HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 17, 2023

Considering Change

UNDERSTANDING SECURITY WEAKNESSES IN SAFETY-CRITICAL SYSTEMS

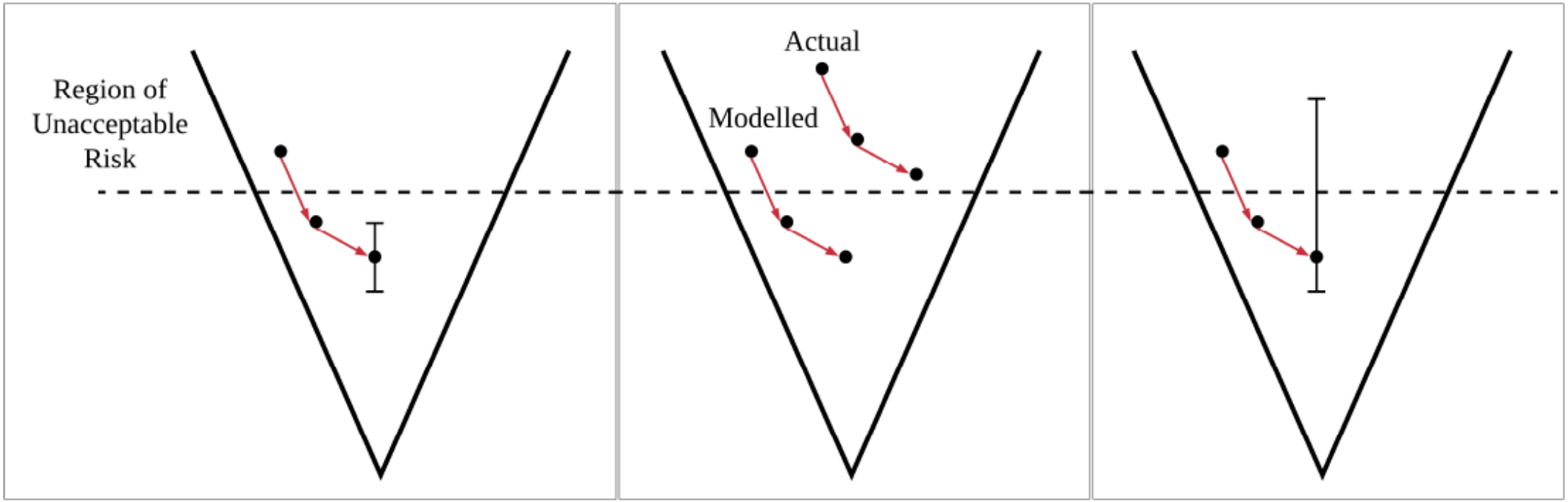
DR NIKITA JOHNSON, ROLLS-ROYCE

17 OCTOBER 2023

Overview

- Fundamentals: Risk, Causal Model, Case
- Security Argument Structure
- Vulnerability Management
- Safety-Security Alignment

Framing the Problems of Security Change on Safety



(a) Security ALARP – understanding Risk

(b) Incorrect risk estimation

(c) Insufficient confidence

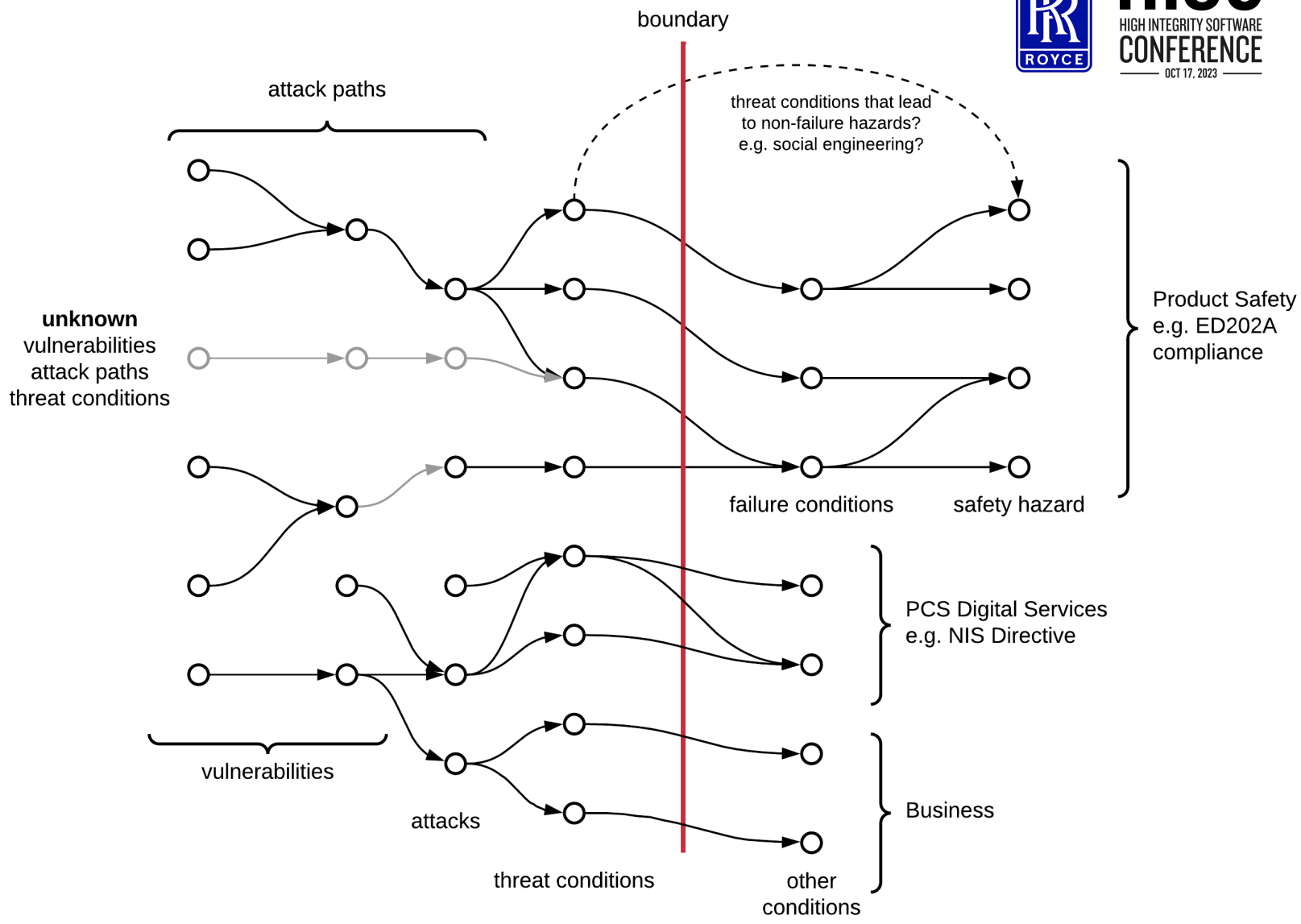
Fundamentals – Causal Model

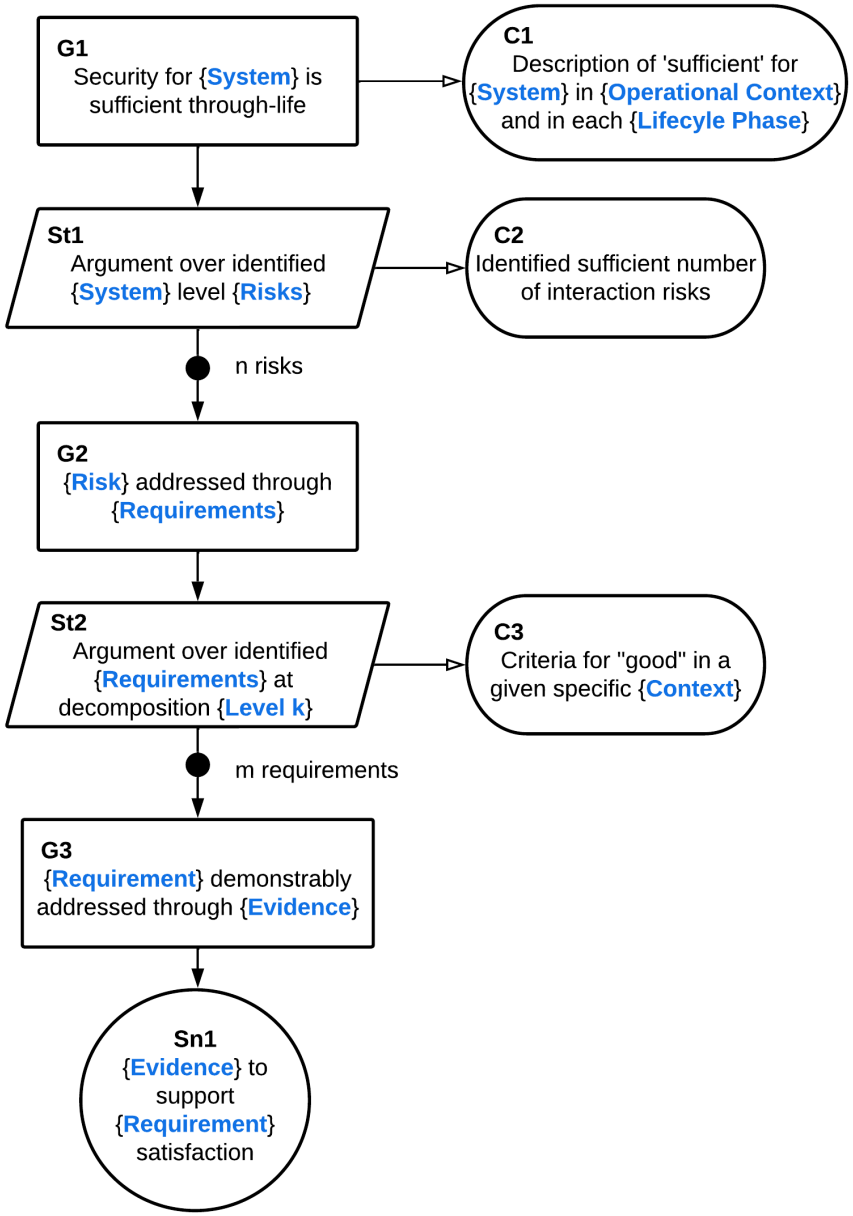
- security risk vs safety risk

- definition of threat condition

- uncertainty introduced by malicious actors

- linking concepts in several sectors
  - Aerospace
  - Rail
  - ICS
  - Nuclear
  - Medical Devices





ROLLS ROYCE HISC HIGH INTEGRITY SOFTWARE CONFERENCE OCT 17, 2023

Security 4+1 Principles

1. Security Requirements Defined
2. Security Requirements Decomposed
3. Security Requirements Satisfied
4. Threats Identified

4+1 Security Confidence

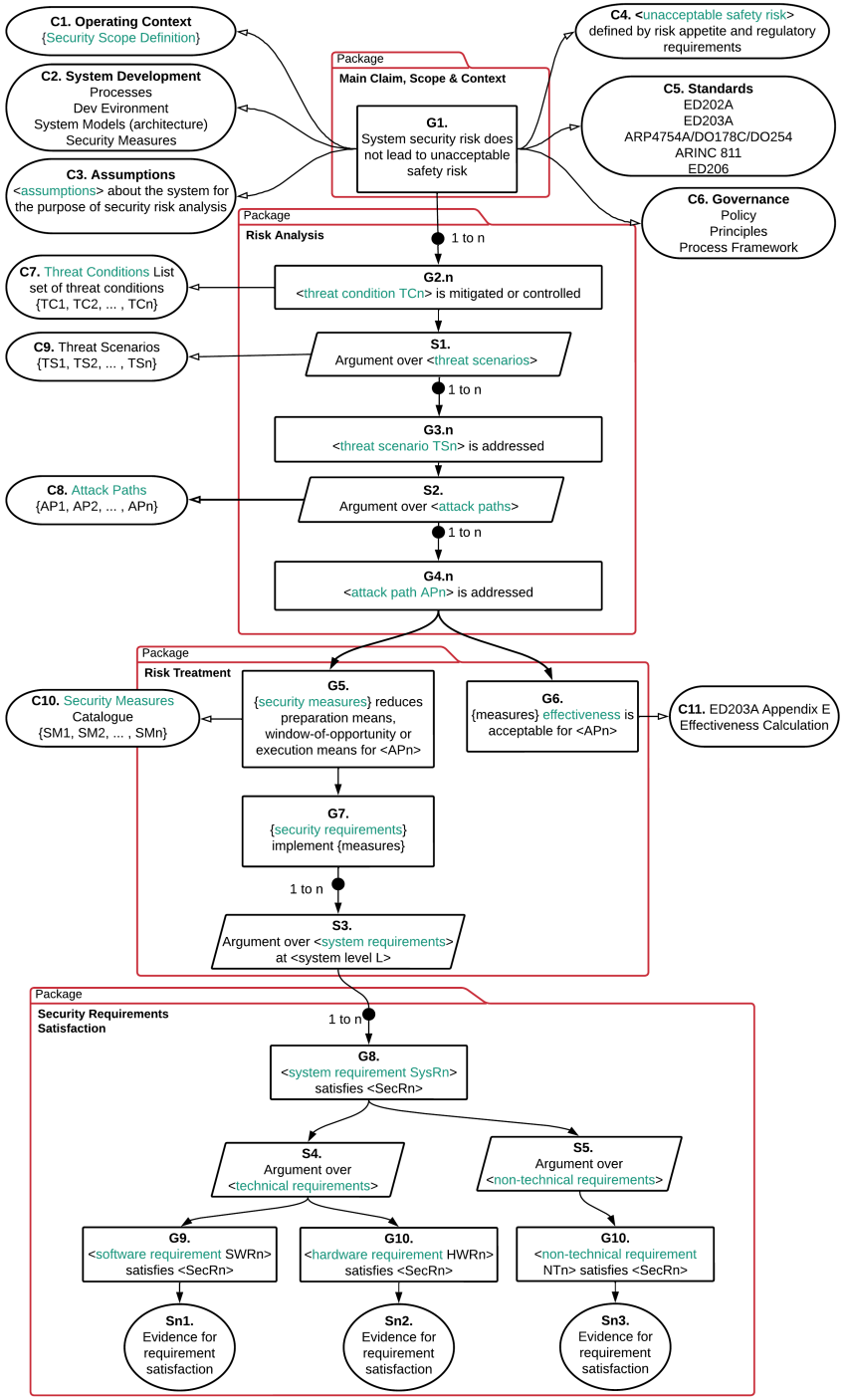
Overview

Fundamentals: Risk, Causal Model, Case

Security Argument Structure

Vulnerability Management

Safety-Security Alignment

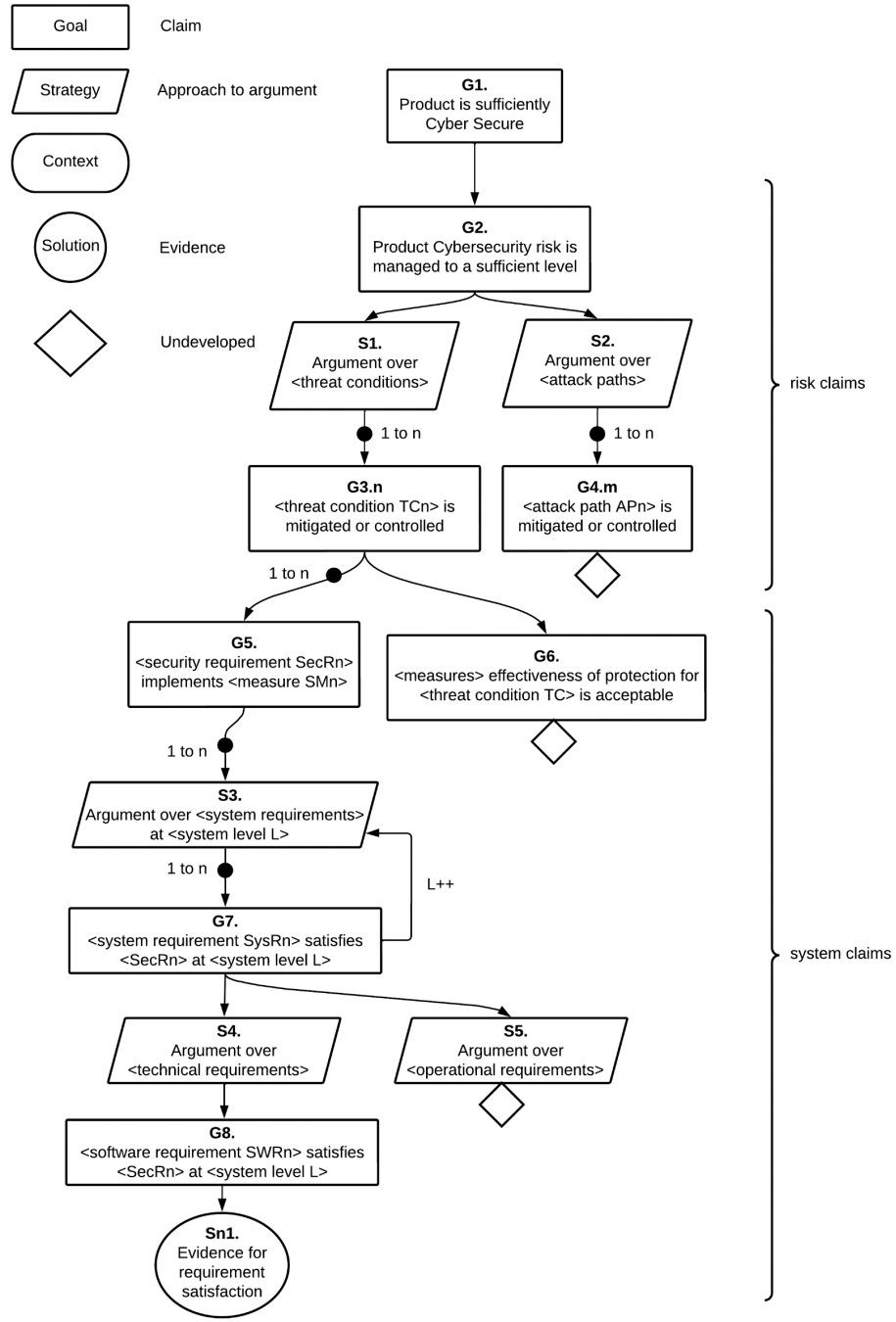


Detailed View of Security Case

Security Case

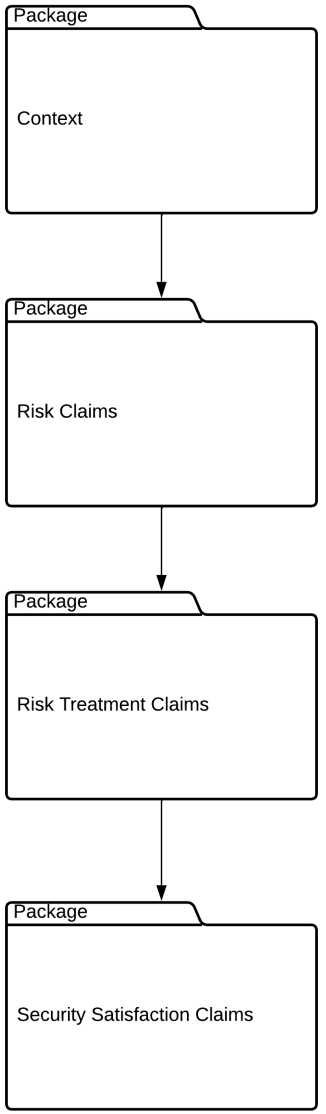
- claims developed during risk and assurance

- claims developed during system, software and hardware development



Security Case “Modules”

- Context and scope
- Risk Package
- Treatment Package
- Requirements Satisfaction Package



Overview

Fundamentals: Risk, Causal Model, Case

Security Argument Structure

Vulnerability Management

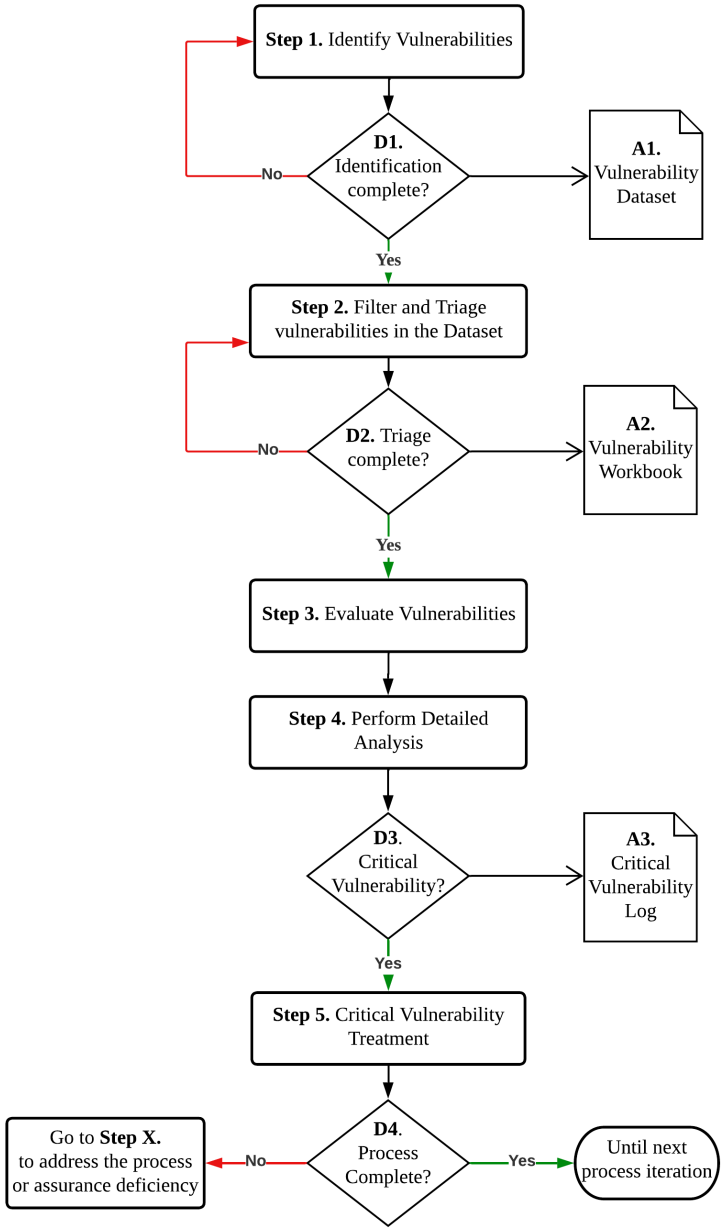
Safety-Security Alignment

HICLASS

AdaCore ALTRAN BAE SYSTEMS Callen-Lenz COBHAM COCOTEC

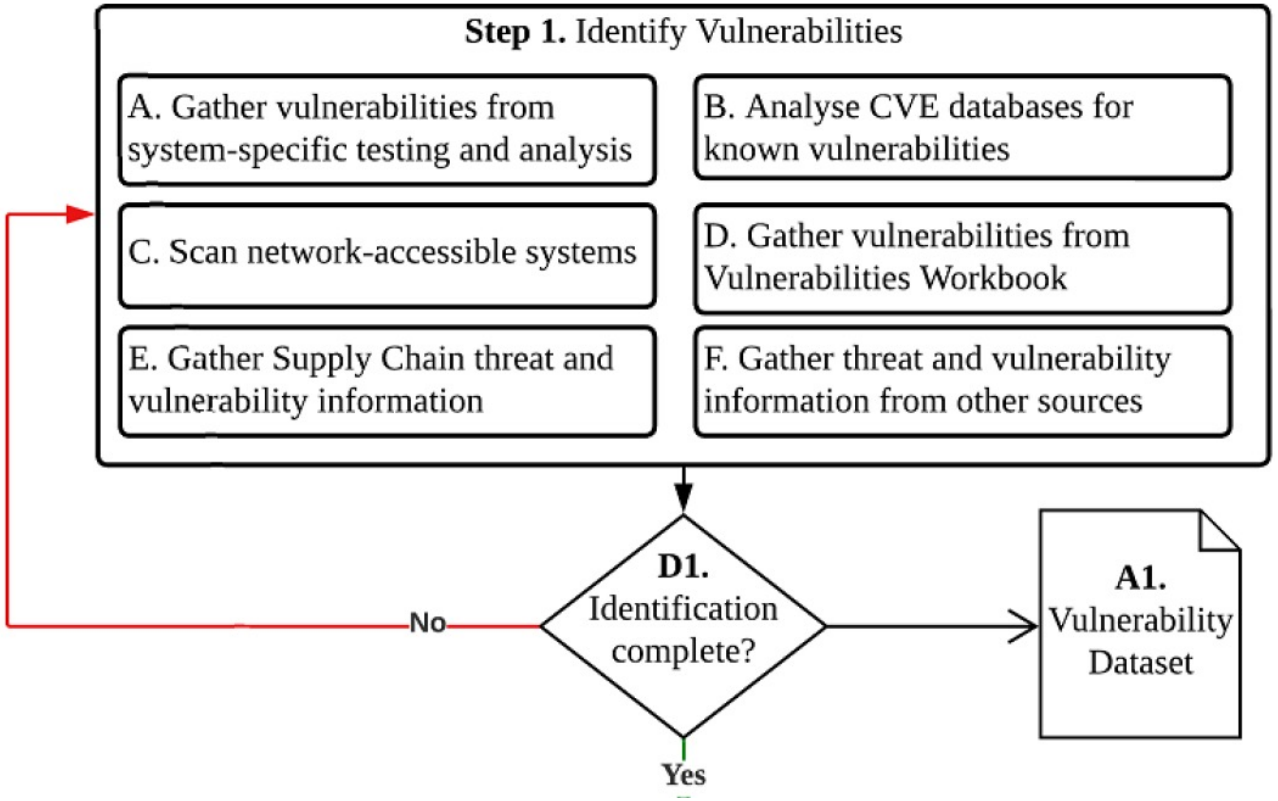
D-RisQ GE Aviation GENERAL DYNAMICS LEONARDO MBDA UNIVERSITY OF OXFORD

RAPITA Rolls-Royce UNIVERSITY OF Southampton THALES Ultra ELECTRONICS CEMS UNIVERSITY of York



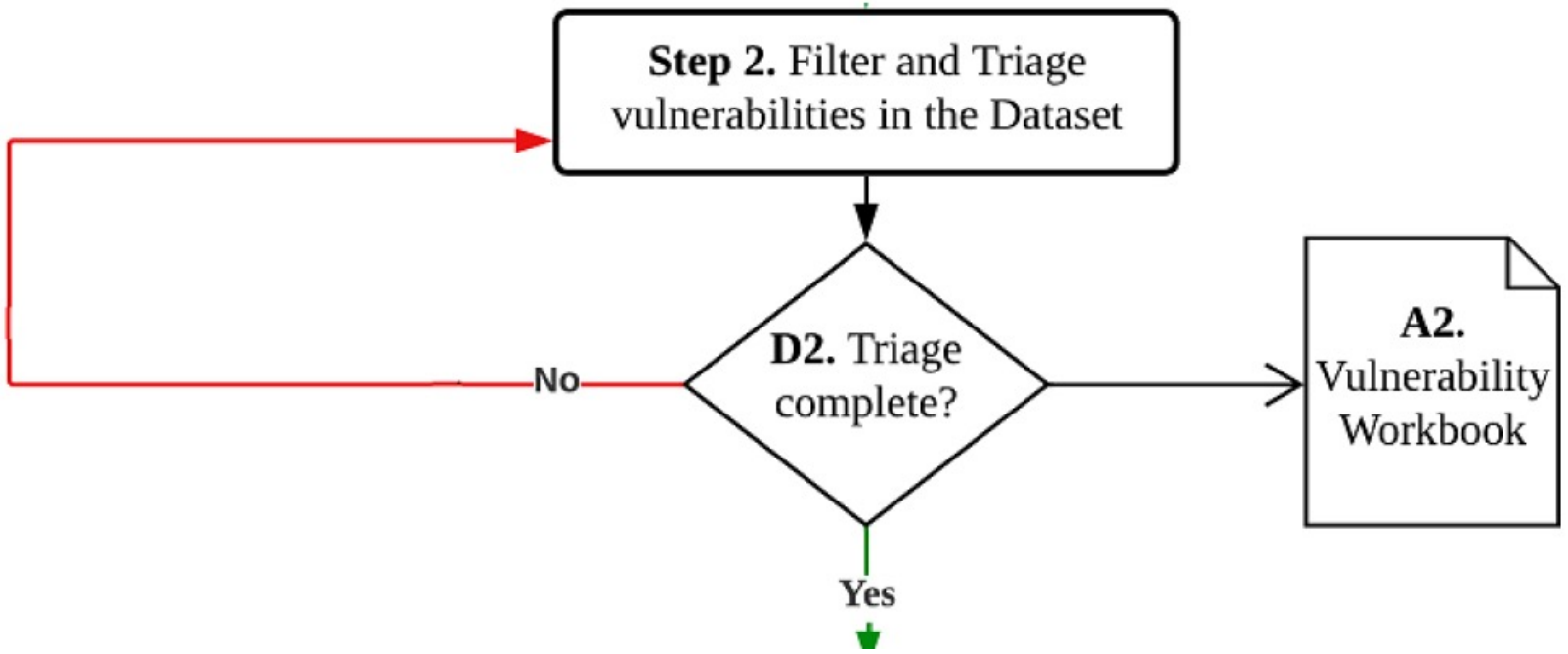
Vulnerability Management

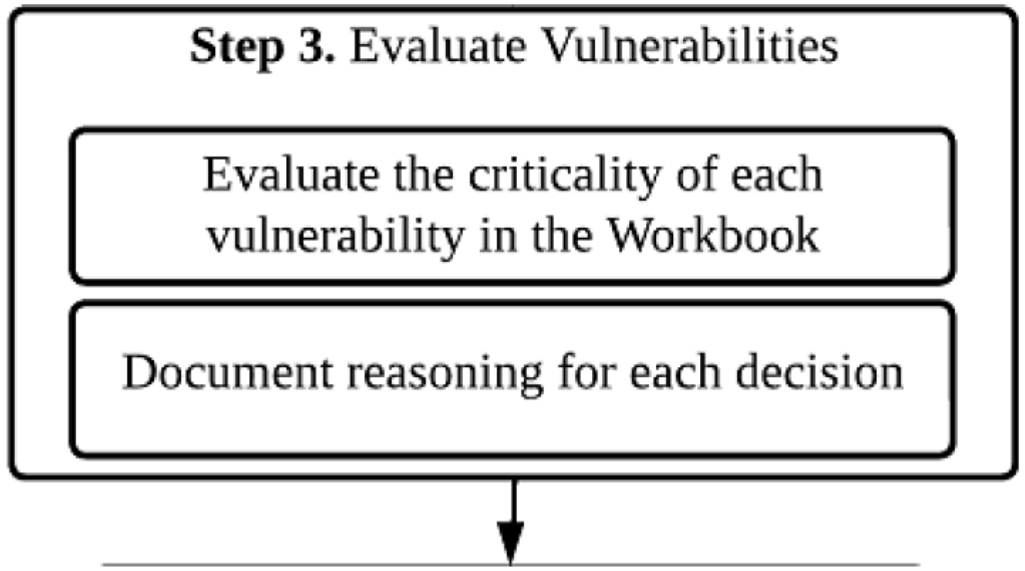
- process to identify weaknesses in the system
- differences to safety risk reduction
- potential for 1000s of vulnerabilities
- identifying change in security risk and security-related system requirements

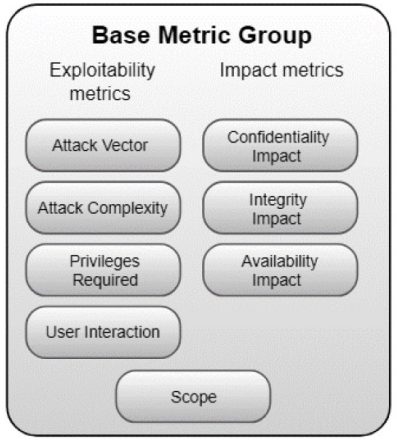


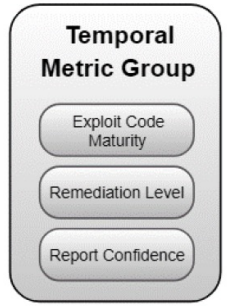
Identify Vulnerabilities

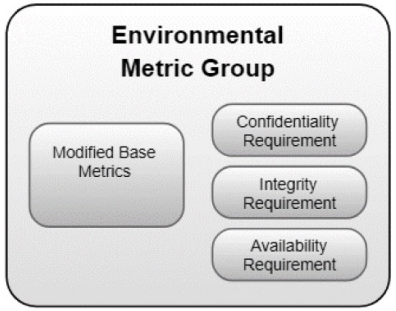
Triage & Filtering

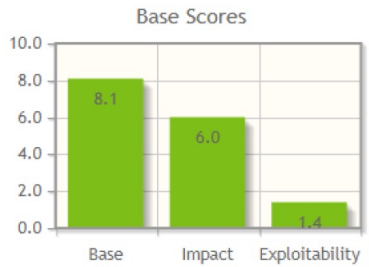


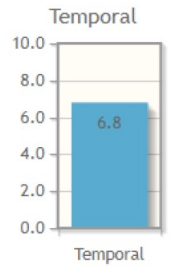


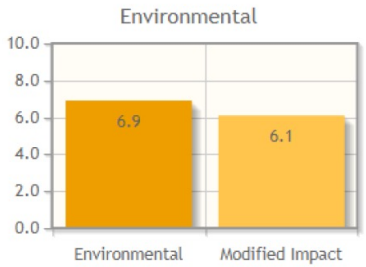


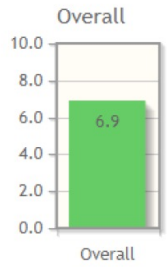






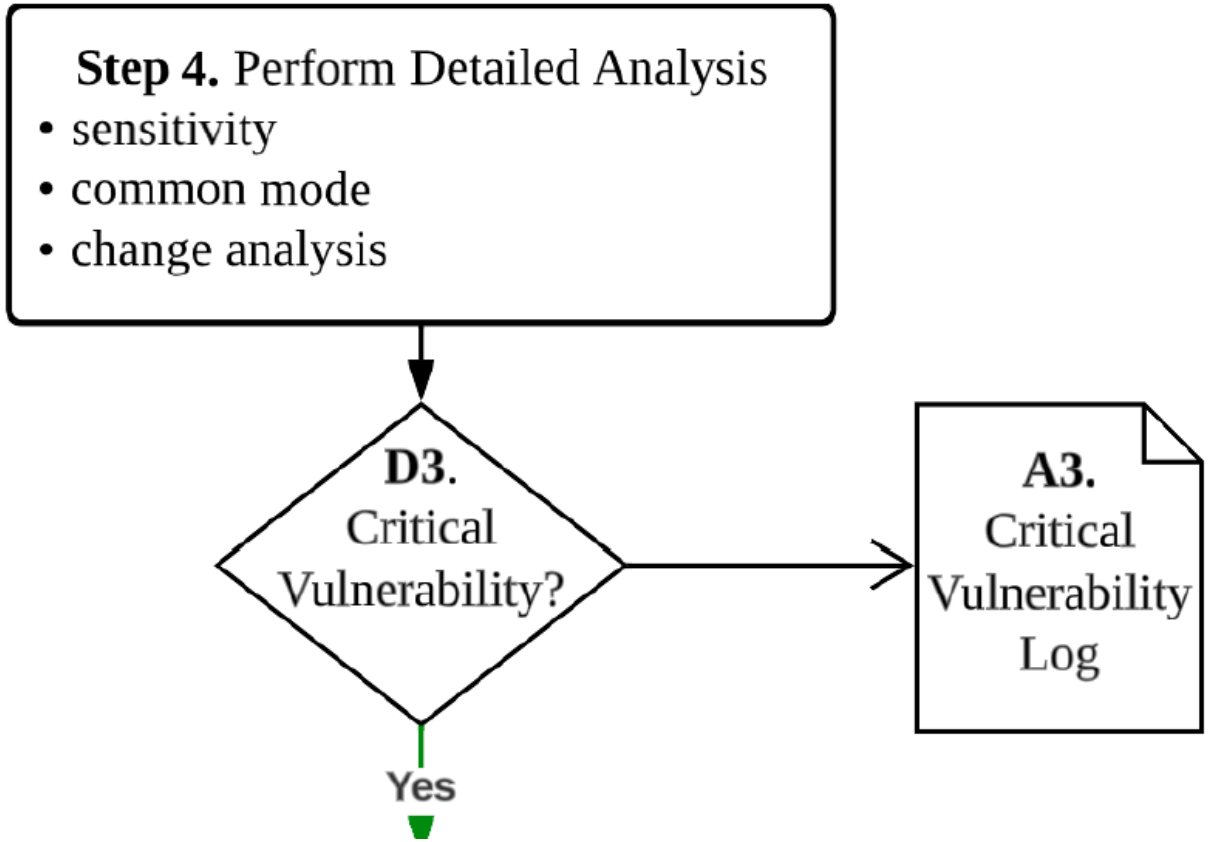




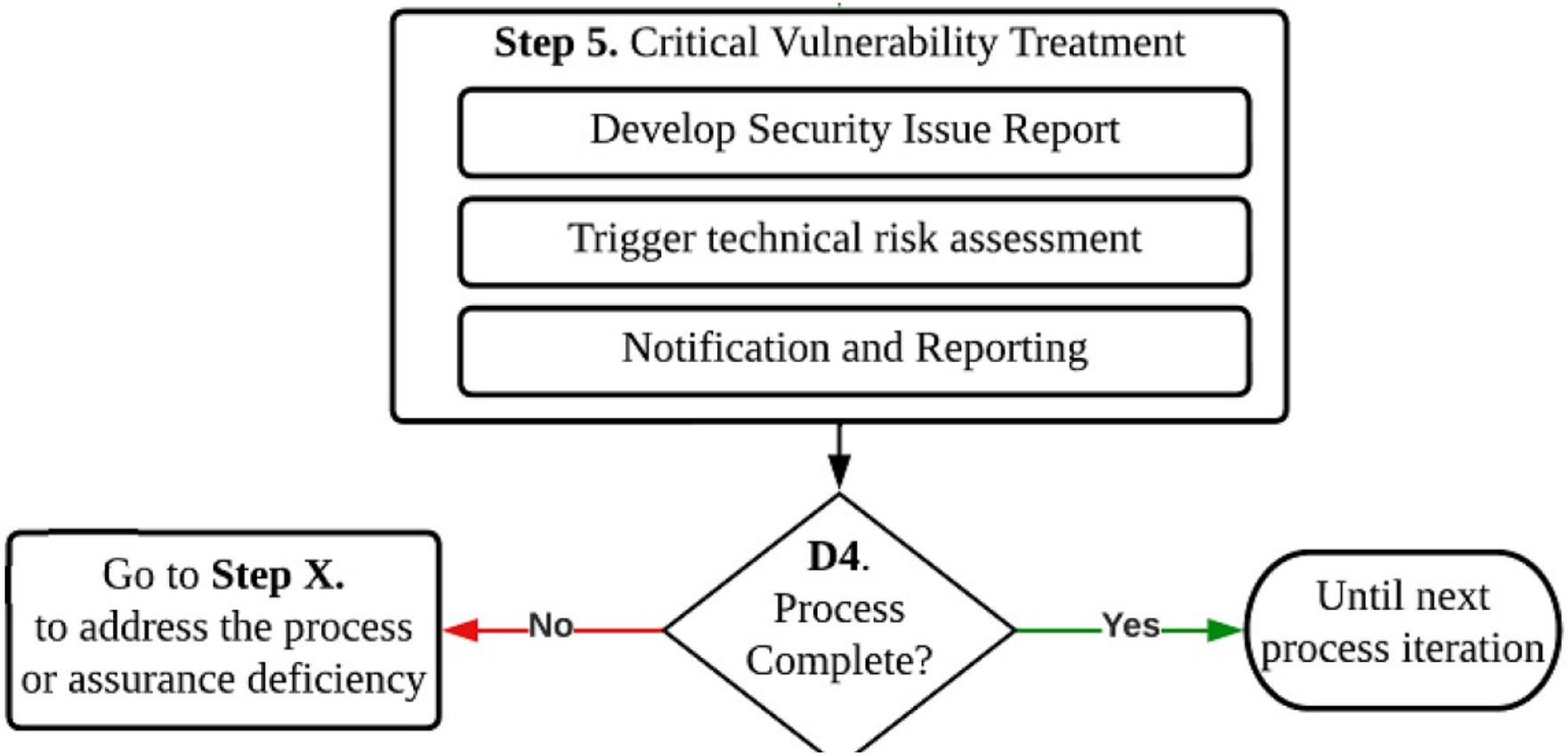


Analysis & Justification

Detailed Analysis

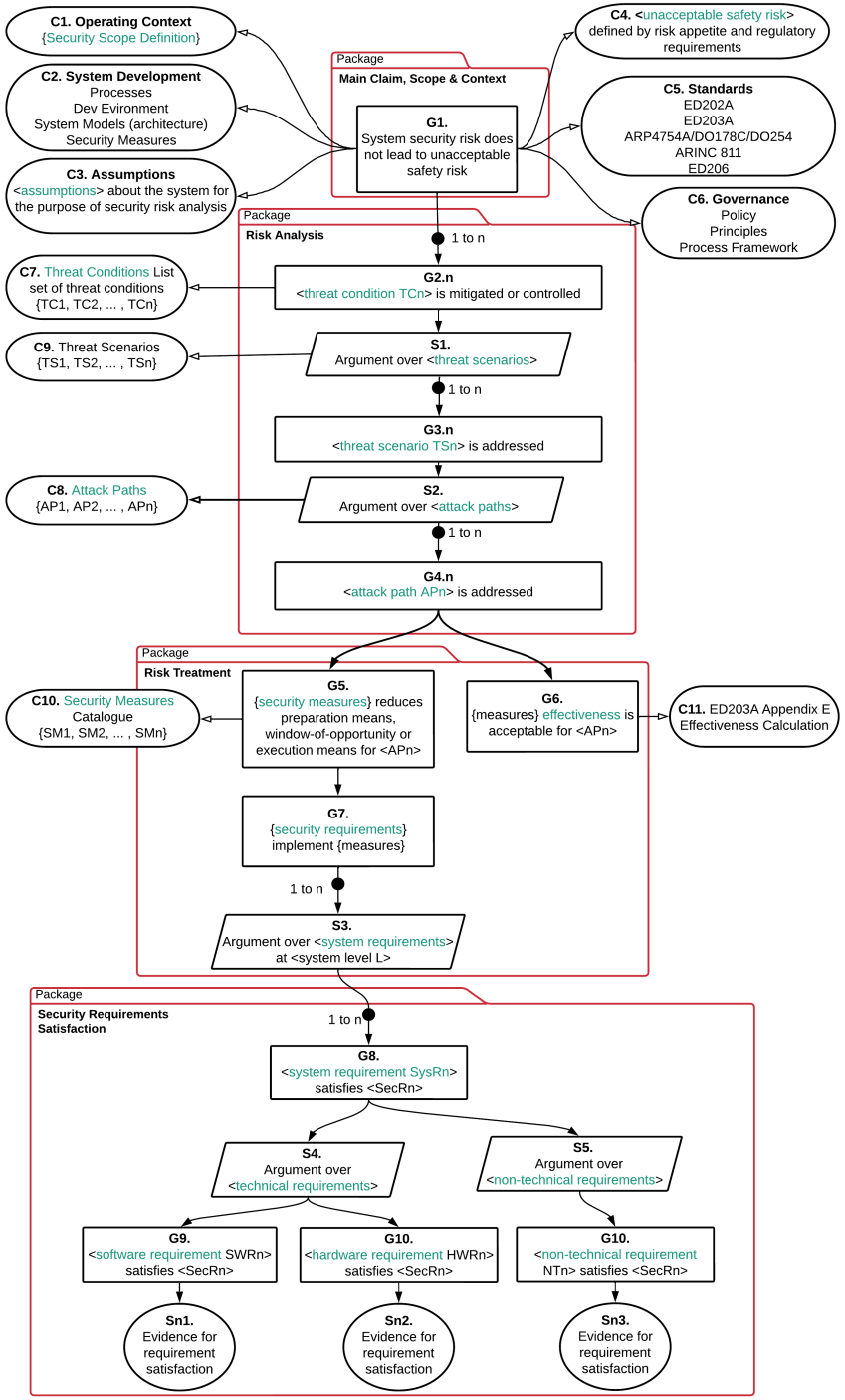


Critical Vulnerability Response



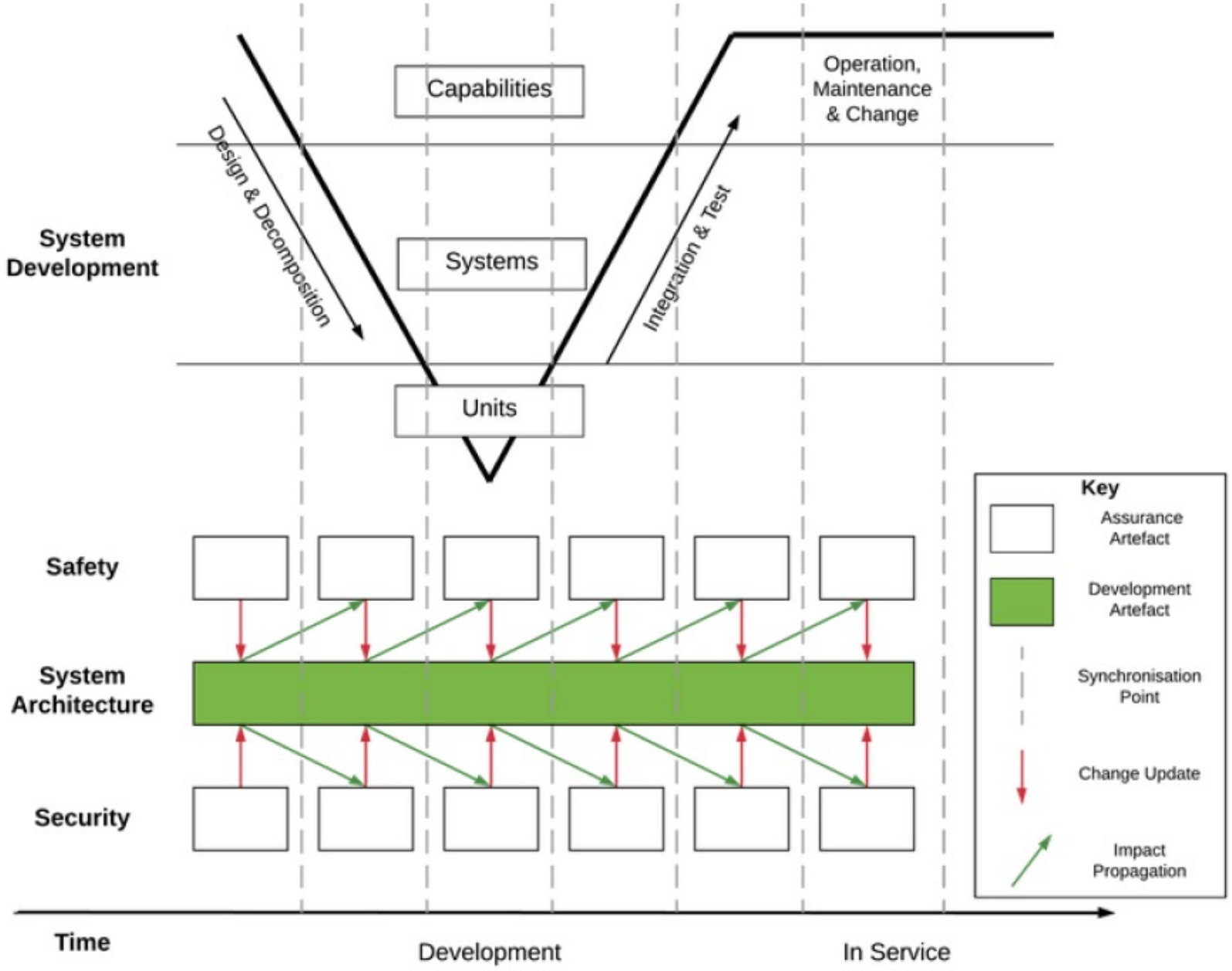
Overview


Fundamentals: Risk, Causal Model, Case
Security Argument Structure
Vulnerability Management
Safety-Security Alignment



Understanding where the Case is undermined

- types of change and impact on argument
- systematic identification and management of uncertainty/change
  - Augmented change processes
  - Pre-analysis and planning
  - Metrics and monitoring
- different to ICS and Enterprise change
  - Tools available
  - Timescales
  - Types of threat



Safety-Security Co-Assurance

- aligning safety and security cases throughout the lifetime of a system

- plan to incorporate changes

- defining monitoring, analysis and response action to foreseeable changes to the security case

Summary

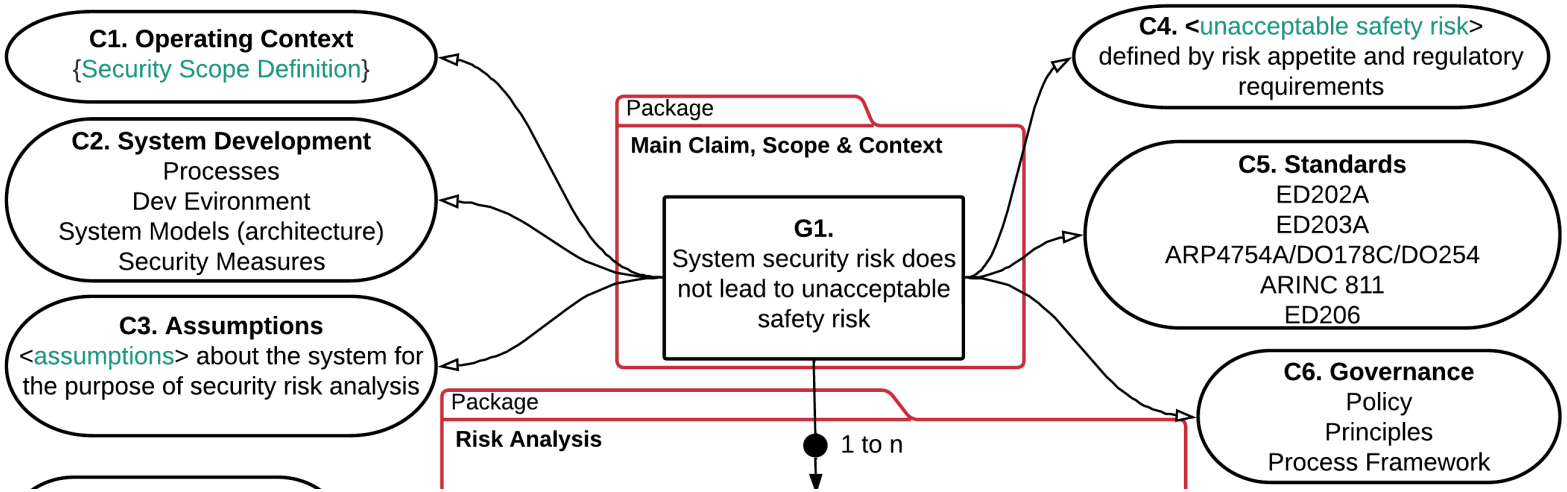
- Fundamentals: Risk, Causal Model, Case
- Security Argument Structure
- Vulnerability Management
- Safety-Security Alignment

Security Case Packages

Security Case: Scope

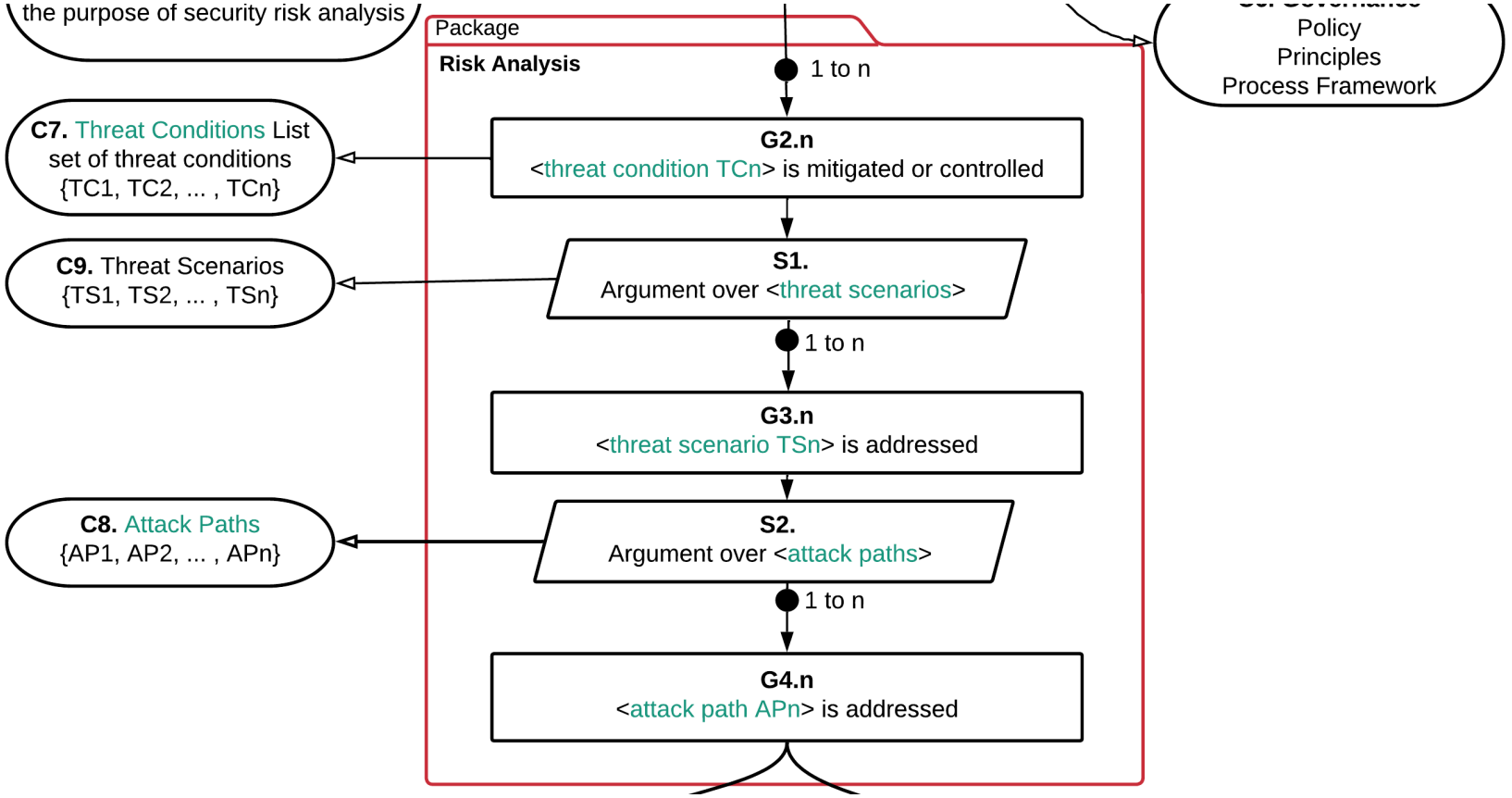
- identify the assets, security perimeter, security environment

- establish risk sharing responsibilities and interfaces



Security Case: Risk

- identification of threat conditions
  - From safety effects
  - Not identified by safety analysis
- threat scenario identification
- identifying security controls
- attack path identification
  - Attack vector
  - Concrete steps
  - Threat actor

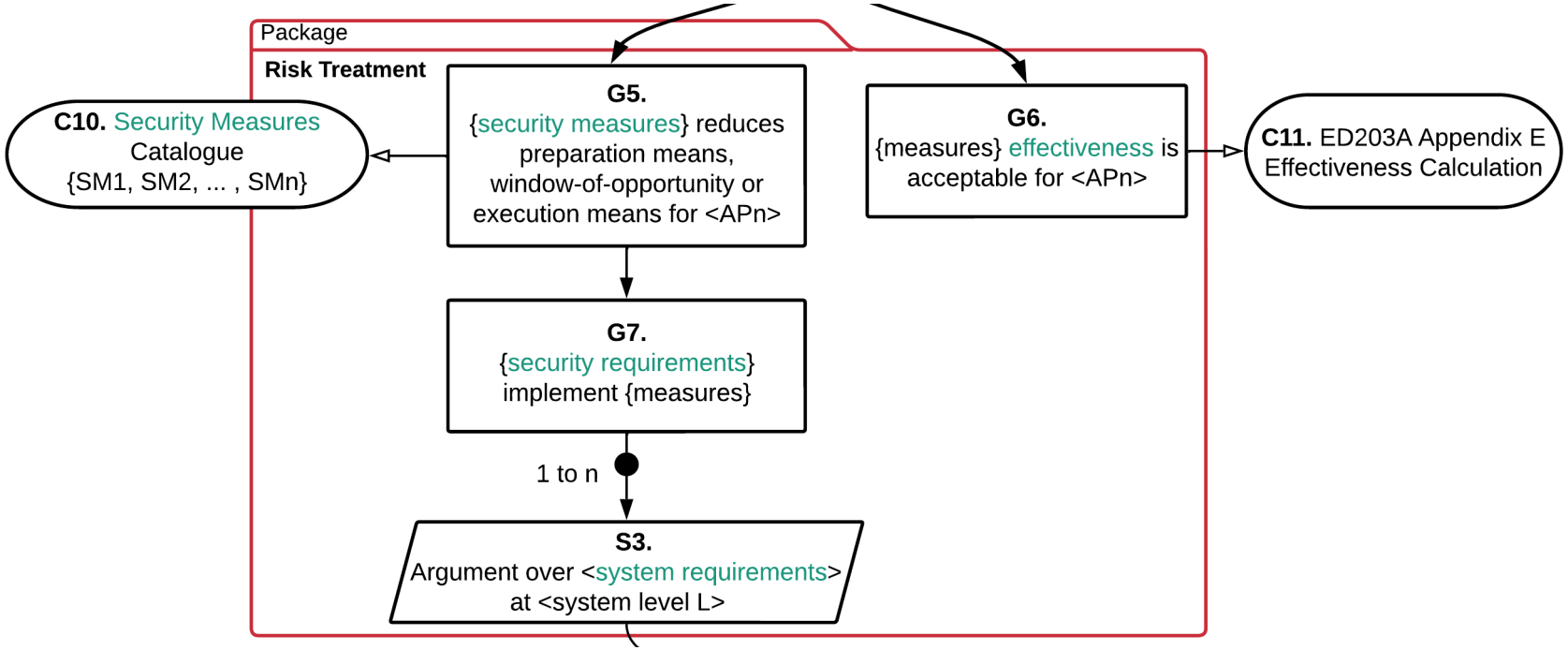


Security Case: Treatment

- security measures from risk assessment

- evaluating the effectiveness of protection
  - Impact from safety
  - Likelihoood: preparation of attack, window-of-opportunity, execution of an attack

- mapping between security measures, security requirements, system requirements



Security Case: Satisfaction

- allocation to software, hardware and procedural

- verification evidence

- test cases from safety

- security refutation

- vulnerability analysis