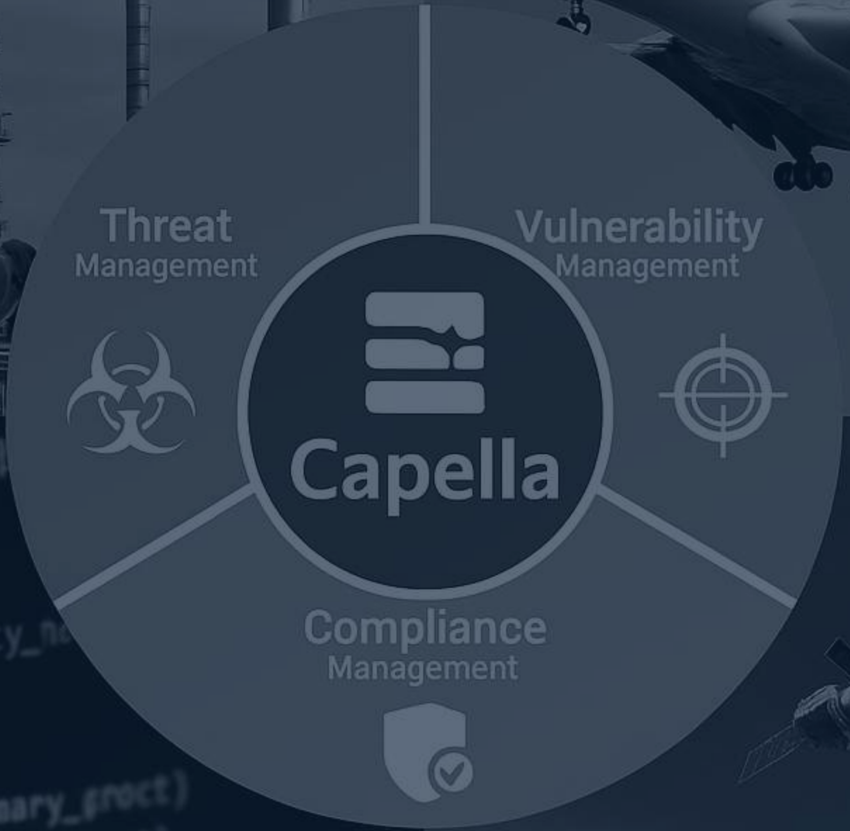
Closing the Loop Between MBSE and Cybersecurity



Threat Management

Vulnerability Management

Compliance Management

Capella

A Vulnerability Analysing Viewpoint for Capella

Integrating runtime cybersecurity concerns into ARCADIA models to enable continuous, model-centric risk control

November 20, 2025

Model-Based Systems Engineering

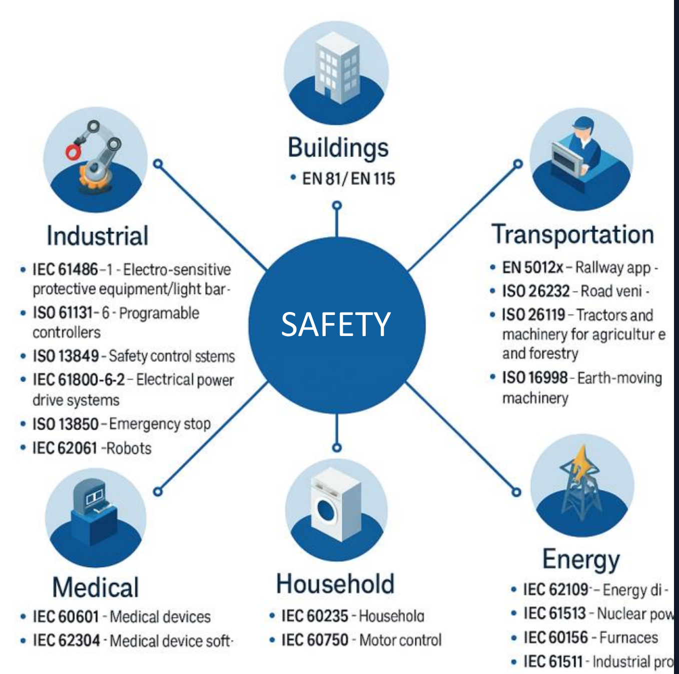
Forough Mokabberi – Jucimar A. Cabral

Functional Safety & Cybersecurity

Functional Safety addresses accidental failures;
Cybersecurity addresses intentional threats.

In Industry:

IEC 61508: Safety Integrity Level
ISO 13849: Performance Level


SAFETY
Buildings
• EN 81/ EN 115
Industrial
• IEC 61486–1 - Electro-sensitive protective equipment/light bar-
• ISO 61131- 6 - Programable controllers
• ISO 13849 - Safety control sstems
• IEC 61800-6-2 – Electrical power drive systems
• ISO 13850 – Emergency stop
• IEC 62061 -Robots
Transportation
• EN 5012x – Rallway app -
• ISO 26232 – Road veni -
• ISO 26119 – Tractors and machinery for agricultur e and forestry
• ISO 16998 - Earth-moving machinery
Medical
• IEC 60601 - Medical devices
• IEC 62304 - Medical device soft-
Household
• IEC 60235 - Househola
• IEC 60750 - Motor control
Energy
• IEC 62109 – Energy di -
• IEC 61513 - Nuclear pow
• IEC 60156 - Furnaces
• IEC 61511 - Industrial pro

⚠ **A cyberattack can trigger a safety hazard**

⚠ **A safety mechanism can be a security attack surface**

Both require:

- **Traceability**
- **Architecture modeling**
- **Defense-in-depth**
- **Verification & validation**
- **Continuous monitoring**

•ISO 26262 (functional safety) + ISO 21434 (cybersecurity)
•IEC 61508 (functional safety) + IEC 62443 (cybersecurity)

Functional Safety & Cybersecurity: MBSE as the Integration Layer

MBSE brings the benefit from its structured, traceable, and architecture-driven approach.

Traceability

High-integrity systems require: Clear traceability from hazards → safety requirements → architecture → implementation → test results.

Architectural Rigor

Define safety functions, safe states, fault tolerance, diagnostic coverage, and redundancy.

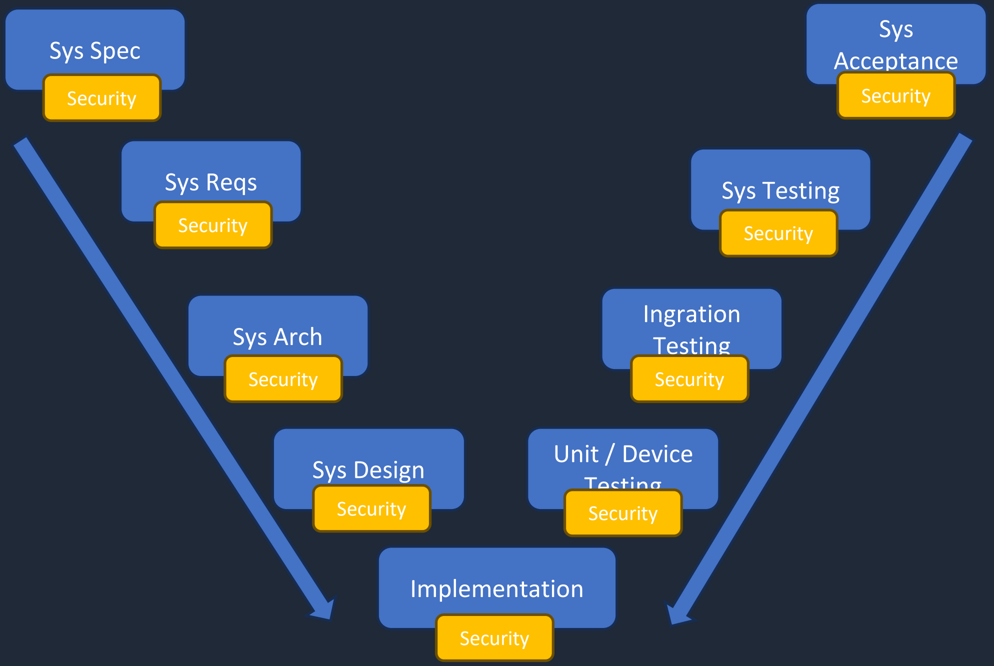
Verification and Validation Alignment

Requirement-based simulation
Allocation-based testing
Automated test generation (model-based testing)

Cyber Threat Analysis

Possible threat and attack surfaces

The Cybersecurity Gap in MBSE



⚠ The V-model is sequential, so once requirements and designs are fixed, it resists changes.

⚠ **Cybersecurity** is often treated as an add-on.

⚠ **Vulnerabilities** are frequently addressed only through remediation efforts.

Integration Challenges

Evolving Threat Landscape

Threats evolve faster

Opaque System Dependencies

Complex interconnections between system components

Delayed Discovery & Patching

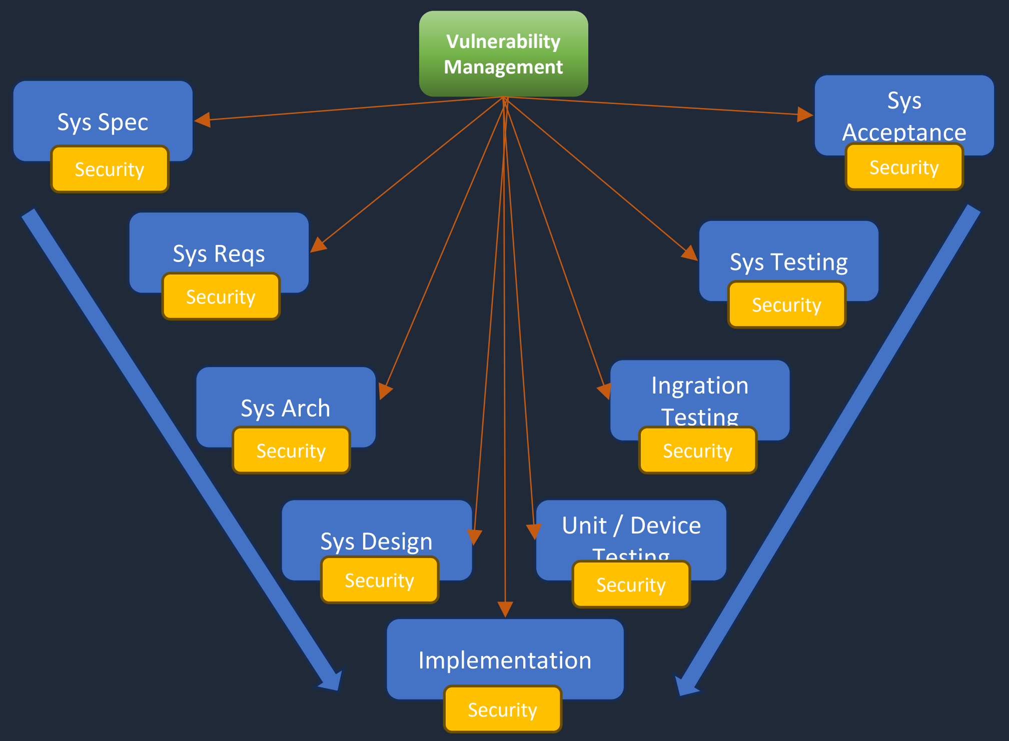
Linear processes delay the identification and remediation

Ineffective Risk Control

Without continuous monitoring and feedback, risk control measures become static and insufficient.

Vulnerability Analyzing Viewpoint (VAV): The Proposed Solution

The Vulnerability Analyzing Viewpoint extends the system model to capture vulnerability propagation, risk relationships, and mitigation strategies across architectural layers.



Bridging MBSE and Cybersecurity

VAV: Integrates runtime cybersecurity concerns directly into the system models.

Key Benefits of VAV

Continuous Risk Control

Enables ongoing security assessment and mitigation.

Model-Centric Approach

Maintains security as an integral part of the system model.

Improved Visibility

Reveals hidden interdependencies and attack paths.

Proactive Security

Shifts security from a reactive to a proactive discipline by identifying.

VAV Meta-Model: Concepts

Vulnerability
Affected Asset
Exploit Path
Risk Assessment
Mitigation
Evidence
Decision

Vulnerability

A weakness or flaw in a system.

Affected Asset

The specific system element (function, component).

Exploit Path

The sequence of steps an attacker follows.

Risk Assessment

Quantifies the potential impact and likelihood .

Mitigation

Actions or controls implemented.

Evidence

Verifiable information supporting the existence of a vulnerability.

Decision

Records choices made regarding vulnerability management.

Integration

These concepts are continuous integrated into ARCADIA model.

What VAV in Capella do?

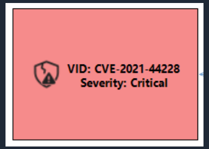
Extends:

Operational → System Need → Logical → Physical viewpoints by focusing on **post-deployment** vulnerability impact analysis.

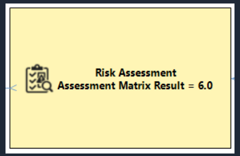
Process

1. Trigger Event: New Vulnerability Identified
2. Risk Analysis Integration
3. Mitigations analyses
3. Trace the vulnerability across Capella

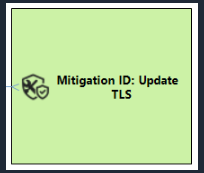
VAV Elements in Capella



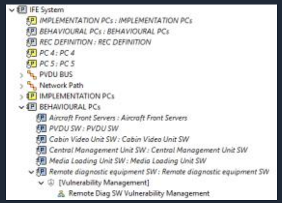
NVD database, vendor advisory, incident detection



Assess likelihood & impact using standard frameworks (ISO 21434, IEC 62443, DO-356A, NIST RMF).



Candidate mitigations



```
IFE System
  IMPLEMENTATION PCs : IMPLEMENTATION PCs
  BEHAVIOURAL PCs : BEHAVIOURAL PCs
  REC DEFINITION : REC DEFINITION
  PC 4 : PC 4
  PC 5 : PC 5
  PVDU BUS
  Network Path
  IMPLEMENTATION PCs
  BEHAVIOURAL PCs
    Aircraft Front Servers : Aircraft Front Servers
    PVDU SW : PVDU SW
    Cabin Video Unit SW : Cabin Video Unit SW
    Central Management Unit SW : Central Management Unit SW
    Media Loading Unit SW : Media Loading Unit SW
    Remote diagnostic equipment SW : Remote diagnostic equipment SW
      [Vulnerability Management]
        Remote Diag SW Vulnerability Management
```

Traceability

What VAV in Capella do?

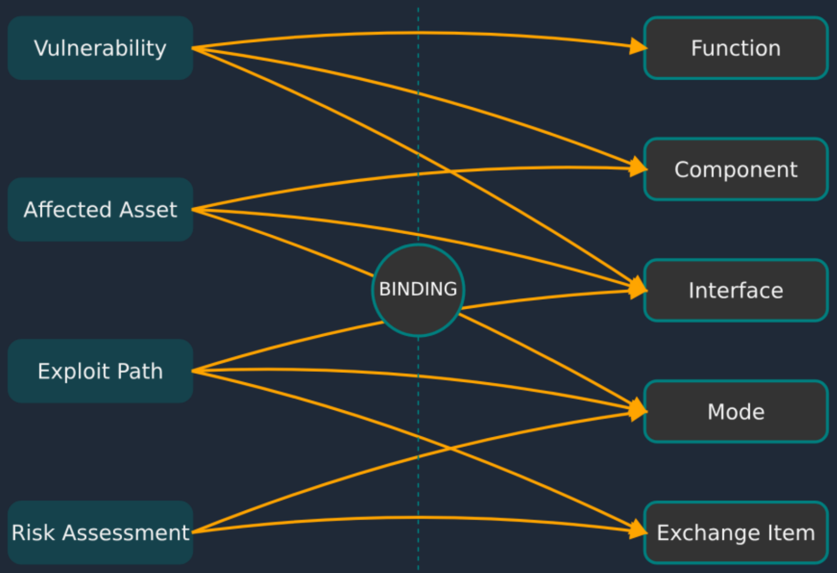
What is Binding?

VAV concepts are continuously integrated by binding them to existing Capella elements.

Key Benefits

- ✓ Model-centric approach to vulnerability analysis
- ✓ Direct linkage between security and architecture
- ✓ Continuous security feedback loop

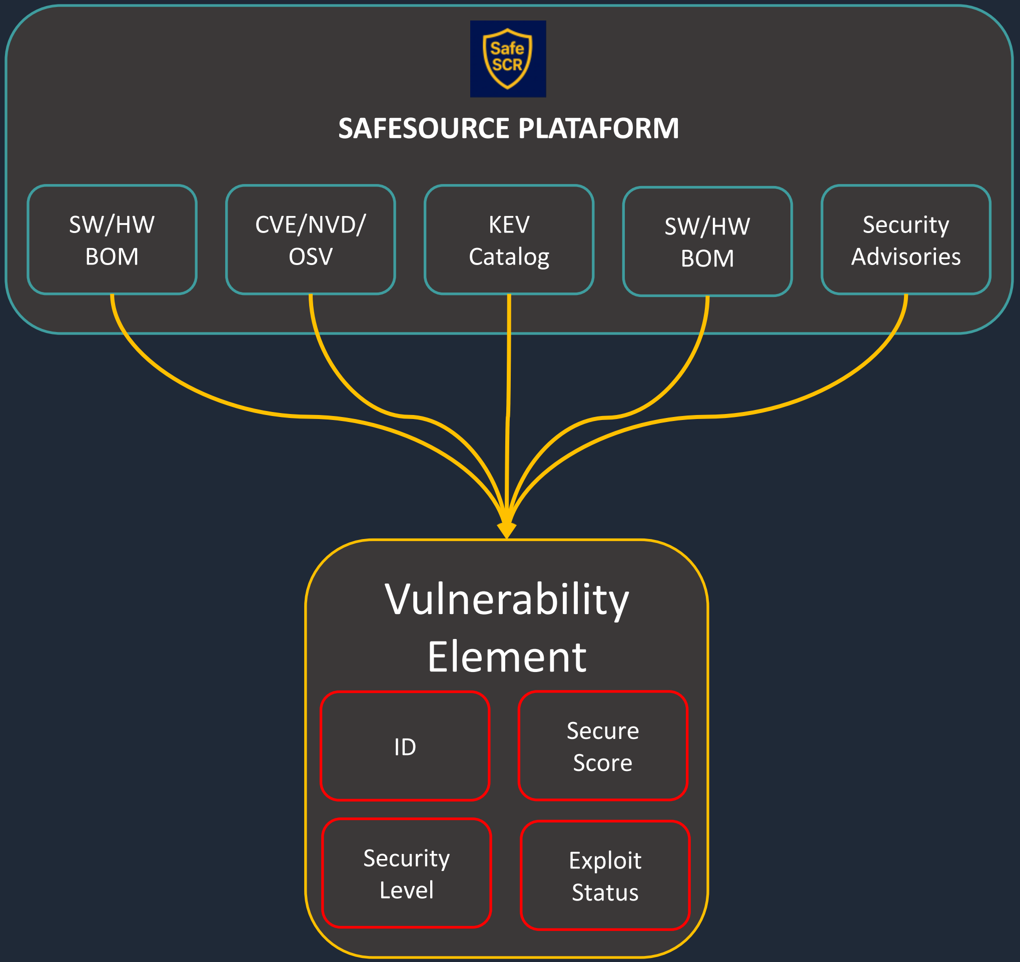
VAV to Capella Element Binding



🟩 VAV Concept □ Capella Element ^ Binding

External Vulnerability Data Integration

Integration Process



External Data Sources

Software/Hardware Bill of Materials (SBOM - HBOM)

Complete list of components, libraries, and dependencies used in a SW/HW system.

CVE/NVD/OSV

Standardized identifiers and detailed information.

Known Exploited Vulnerabilities (KEV) Catalog

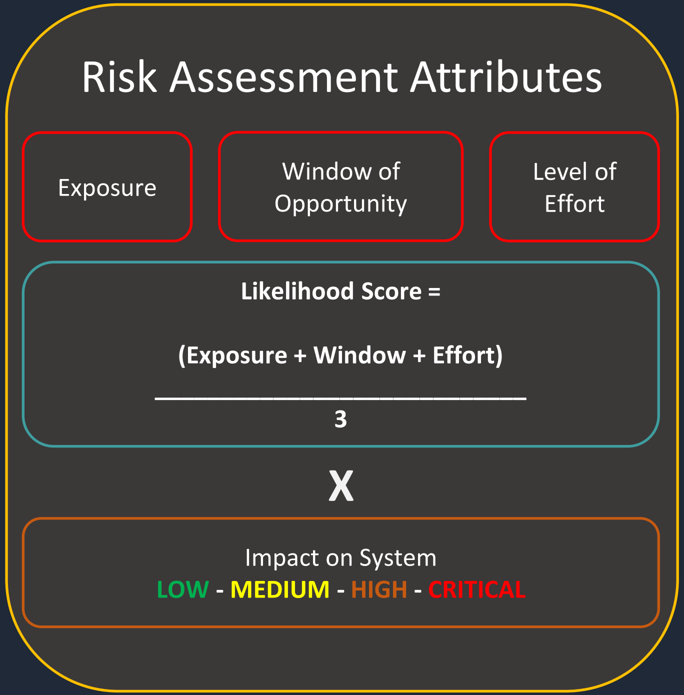
CISA-maintained catalog listing vulnerabilities that have been actively exploited.

Security Advisories

Official notifications from vendors, security researchers, or government agencies.

Risk Assessment Matrix

Dynamic Risk Matrix



Risk Assessment Attributes

Exposure

Window of Opportunity

Level of Effort

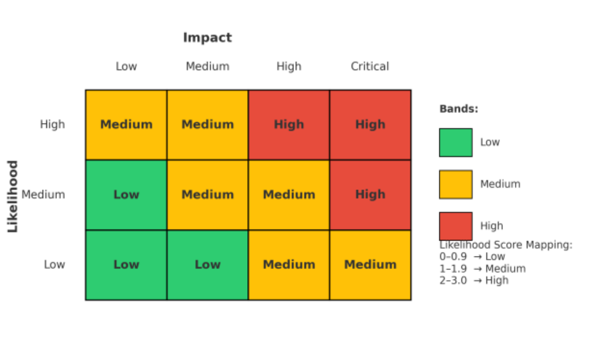
Likelihood Score =

$$\frac{\textbf{(Exposure + Window + Effort)}}{\textbf{3}}$$

X

Impact on System

LOW - **MEDIUM** - **HIGH** - **CRITICAL**



		Impact			
		Low	Medium	High	Critical
Likelihood	High	Medium	Medium	High	High
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	Medium

Bands:

🟩 Low

🟨 Medium

🟥 High

Likelihood Score Mapping:
0–0.9 → Low
1–1.9 → Medium
2–3.0 → High

Risk Assessment Approach

Exposure

Measures how much of the system or asset is exposed to a potential threat.

Window of Opportunity

Represents the time an attacker has to exploit the vulnerability.

Level of Effort

Reflects how difficult it is for an attacker to exploit the vulnerability.

Likelihood Score

Provides an averaged measure of how likely a vulnerability is to be exploited.

Impact on System

LOW: Minimal operational or data impact.

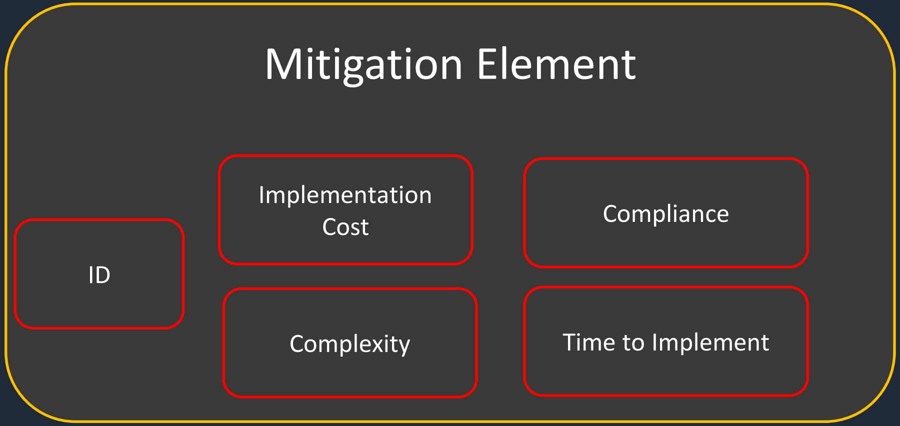
MEDIUM: Noticeable but contained system degradation.

HIGH: Major system compromise or operational failure.

CRITICAL: Catastrophic impact — safety, mission, or compliance failure.

Mitigation

Each element provides a dimension for assessing and prioritizing mitigation strategies.



Mitigation Approach

Implementation Cost

The estimated financial or resource expense to apply the mitigation.

Time to Implement

Estimated duration required to plan, develop, verify, and deploy the mitigation.

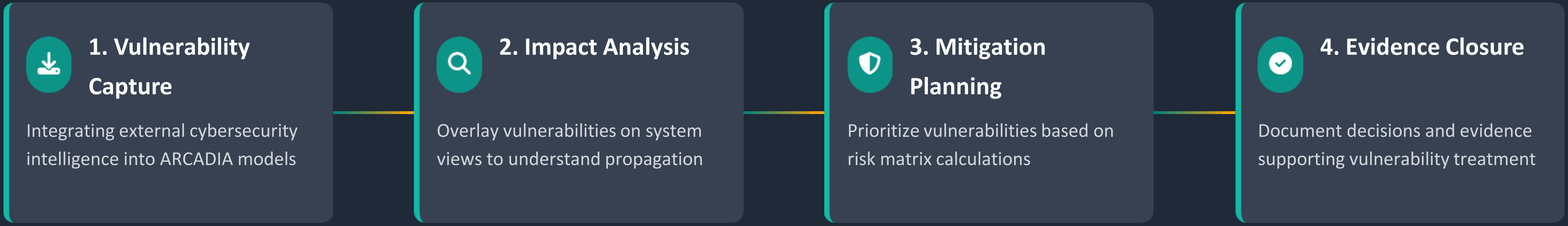
Complexity

The level of technical difficulty in implementing the mitigation.

Compliance

Degree to which the mitigation supports regulatory, safety, or cybersecurity standards.

VAV Workflow Overview



1. Vulnerability Capture

Integrating external cybersecurity intelligence into ARCADIA models

2. Impact Analysis

Overlay vulnerabilities on system views to understand propagation

3. Mitigation Planning

Prioritize vulnerabilities based on risk matrix calculations

4. Evidence Closure

Document decisions and evidence supporting vulnerability treatment

External Data Sources

- Software Bill of Materials (SBOM) Hardware Bill of Materials (HBOM)
- CVE/NVD/OSV Databases
- Known Exploited Vulnerabilities (KEV)
- Security Advisories

Analysis Techniques

- Impact Overlay on logical, physical views
- Attack-Path Overlay traversal
- Exploit path visualization
- Subsystem propagation analysis

Risk Management

- Dynamic risk matrix computation
- Likelihood and consequence calculation
- Risk-based prioritization
- Mitigation strategy development

Documentation

- Evidence collection and verification
- Decision recording framework
- Audit trail maintenance
- Remediation verification

Supervisory Control and Data Acquisition (SCADA) Case Study: Introduction

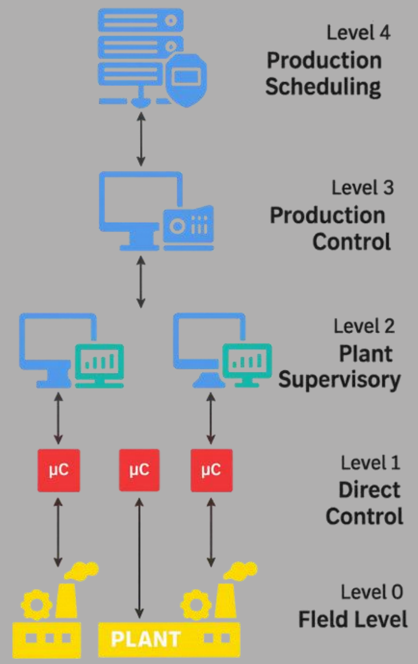
Case Study Overview

Real-World Validation

Validation Purpose

Methodology

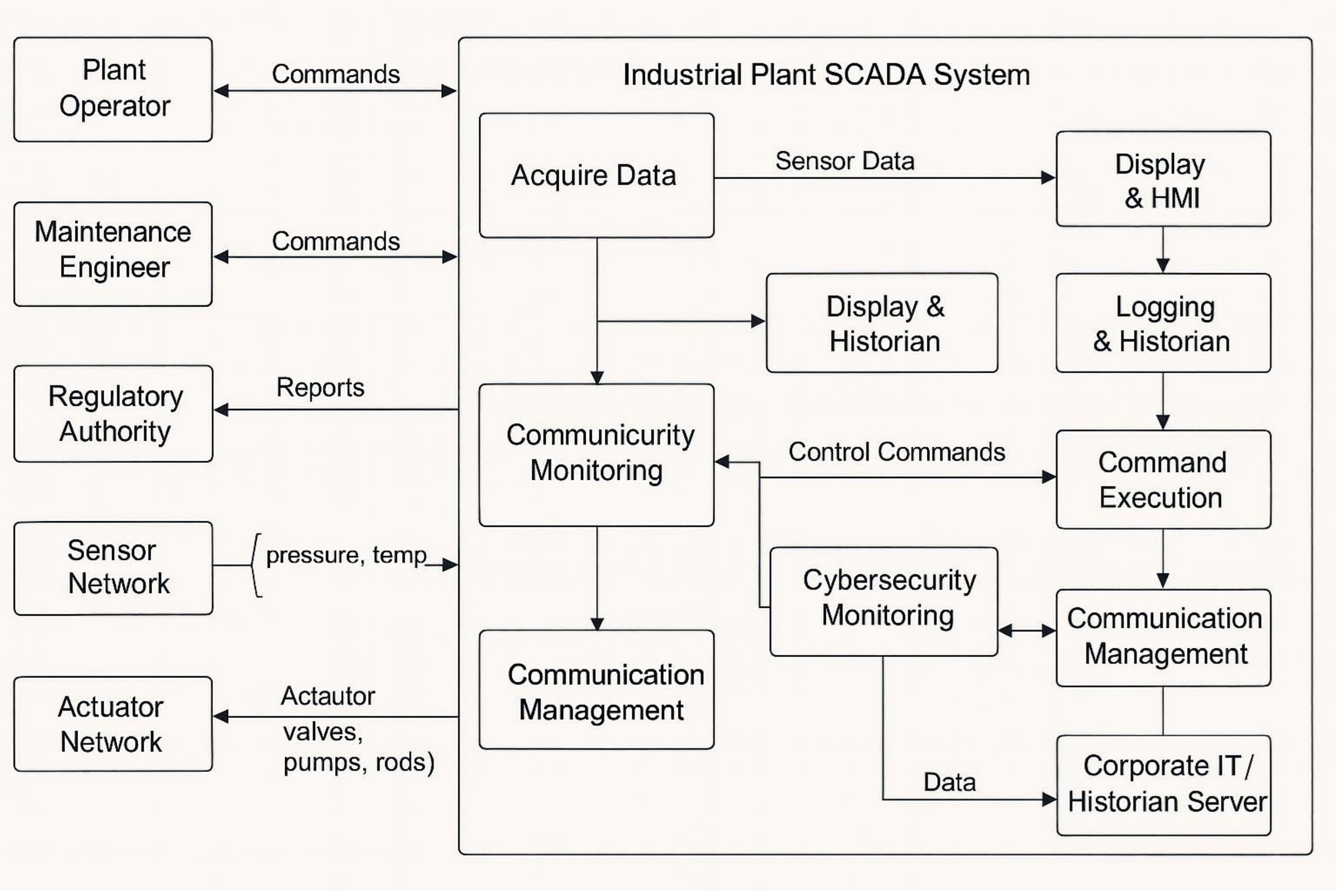
Industrial Control System



Key Components: The industrial control system consists of multiple interconnected subsystems, highlighting the complexity of modern operational environments.

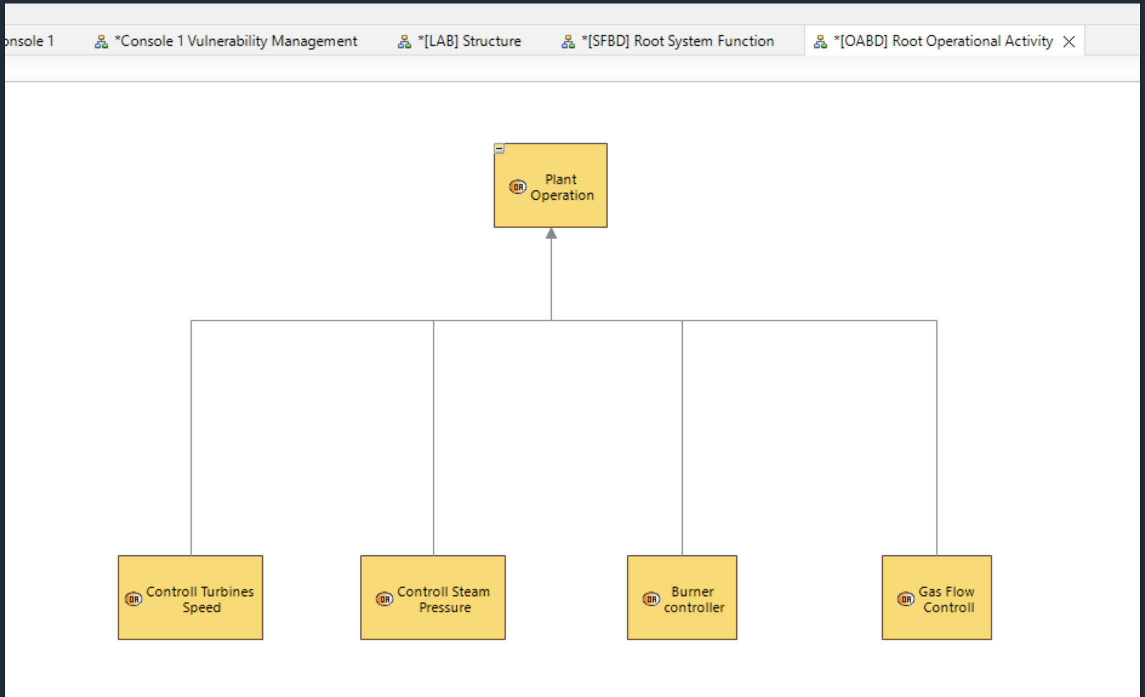
SCADA in Industrial Plant

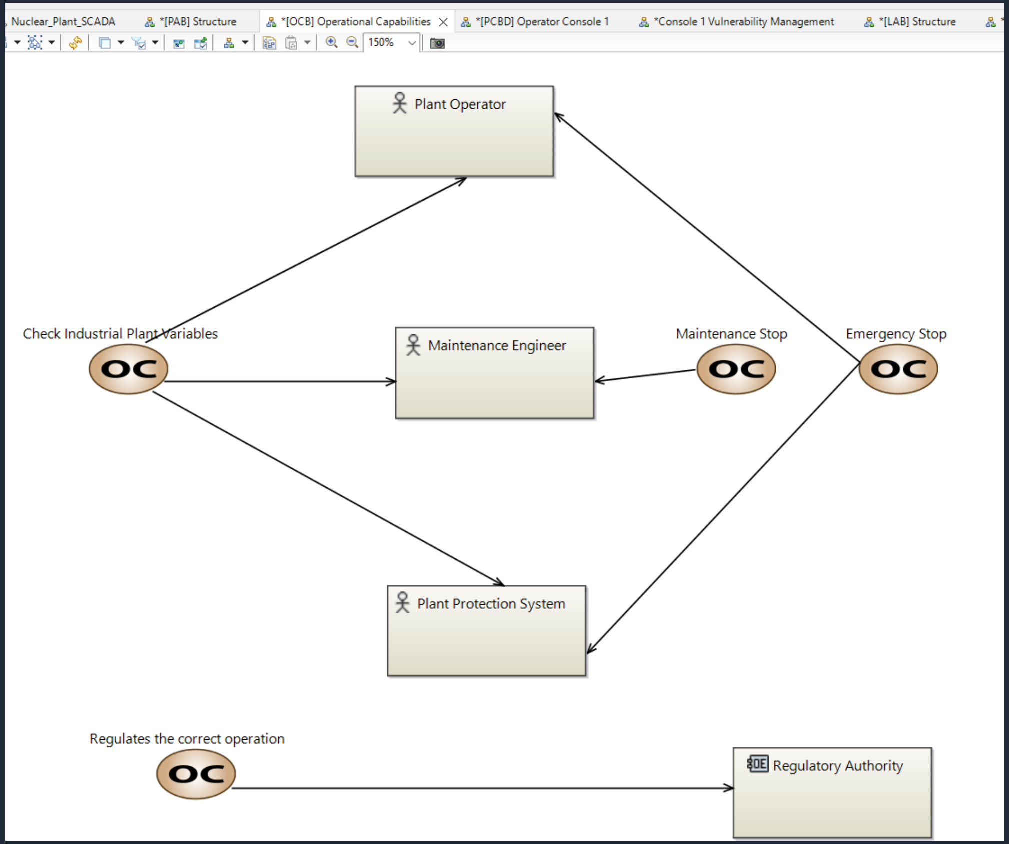
Idustrial plant SCADA systems are **Supervisory Control and Data Acquisition platforms** designed to **monitor, analyze, and control critical processes** within an industrial plant — covering everything from **environmental monitoring** to **industrial operations**.



Industrial Plant Model in Capella

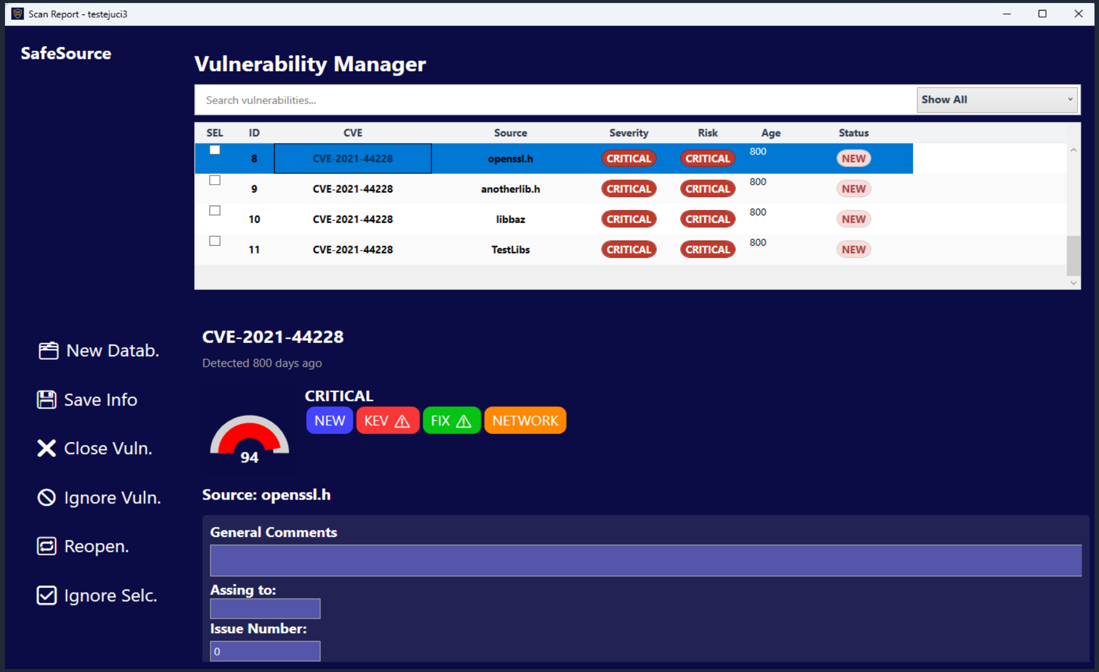
Operational Analysis





Trigger Event: New Vulnerability Identified in Operator Console SW

An attacker can execute arbitrary code loaded from servers through the log messages or log message parameters in Apache Logging Services



Vulnerability Manager

SEL	ID	CVE	Source	Severity	Risk	Age	Status
□	8	CVE-2021-44228	openssl.h	CRITICAL	CRITICAL	800	NEW
□	9	CVE-2021-44228	anotherlib.h	CRITICAL	CRITICAL	800	NEW
□	10	CVE-2021-44228	libbaz	CRITICAL	CRITICAL	800	NEW
□	11	CVE-2021-44228	TestLibs	CRITICAL	CRITICAL	800	NEW

CVE-2021-44228

Detected 800 days ago

CRITICAL

Source: openssl.h

General Comments:

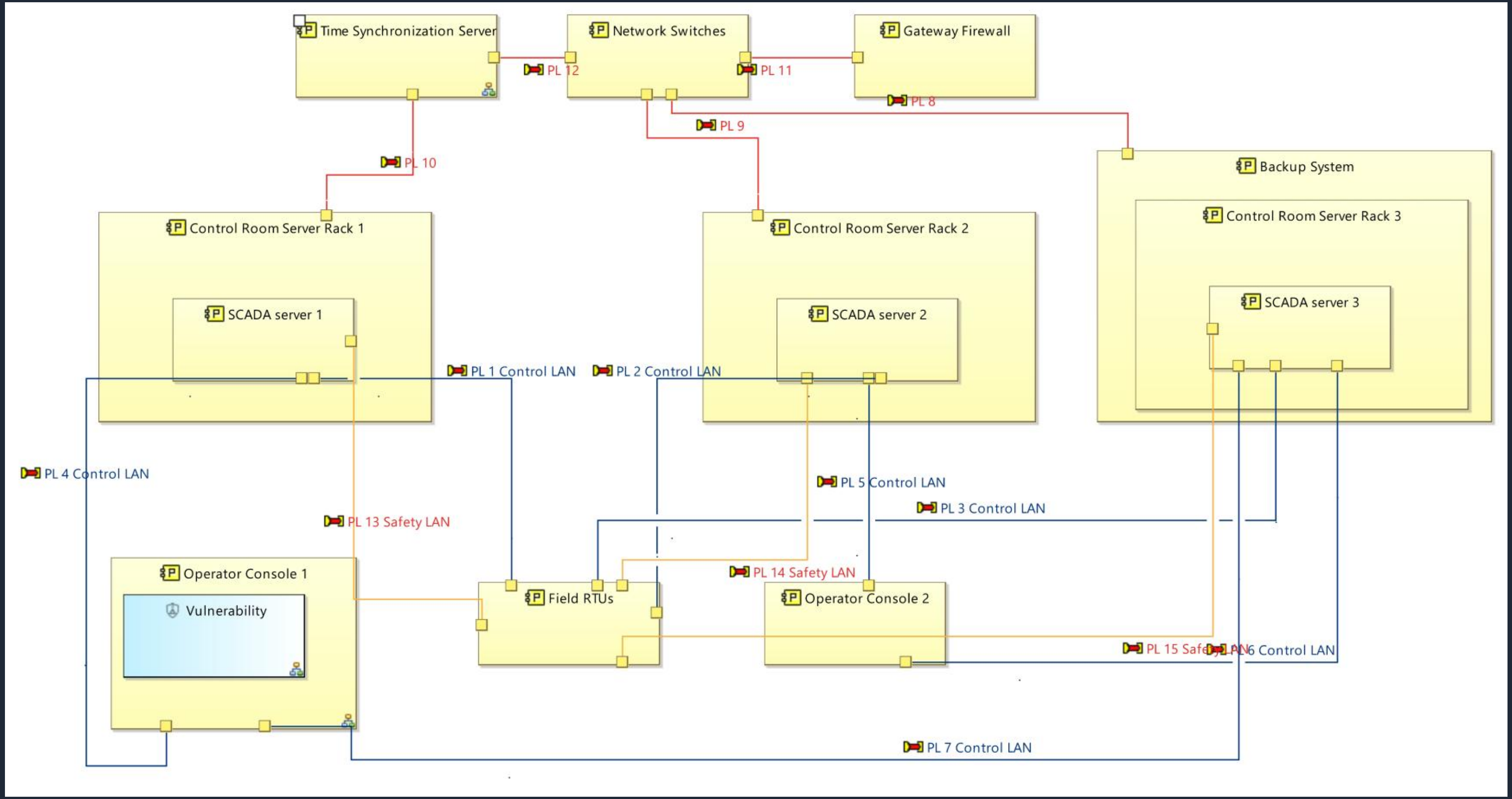
Assing to:

Issue Number: 0

Vulnerability loaded in the System

Physical Architecture

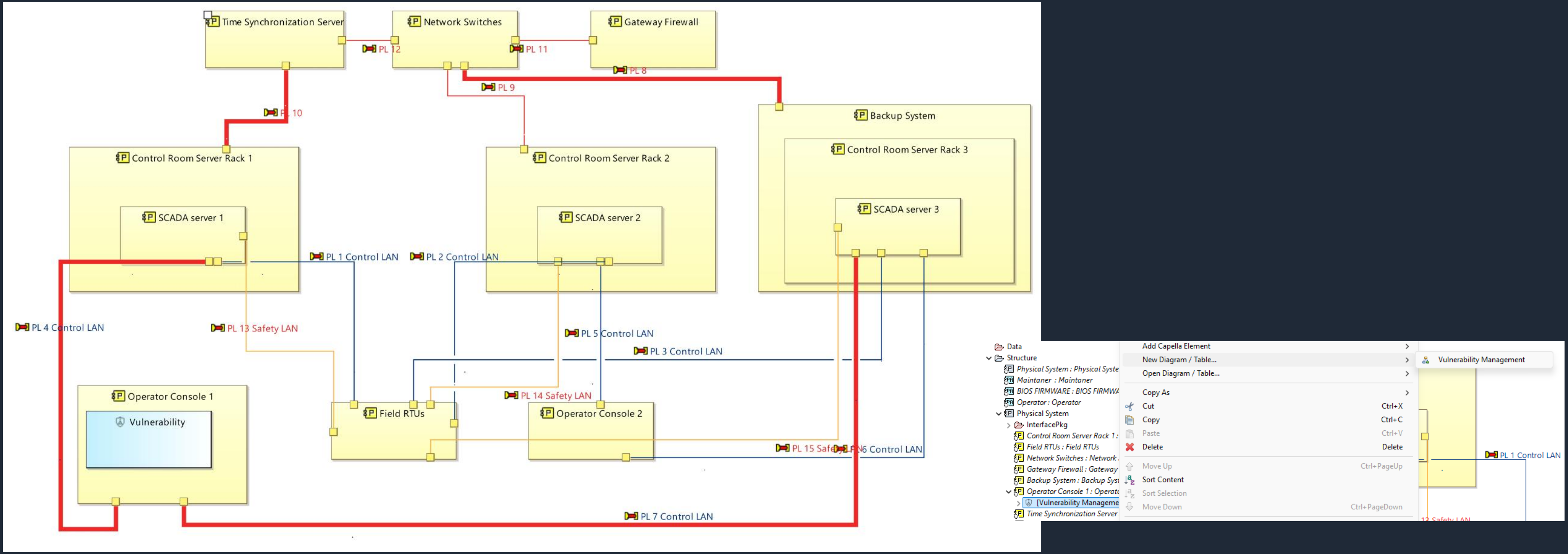
Operator Console Vulnerability inserted to trigger the process of assessment



Vulnerability Path Propagation

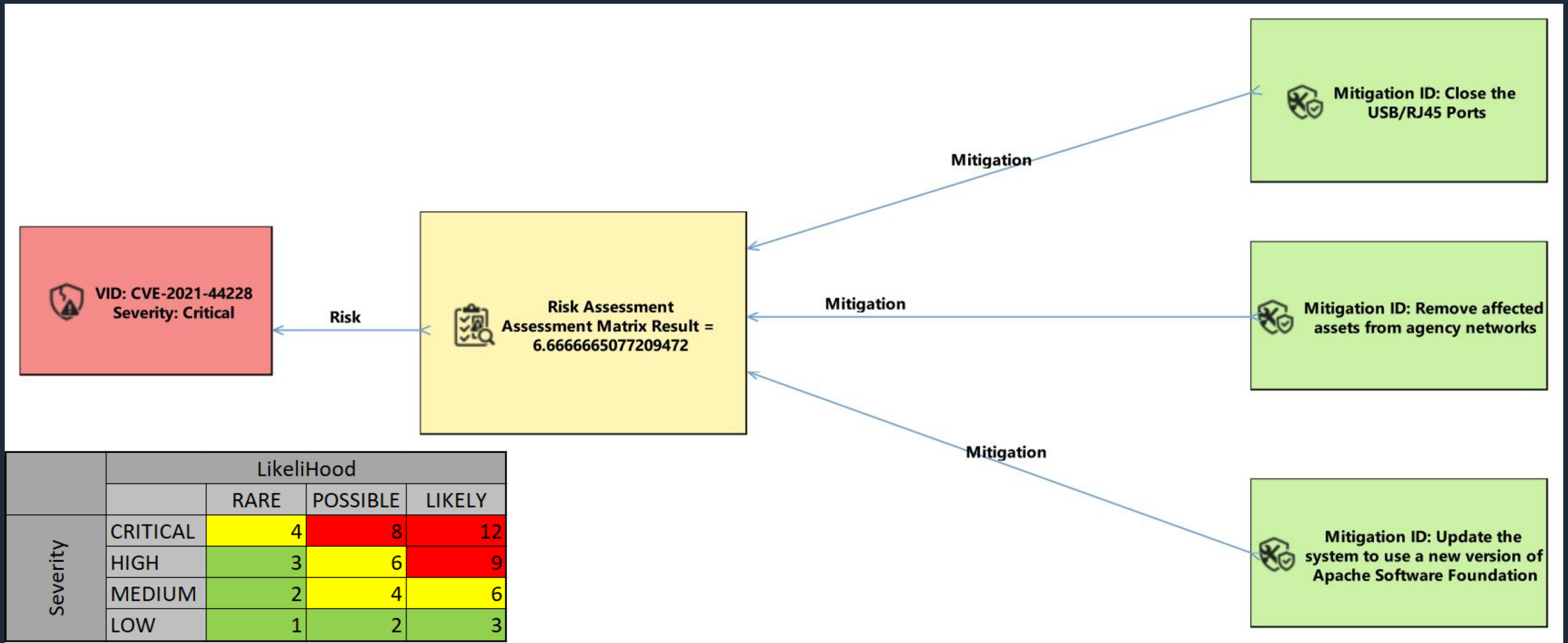
Vulnerability –> SCADA Server –> Time Sync Server –> Network Switch

The same is applied to the Operator Console 2



Cybersecurity Vulnerability Analysis

- Vulnerability Management (VM) diagram
- Vulnerability Element (Node)
- Risk Assessment (Node)
- Possible Mitigations (Node)



VID: CVE-2021-44228
Severity: Critical

Risk

Risk Assessment
Assessment Matrix Result =
6.6666665077209472

Mitigation

Mitigation ID: Close the USB/RJ45 Ports

Mitigation

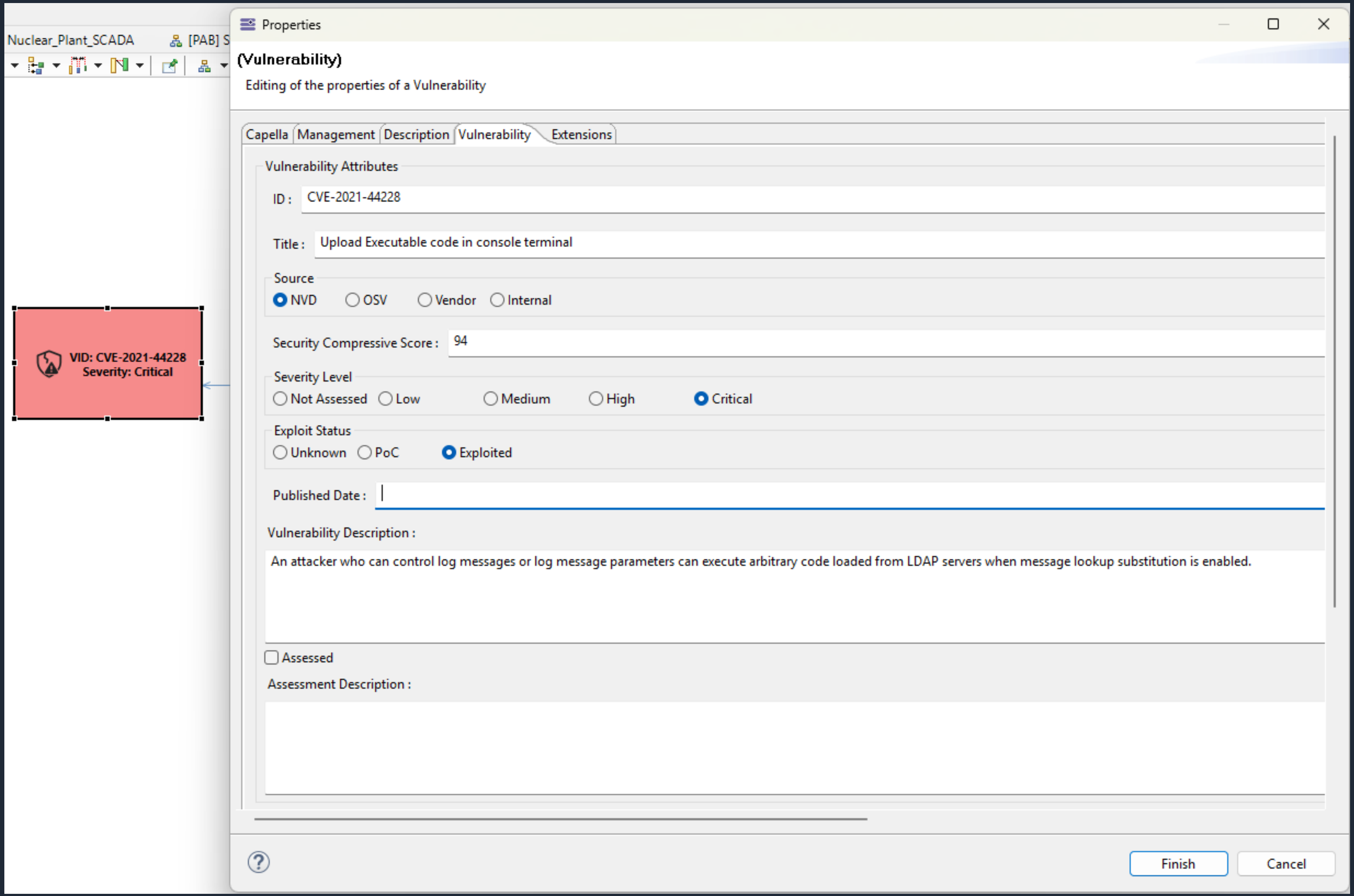
Mitigation ID: Remove affected assets from agency networks

Mitigation

Mitigation ID: Update the system to use a new version of Apache Software Foundation

		LikeliHood		
		RARE	POSSIBLE	LIKELY
Severity	CRITICAL	4	8	12
	HIGH	3	6	9
	MEDIUM	2	4	6
	LOW	1	2	3

Vulnerability Node



(Vulnerability)

Editing of the properties of a Vulnerability

Vulnerability Attributes

ID : CVE-2021-44228

Title : Upload Executable code in console terminal

Source

● NVD ○ OSV ○ Vendor ○ Internal

Security Compressive Score : 94

Severity Level

○ Not Assessed ○ Low ○ Medium ○ High ● Critical

Exploit Status

○ Unknown ○ PoC ● Exploited

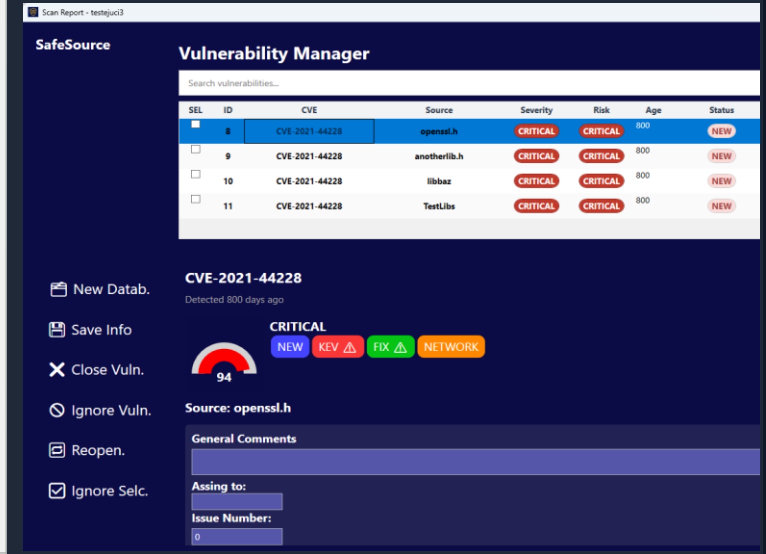
Published Date :

Vulnerability Description :

An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

□ Assessed

Assessment Description :



Vulnerability Manager

SEL	ID	CVE	Source	Severity	Risk	Age	Status
□	8	CVE-2021-44228	openssl.h	CRITICAL	CRITICAL	800	NEW
□	9	CVE-2021-44228	anotherlib.h	CRITICAL	CRITICAL	800	NEW
□	10	CVE-2021-44228	libbaz	CRITICAL	CRITICAL	800	NEW
□	11	CVE-2021-44228	TestLibs	CRITICAL	CRITICAL	800	NEW

CVE-2021-44228

Detected 800 days ago

CRITICAL

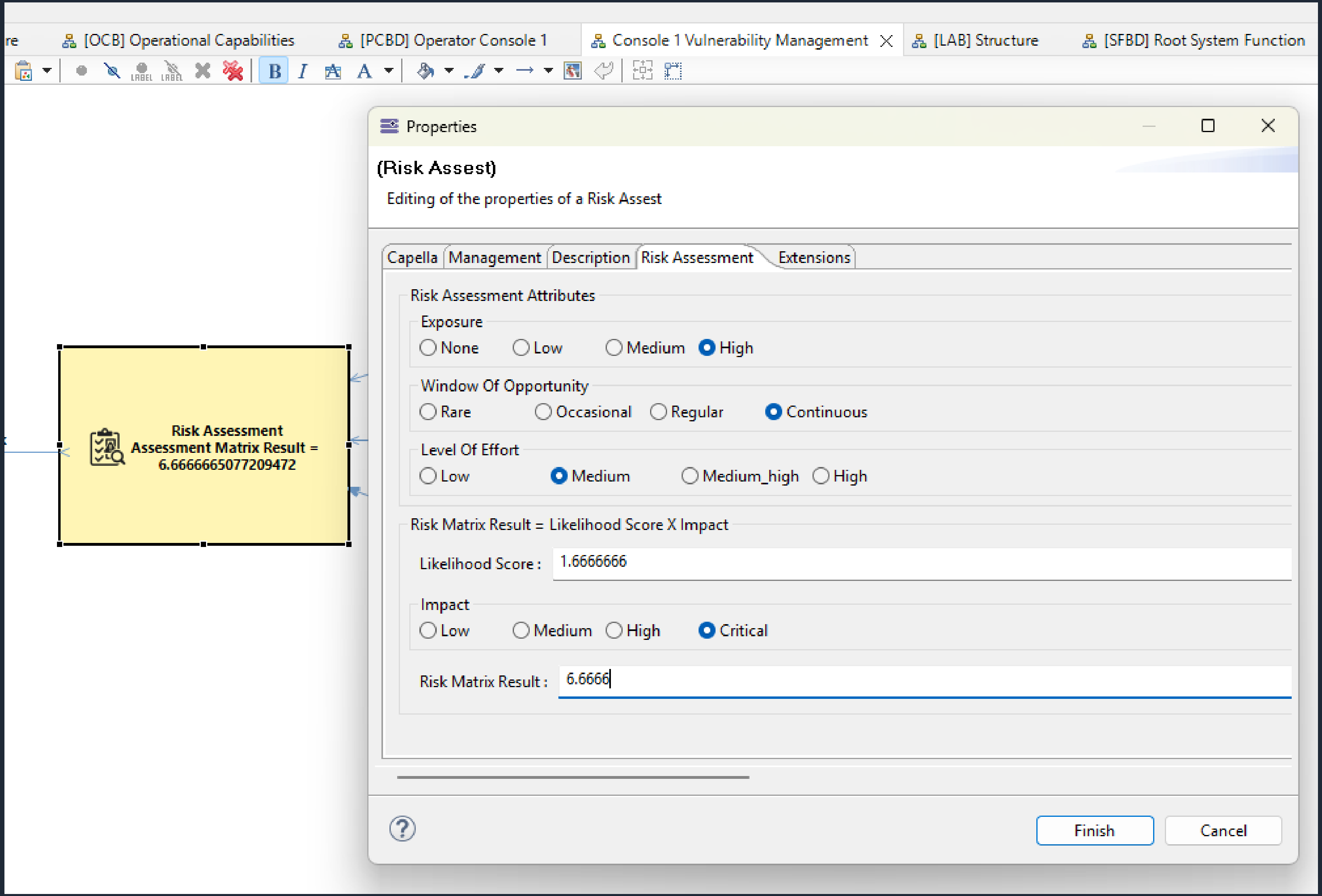
Source: openssl.h

General Comments

Assing to:

Issue Number: 0

Risk Assessment Node


re
[OCB] Operational Capabilities
[PCBD] Operator Console 1
Console 1 Vulnerability Management
[LAB] Structure
[SFBD] Root System Function

Risk Assessment
Assessment Matrix Result =
6.6666665077209472

Properties

(Risk Assest)

Editing of the properties of a Risk Assest

Capella
Management
Description
Risk Assessment
Extensions

Risk Assessment Attributes

Exposure
○ None ○ Low ○ Medium ● High

Window Of Opportunity
○ Rare ○ Occasional ○ Regular ● Continuous

Level Of Effort
○ Low ● Medium ○ Medium_high ○ High

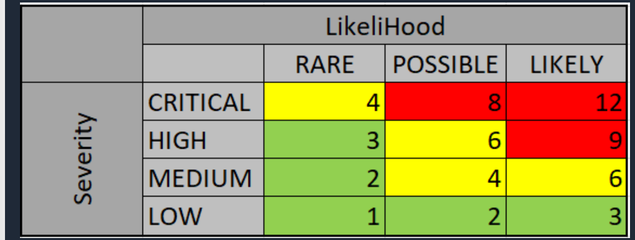
Risk Matrix Result = Likelihood Score X Impact

Likelihood Score : 1.6666666

Impact
○ Low ○ Medium ○ High ● Critical

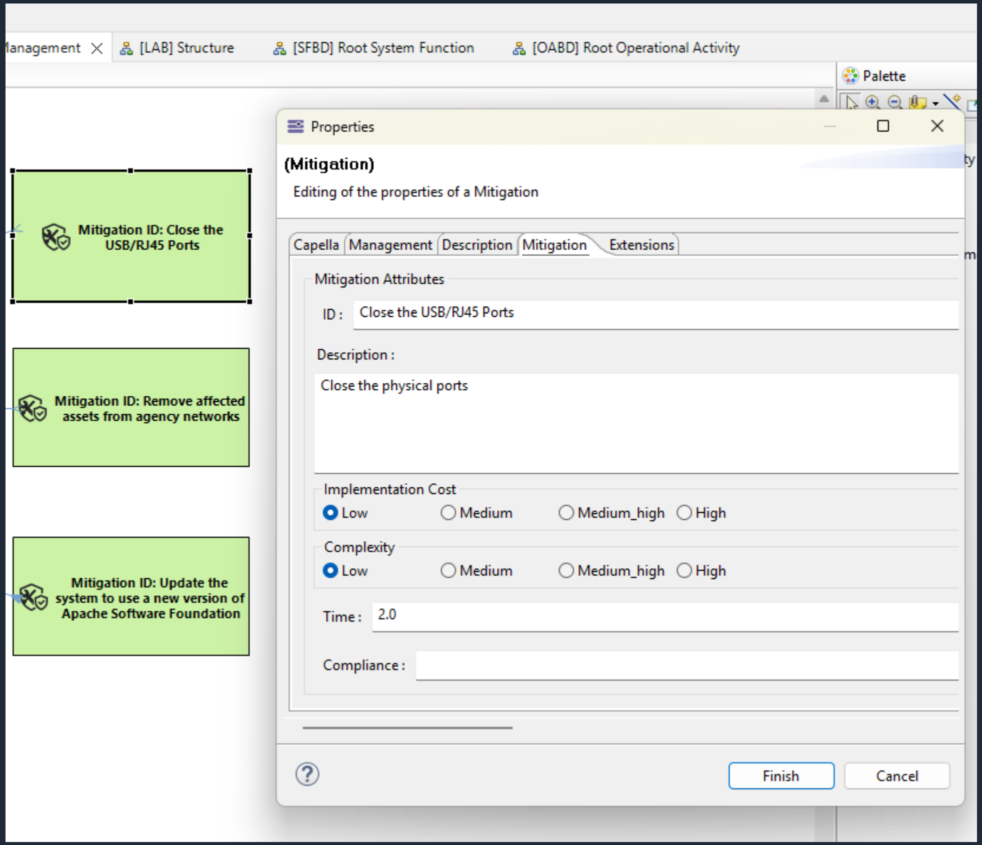
Risk Matrix Result : 6.6666

Finish
Cancel



		LikeliHood		
		RARE	POSSIBLE	LIKELY
Severity	CRITICAL	4	8	12
	HIGH	3	6	9
	MEDIUM	2	4	6
	LOW	1	2	3

Mitigation Node


lanagement
[LAB] Structure
[SFBD] Root System Function
[OABD] Root Operational Activity
Palette
Mitigation ID: Close the USB/RJ45 Ports
Mitigation ID: Remove affected assets from agency networks
Mitigation ID: Update the system to use a new version of Apache Software Foundation
Properties
Capella
Management
Description
Mitigation
Extensions
Finish
Cancel

(Mitigation)

Editing of the properties of a Mitigation

Mitigation Attributes

ID : Close the USB/RJ45 Ports

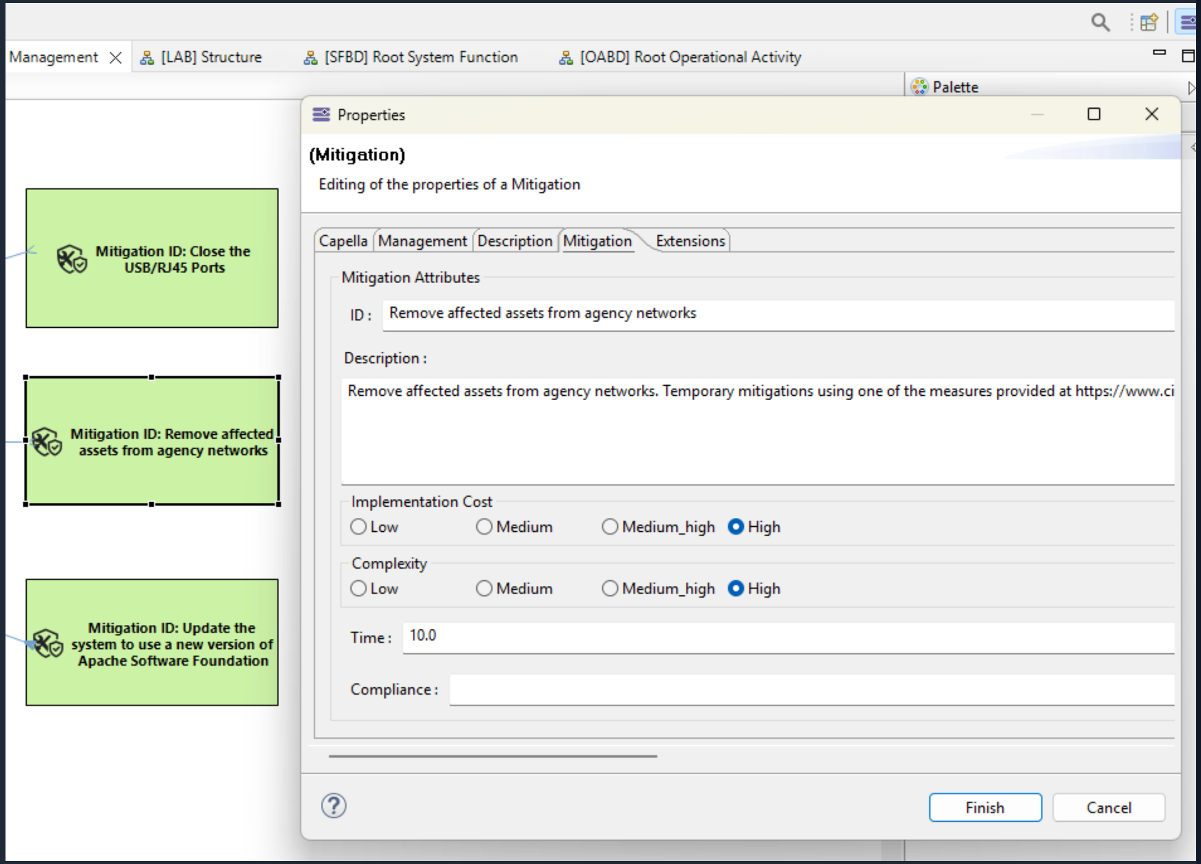
Description : Close the physical ports

Implementation Cost: ● Low ○ Medium ○ Medium_high ○ High

Complexity: ● Low ○ Medium ○ Medium_high ○ High

Time : 2.0

Compliance :


Management
[LAB] Structure
[SFBD] Root System Function
[OABD] Root Operational Activity
Palette
Mitigation ID: Close the USB/RJ45 Ports
Mitigation ID: Remove affected assets from agency networks
Mitigation ID: Update the system to use a new version of Apache Software Foundation
Properties
Capella
Management
Description
Mitigation
Extensions
Finish
Cancel

(Mitigation)

Editing of the properties of a Mitigation

Mitigation Attributes

ID : Remove affected assets from agency networks

Description : Remove affected assets from agency networks. Temporary mitigations using one of the measures provided at https://www.ci

Implementation Cost: ○ Low ○ Medium ○ Medium_high ● High

Complexity: ○ Low ○ Medium ○ Medium_high ● High

Time : 10.0

Compliance :

Measured Benefits in Practice

Reduced Mean Time to Mitigation

VAV significantly decreased the time required to:

- ✓ Identify vulnerabilities
- ✓ Analyze impact and exploit paths
- ✓ Implement targeted mitigations

● Streamlined remediation process

Highlighted Interdependencies

The attack-path revealed vulnerabilities dependencies between subsystems:

- ✓ Comprehensive understanding of vulnerability propagation
- ✓ Identification of critical attack vectors
- ✓ More effective mitigation strategies

● Enhanced system resilience

Avoided Late-Cycle Rework

By integrating cybersecurity concerns earlier and continuously throughout the development lifecycle:

- ✓ Proactive identification of vulnerabilities
- ✓ Prevention of costly late-stage changes
- ✓ Reduced security issue backlog

● Efficient resource allocation

Key Insight: VAV's model-centric approach transformed vulnerability management from a reactive, time-consuming process into a proactive, efficient activity that enhances system security without disrupting development schedules.

Summary of Contributions

1. VAV Meta-Model & Viewpoint Definitions

Formal definition cybersecurity vulnerabilities concepts integrated into ARCADIA models:

- Vulnerability
- Affected Asset
- Exploit Path
- Risk Assessment
- Mitigation
- Evidence

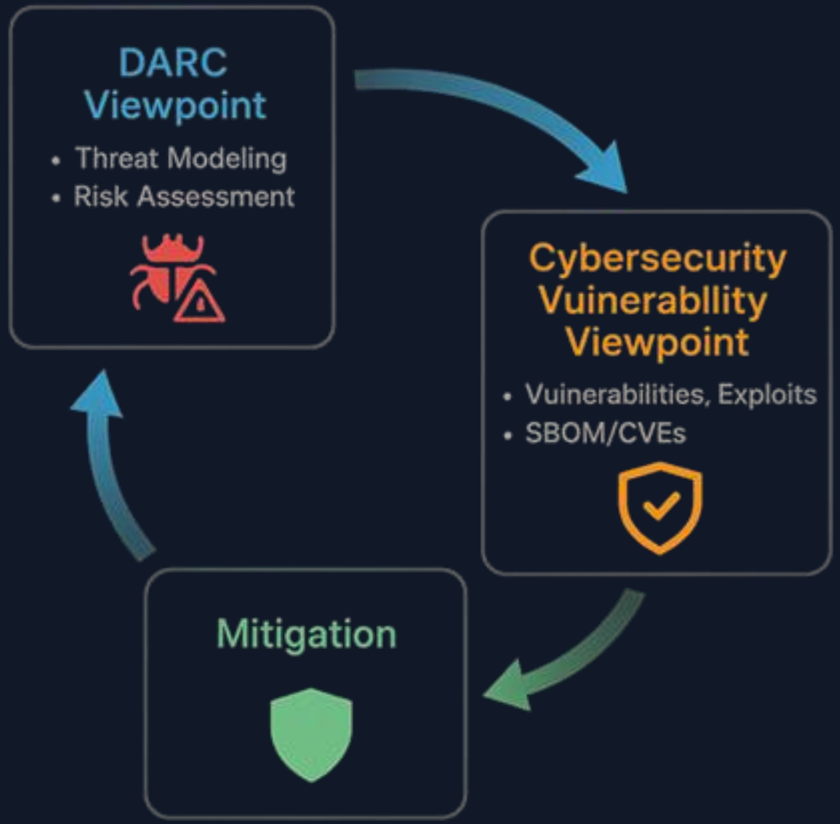
2. Best-Practice Workflows

Comprehensive workflows for systematic vulnerability management throughout the system lifecycle:

- Vulnerability Capture
- Impact Analysis
- Mitigation Planning
- Evidence Closure

Practical Guidance: Step-by-step processes for identifying, assessing, and managing vulnerabilities in MBSE

Complete Capella Cybersecurity Lifecycle



● DARC viewpoint

Threats (STRIDE / MITRE)

Trust Boundaries

Risk Scenarios / Attack Chains

● Vulnerability viewpoint

Vulnerability (linked to CVE, SBOM, KEV)

Affected component

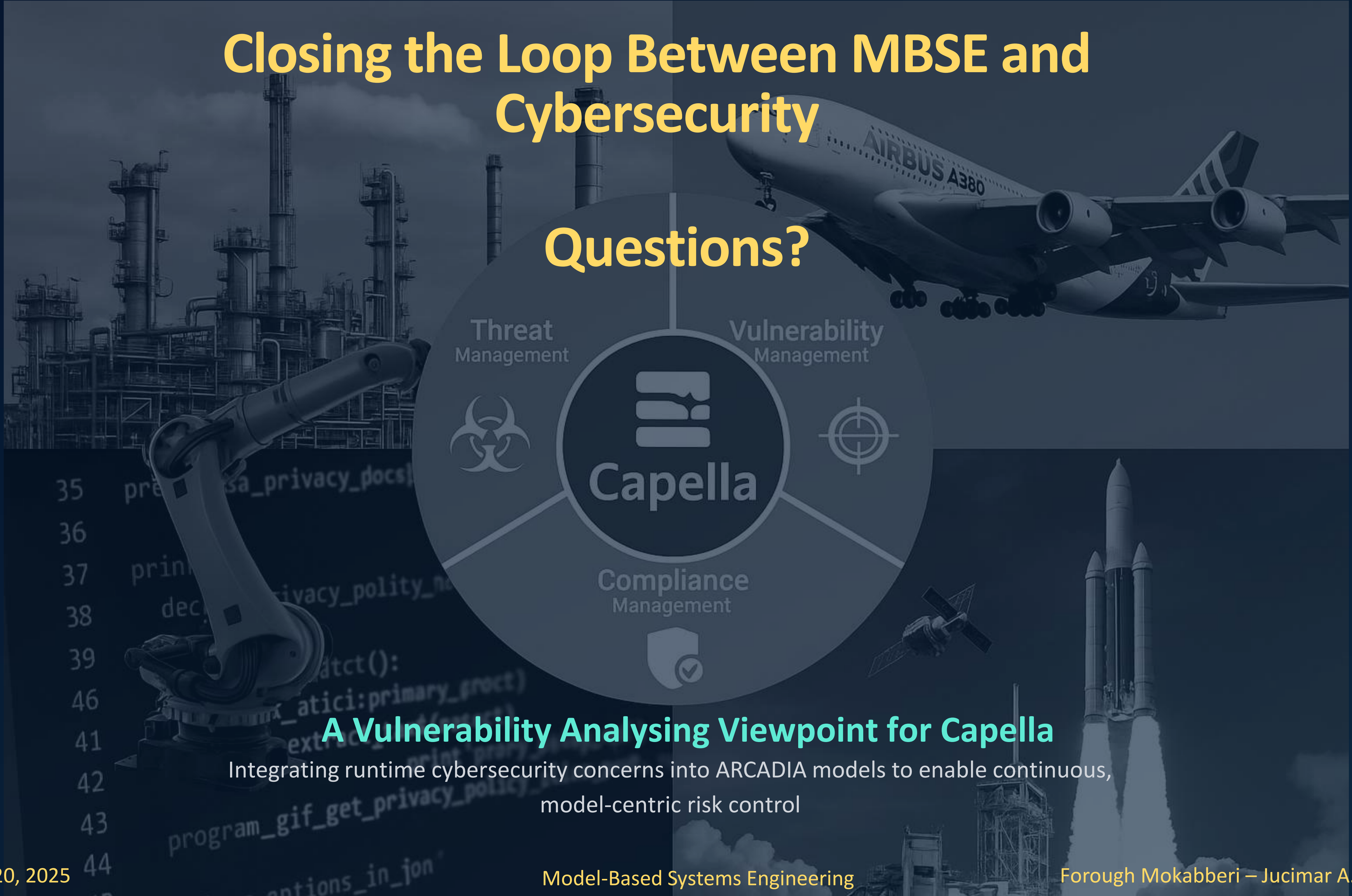
ExploitPath (if you modeled attack traversal)

RiskAssest (runtime risk reassessment)

Mitigation

Closing the Loop Between MBSE and Cybersecurity

Questions?



A Vulnerability Analysing Viewpoint for Capella

Integrating runtime cybersecurity concerns into ARCADIA models to enable continuous, model-centric risk control