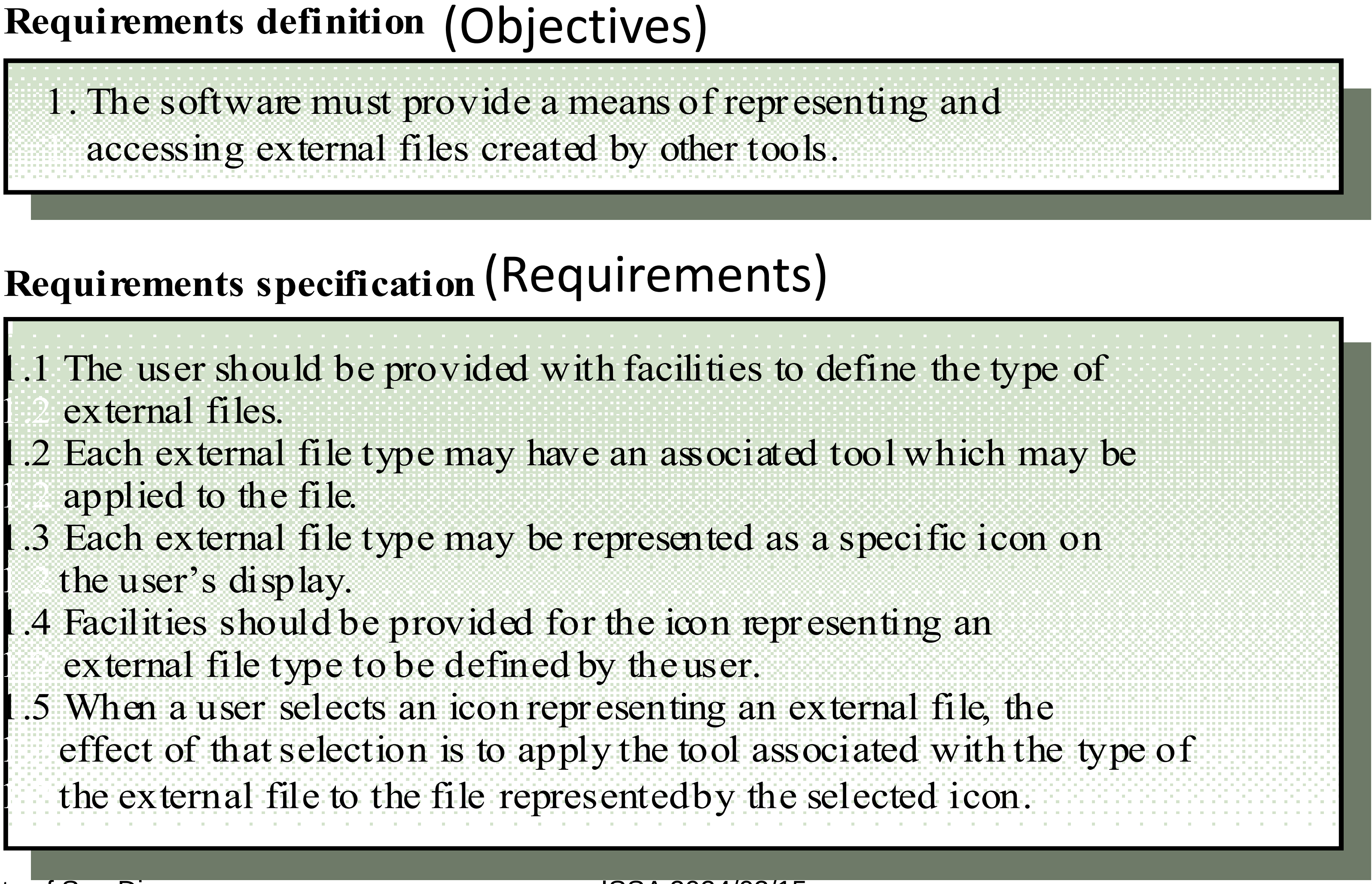
Organizational Objective

Security Objectives

Security Requirements

http://csis.pace.edu/~marchese/CS775/Lectures/775L9.ppt

Requirements Derived from Objectives



Requirements definition (Objectives)

1. The software must provide a means of representing and accessing external files created by other tools.

Requirements specification (Requirements)

1.1 The user should be provided with facilities to define the type of external files.

1.2 Each external file type may have an associated tool which may be applied to the file.

1.3 Each external file type may be represented as a specific icon on the user's display.

1.4 Facilities should be provided for the icon representing an external file type to be defined by the user.

1.5 When a user selects an icon representing an external file, the effect of that selection is to apply the tool associated with the type of the external file to the file represented by the selected icon.

Ian Sommerville, Software Engineering

Example Security Objective, Policy, Etc.

- **Organizational Objective** – “Only authorized people have access to protected data”
- **Security Objective** – What data is protected, who has access, what kind of access they have
- **Requirement** – Must be able to reliably identify people who are authorized
- **Requirement** – Data must be protected from access by unauthorized people or people who haven’t been identified
- **Control** – Passwords (or multi-factor)
- **Control** – Encryption

Traceability

- Required in both directions

- **How can you show that you have sufficient mechanisms to satisfy a requirement?**
  - For each requirement, you must show that the mechanisms are sufficient and consistent
- **How can you show that a mechanism is necessary and not just a waste of money and time?**
  - For each mechanism, you must show how it helps to satisfy a requirement