Threat Modelling - Key Methodologies and Applications from OSS CIP (Civil Infrastructure Platform) Perspective

Dinesh Kumar
Project Manager, Toshiba Software India
SZ Lin (林上智)
TSC Representative, Moxa Inc.

ELCE 2020, 27th Oct.

About Us

- **Dinesh Kumar <**dinesh.kumar@toshiba-tsip.com**>**
  - Working for Toshiba Software India
  - Works for CIP Security work group
- **SZ Lin (林上智)** <sz.lin@moxa.com>
  - Working for Moxa Inc.
  - Contribute to Linux and other OSS projects
  - **4096R/9561F3F9**
    - 178F 8338 B314 01E3 04FC 44BA A959 B38A 9561 F3F9

Civil Infrastructure

https://www.airpano.com/360Degree-VirtualTour.php?3D=San-Francisco-USA

The key challenges

- **Apply IoT concepts to industrial systems.**
- **Ensure quality and longevity of products.**
- **Keep millions of connected systems secure.**

Industrial grade

- Reliability
- Functional Safety
- Real-time capabilities

Sustainability

- Product life-cycles of decades
- Backwards compatibility
- Standards

Security

- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions

CIP is the Solution

Industrial grade

- Reliability
- Functional Safety
- Real-time capabilities

Sustainability

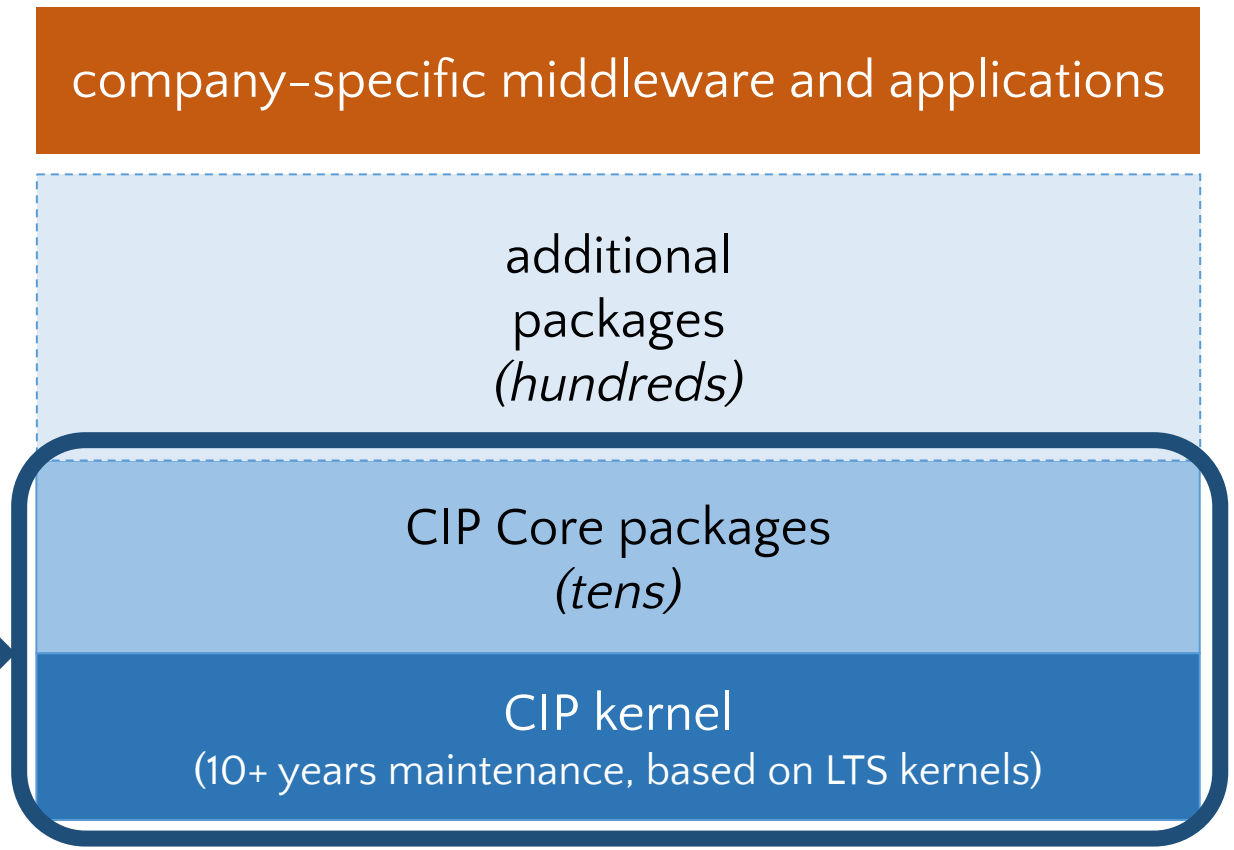
- Product life-cycles of decades
- Backwards compatibility
- Standards

Security

- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions

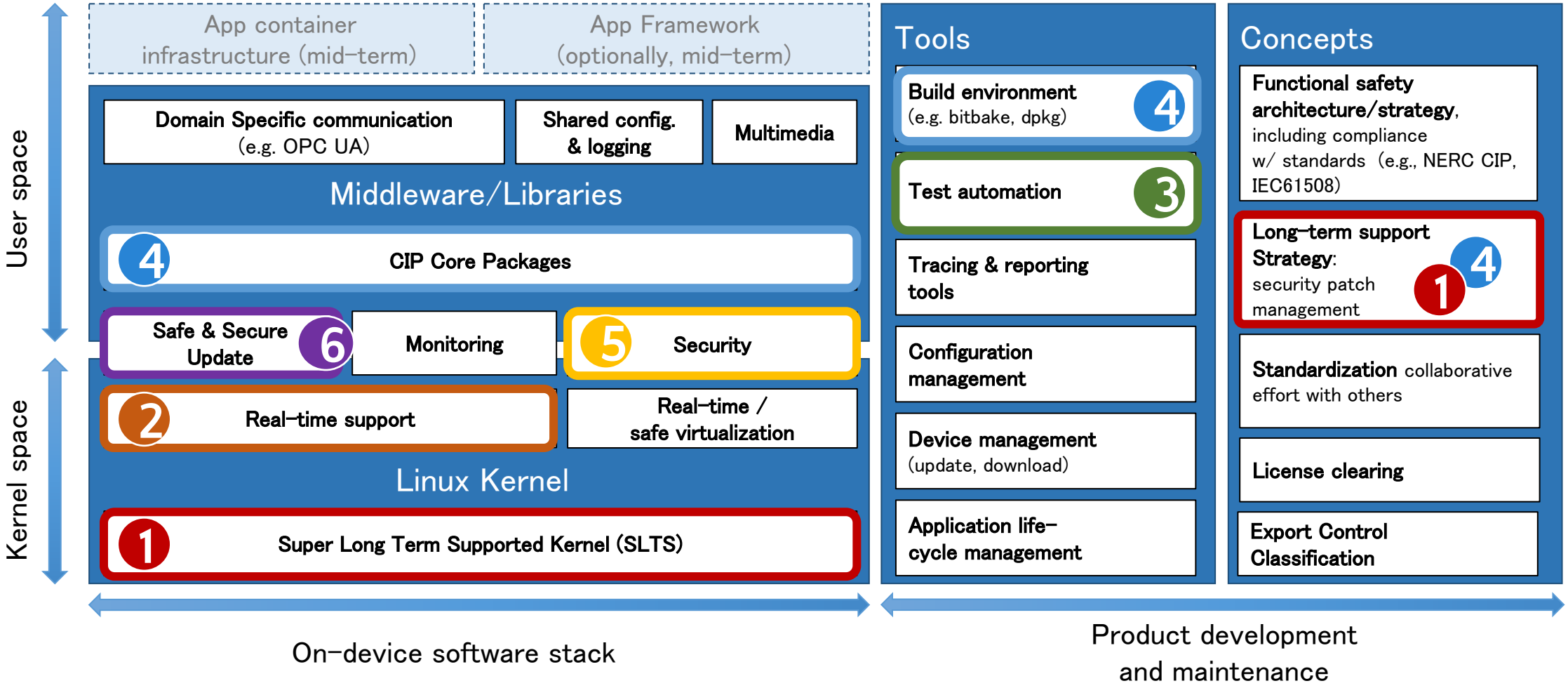
CIP is the Solution

CIVIL INFRASTRUCTURE PLATFORM



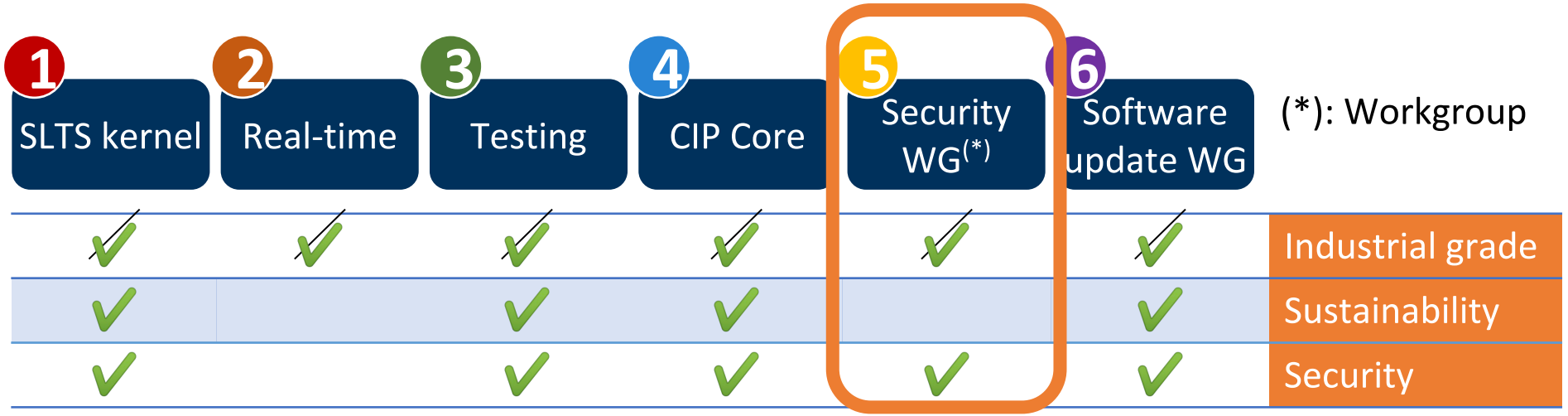
Establishes an "Open Source Base Layer (OSBL)"

The Scope of CIP



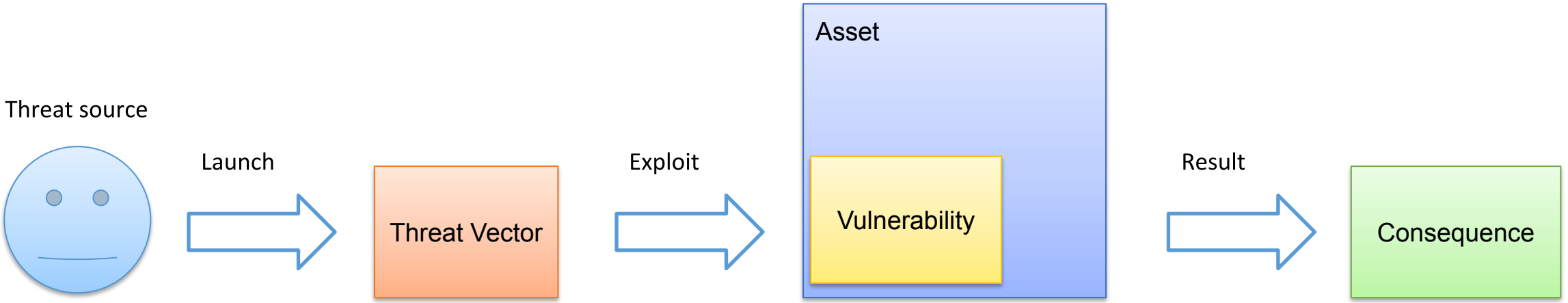
Security Workgroup

- Protect the asset in the civil infrastructure system by reducing the risk
- Adapt the international standard - ISA/ IEC 62443 (Industrial Automation & Control System Cybersecurity Standards)



CIP Projects and its scopes

Cybersecurity Risk



e.g., Insiders, hackers

e.g., Unauthorized access to system/ data, social engineering

e.g., Unpatched system, plaintext communication

e.g., critical data leakage, service disruptions

Risk = Threat X Vulnerability X Consequence

What is Threat?

Threat

- Can be initiated by system itself as well as outsider
- Comparatively hard to detect than attacks
- Information may or may not be altered or damaged
- Circumstance that has ability to cause damage
- May or may not be malicious
- Can be intentional or unintentional

src: https://pixabay.com/zh/illustrations/away-junction-direction-1020200/

Threat Modelling

The process of anticipating

“what could go wrong”

and then forecasting

“how it can go wrong.”

CIVIL INFRASTRUCTURE PLATFORM

General Threat Modelling Objectives

- Attack surface reduction
- Secure default configurations
- Least privilege
- Defense in depth
- Compartmentalization
- Policy compliance

CIP - Objective of Threat Modelling

- Help CIP end users to re-use CIP platform reference threat modelling and build further security on top of it
- Periodically review and update threat model to incorporate newly reported threats
- Reduce the risk of Open Source Base Layer

Threat Modelling Methodologies

Threat source/ viewpoint

Model capability, intent, and targeting for adversarial threats. Find out the actions that the threat agent might conduct.

Threat actions

Model the actions which might conducted by threat actor. The common method is STRIDE model developed by Microsoft.

Threat activity

Model the activity which conducted by a series of threat actions to achieve desired outcome. The common method is attack tree.

Vulnerability viewpoint

Model the vulnerability within the asset which may existed in the organization. Typically, massive of technical information is essential as indicators

Key Threat Modelling Methodologies

- STRIDE threat modelling
- Attack trees
- Process for Attack Simulation and Threat Analysis (PASTA)
- Common Vulnerability Scoring System (CVSS)
- Security Cards
- Hybrid Threat Modelling Method (hTMM)

Risk mitigation by Threat Modelling

- **Four ways to reduce risk by using threat analysis report**
  - Redesign to eliminate
    - Takes more time more resources, sometime may not be feasible as component development is out of your control
  - Apply standard mitigations
    - Investigate or re-use how similar threats were mitigated
  - Invent new mitigations
    - It could be riskier if not done properly
  - Adapt compensating controls
    - Take appropriate extra measures in implementation

Data-flow Diagram (DFD) cont...

- Processes
  - are elements that, based on their input, perform actions and/or generate outputs.
- Data stores
  - are sinks or sources of data. Examples are databases or internal storage.
- Data flows
  - represent the flow of information between elements. A data flow can be a protocol specific communication link such as HTTPS or UDP.
- External interactors
  - are elements whose influence should be taken into account, but which are outside the scope of the analysis.
- Trust boundaries
  - divide the elements in the diagram into different trust zones, e.g. elements in open networks vs elements in internal networks

Data-flow Diagram (DFD)

External Entity

- People
- Other systems
- Web portals

Processes

- DLL/.so
- Components
- Services
- exe
- Web services
- Assemblies

Data flow

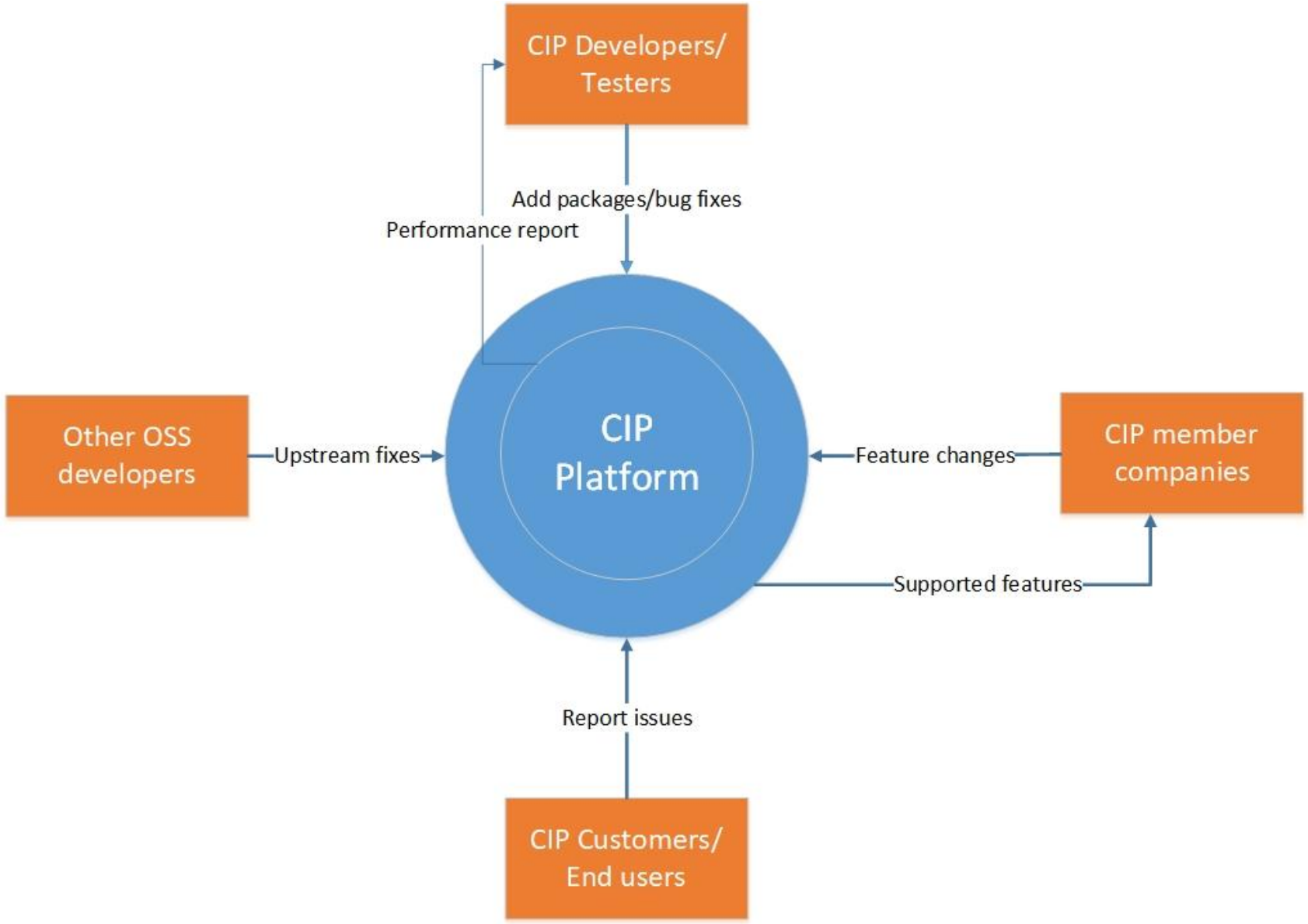
- Function call
- Network traffic
- RPC

Data Store

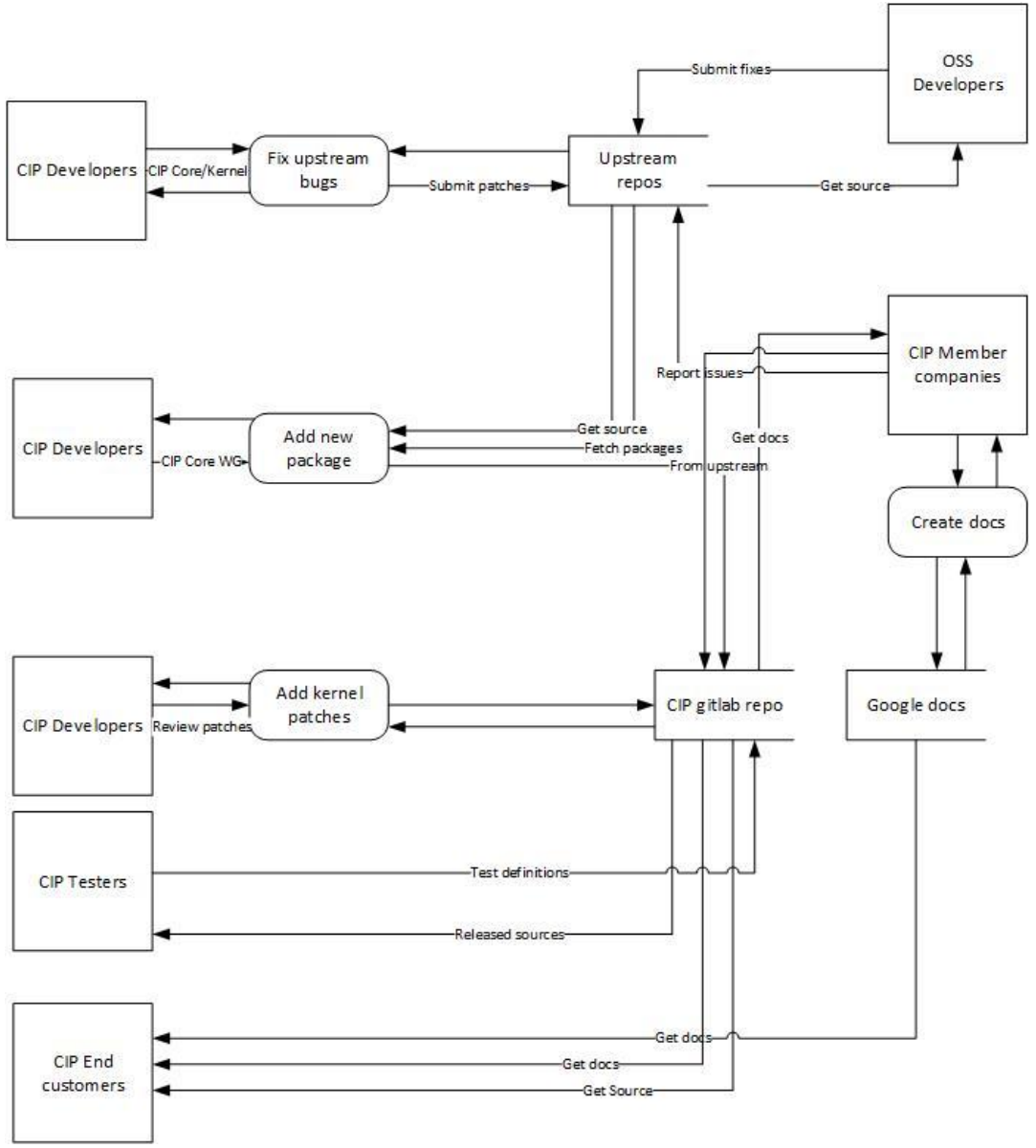
- Database
- File
- Registry
- Config files
- Shared memory file

CIVIL INFRASTRUCTURE PLATFORM

CIP Development Context Diagram



CIP Development DFD

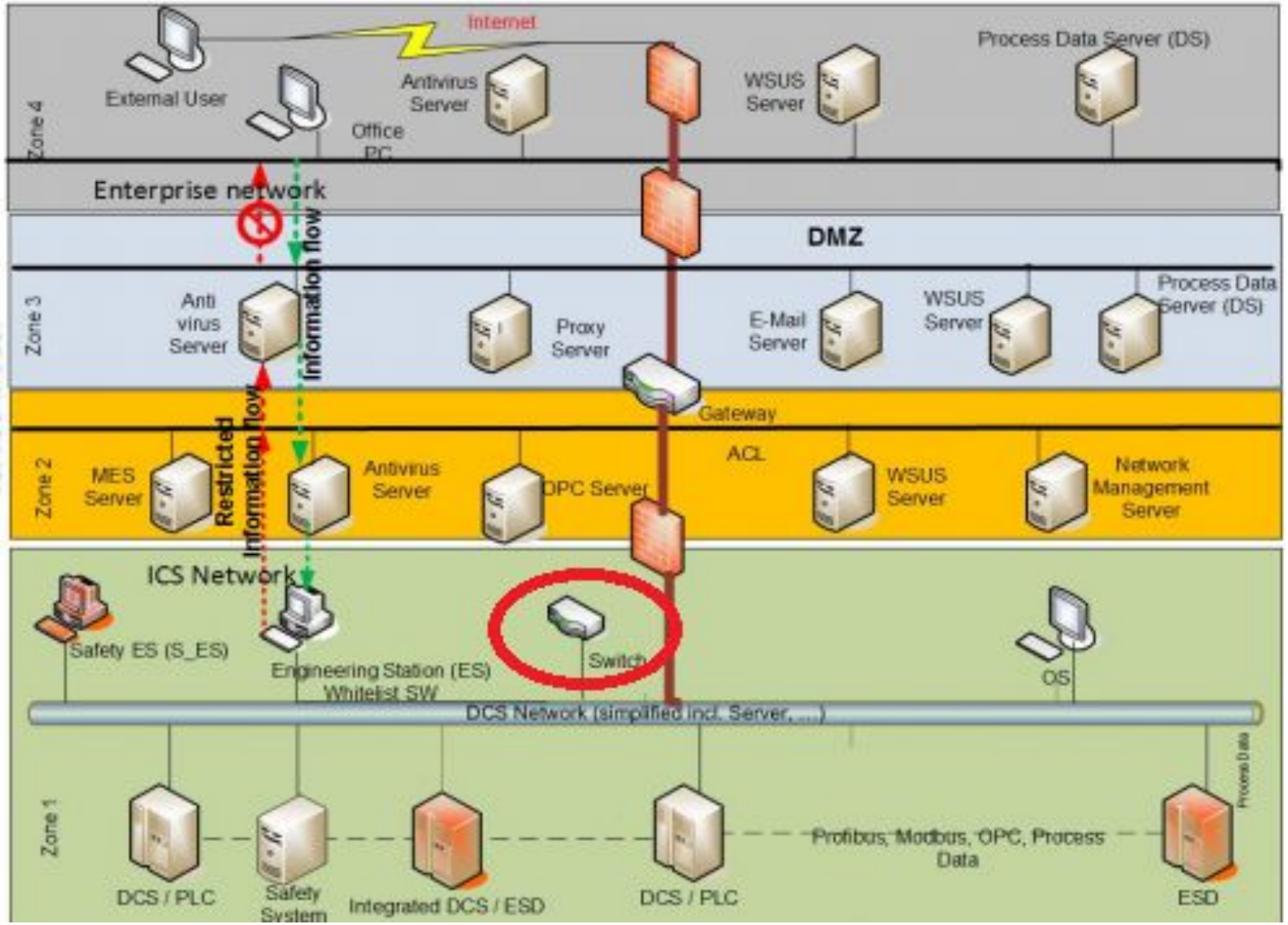


STRIDE: Threats affecting elements

Elements	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flows		✖		✖	✖	
Data Stores		✖		✖	✖	
Processes	✖	✖	✖	✖	✖	✖
Interactors	✖		✖			

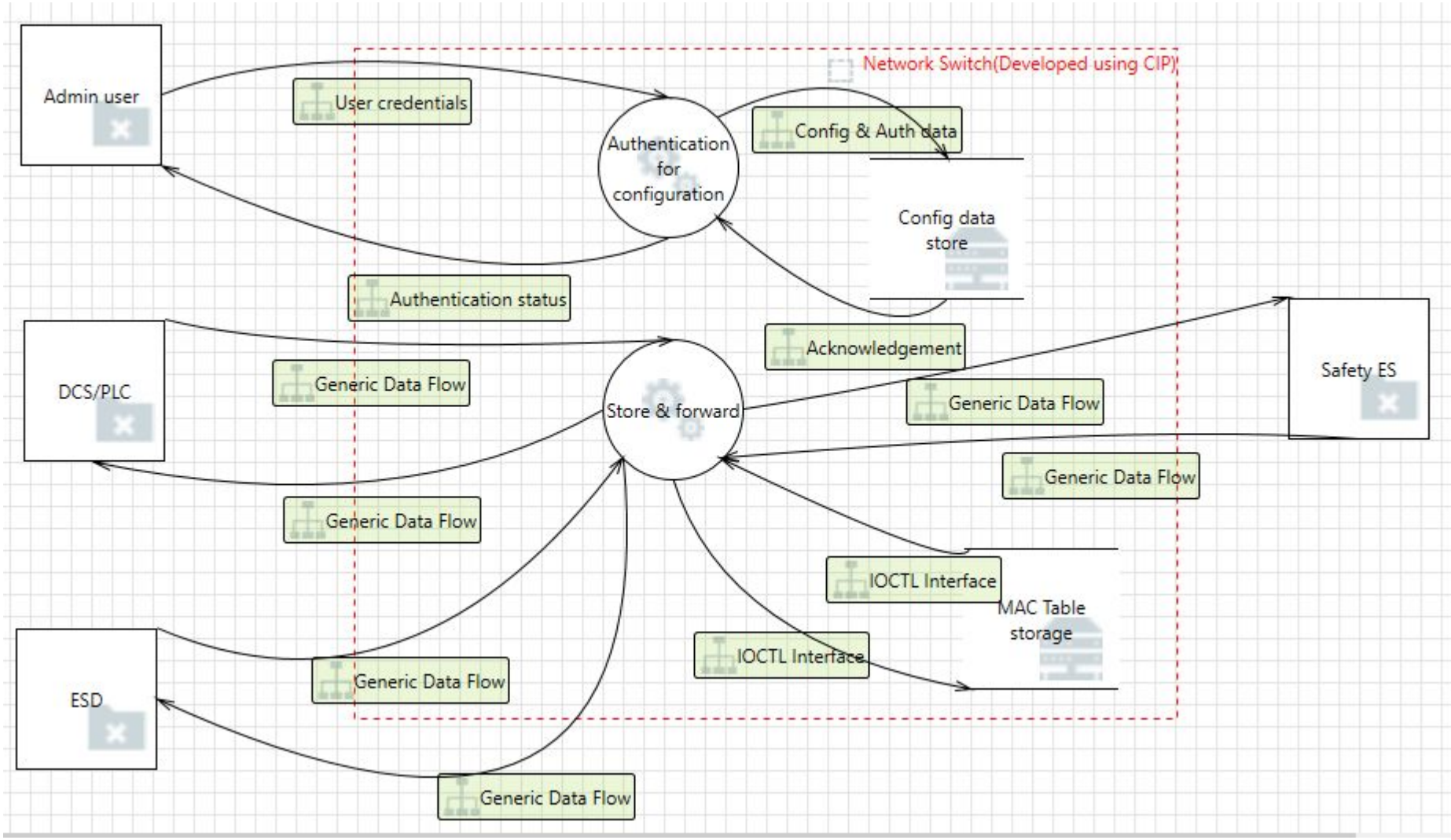
CIP as Networking Switch Use Case

- The image depicts ICS reference architecture for Zones and Conduits
- Zone-1 components consist of core components
- Let's try to create DFD and threat model for network switch assuming switch is based on CIP platform

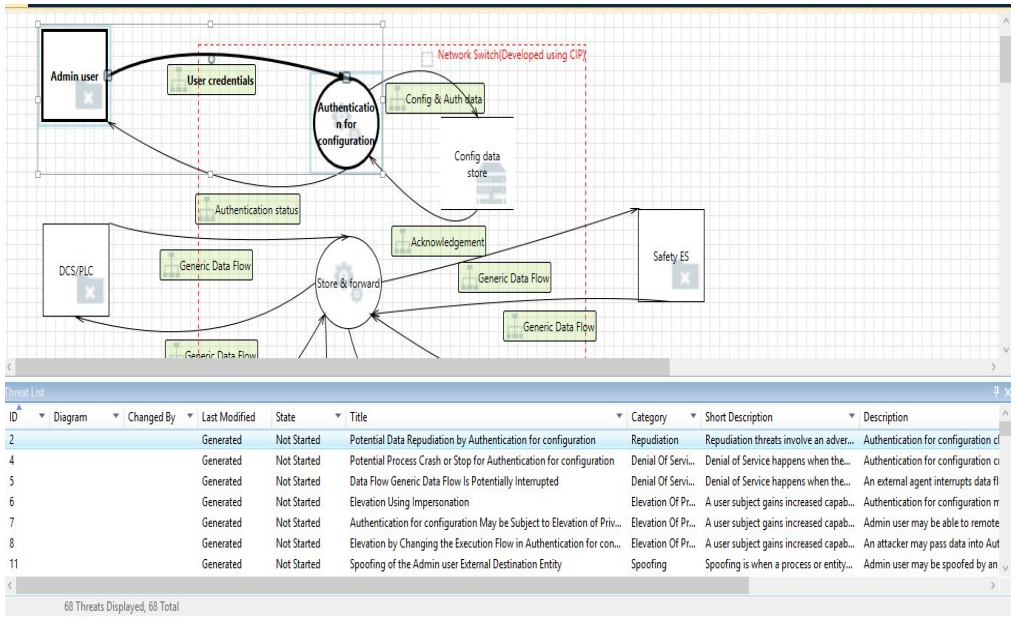


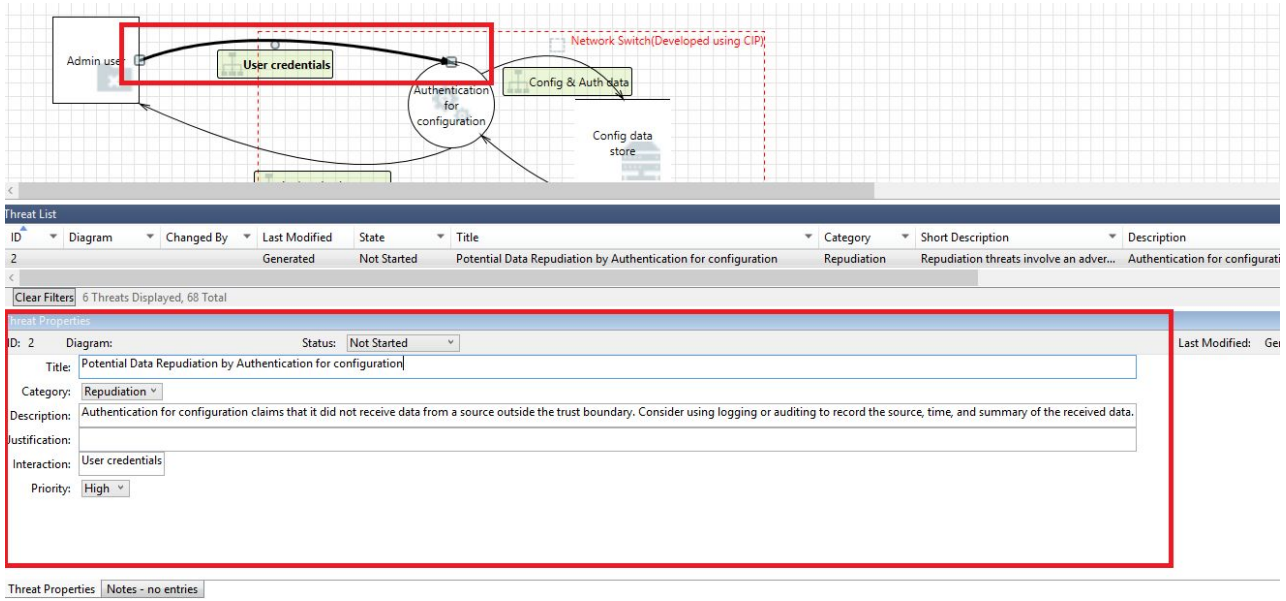
https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf

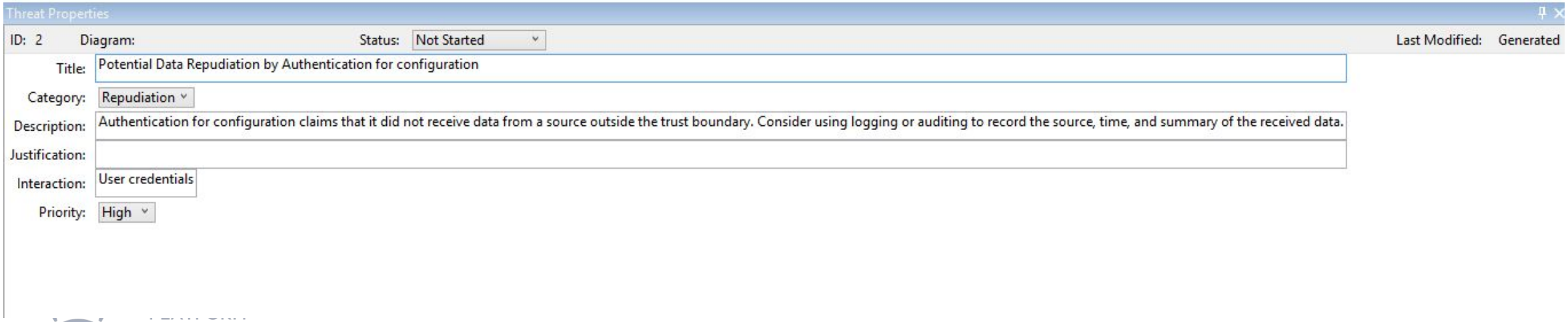
STRIDE: CIP DFD (As Networking Switch)



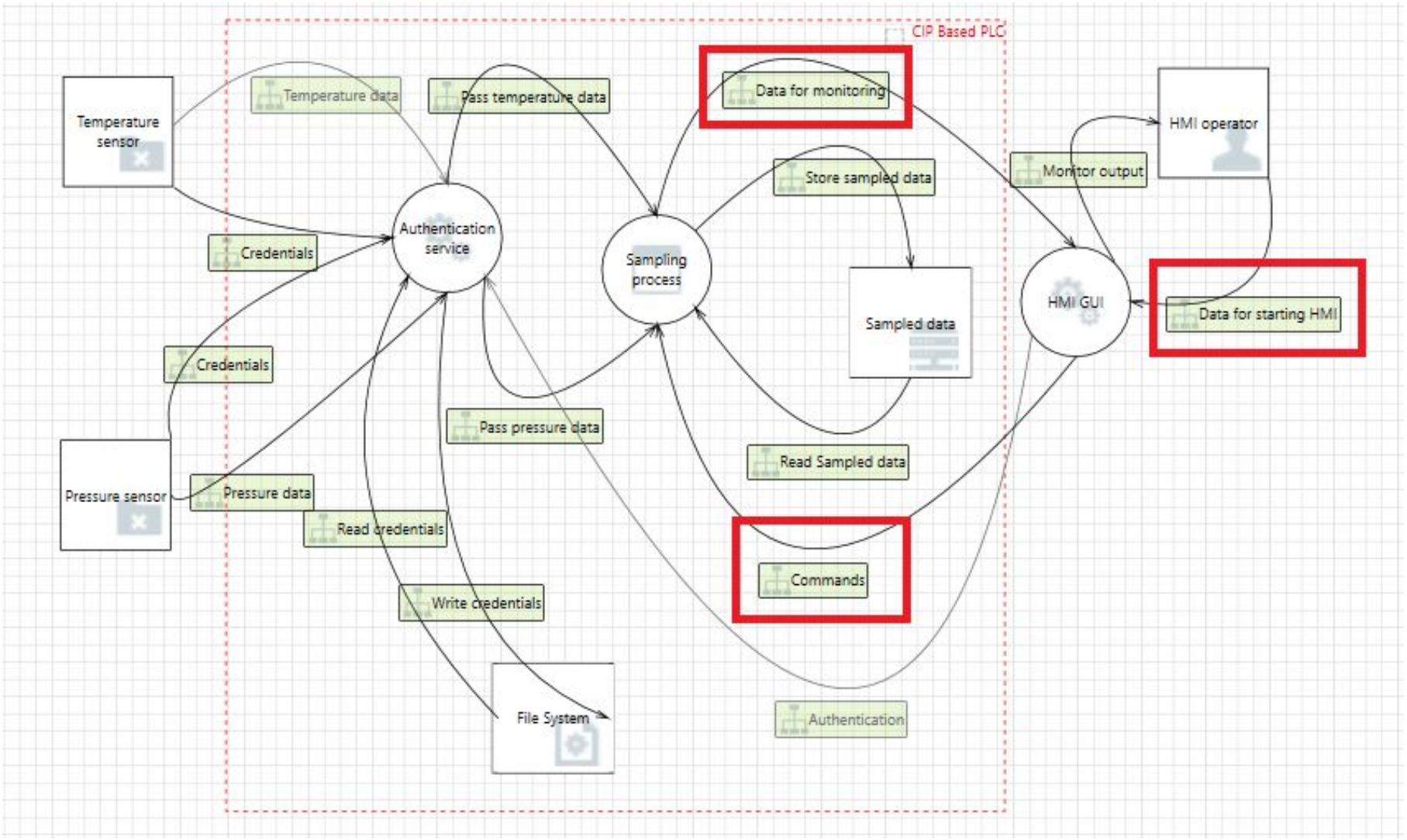
STRIDE: Networking Switch (CIP Threat Analysis View)





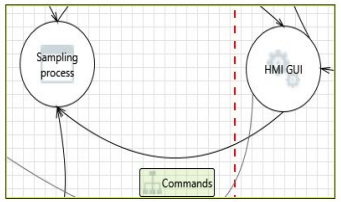


CIP DFD (As PLC Use Case)



STRIDE: Threat Model Analysis Report

Interaction: Commands



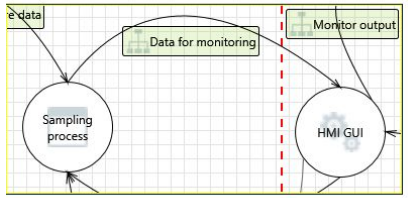
1. Virtual Machine Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering
Description: If HMI GUI is given access to memory, such as shared memory or pointers, or is given the ability to control what Sampling process executes (for example, passing back a function pointer), then HMI GUI can tamper with Sampling process. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.
Justification: <no mitigation provided>

2. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Sampling process may be able to impersonate the context of HMI GUI in order to gain additional privilege.
Justification: <no mitigation provided>

Interaction: Data for monitoring



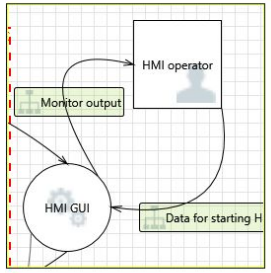
32. Replay Attacks [State: Not Started] [Priority: High]

Category: Tampering
Description: Packets or messages without sequence numbers or timestamps can be captured and replayed in a wide variety of ways. Implement or utilize an existing communication protocol that supports anti-replay techniques (investigate sequence numbers before timers) and strong integrity.
Justification: <no mitigation provided>

33. Collision Attacks [State: Not Started] [Priority: High]

Category: Tampering
Description: Attackers who can send a series of packets or messages may be able to overlap data. For example, packet 1 may be 100 bytes starting at offset 0. Packet 2 may be 100 bytes starting at offset 25. Packet 2 will overwrite 75 bytes of packet 1. Ensure you reassemble data before filtering it, and ensure you explicitly handle these sorts of cases.

Interaction: Data for starting HMI



44. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: HMI GUI may be able to impersonate the context of HMI operator in order to gain additional privilege.
Justification: <no mitigation provided>

45. Spoofing the HMI operator External Entity [State: Not Started] [Priority: High]

Category: Spoofing
Description: HMI operator may be spoofed by an attacker and this may lead to unauthorized access to HMI GUI. Consider using a standard authentication mechanism to identify the external entity.

- Threat Model Analysis Report reveals about the missing security measures in existing models
- For each missing point, counter measures information should be provided or security measures should be taken
- At each design change or new package addition this step should be repeated

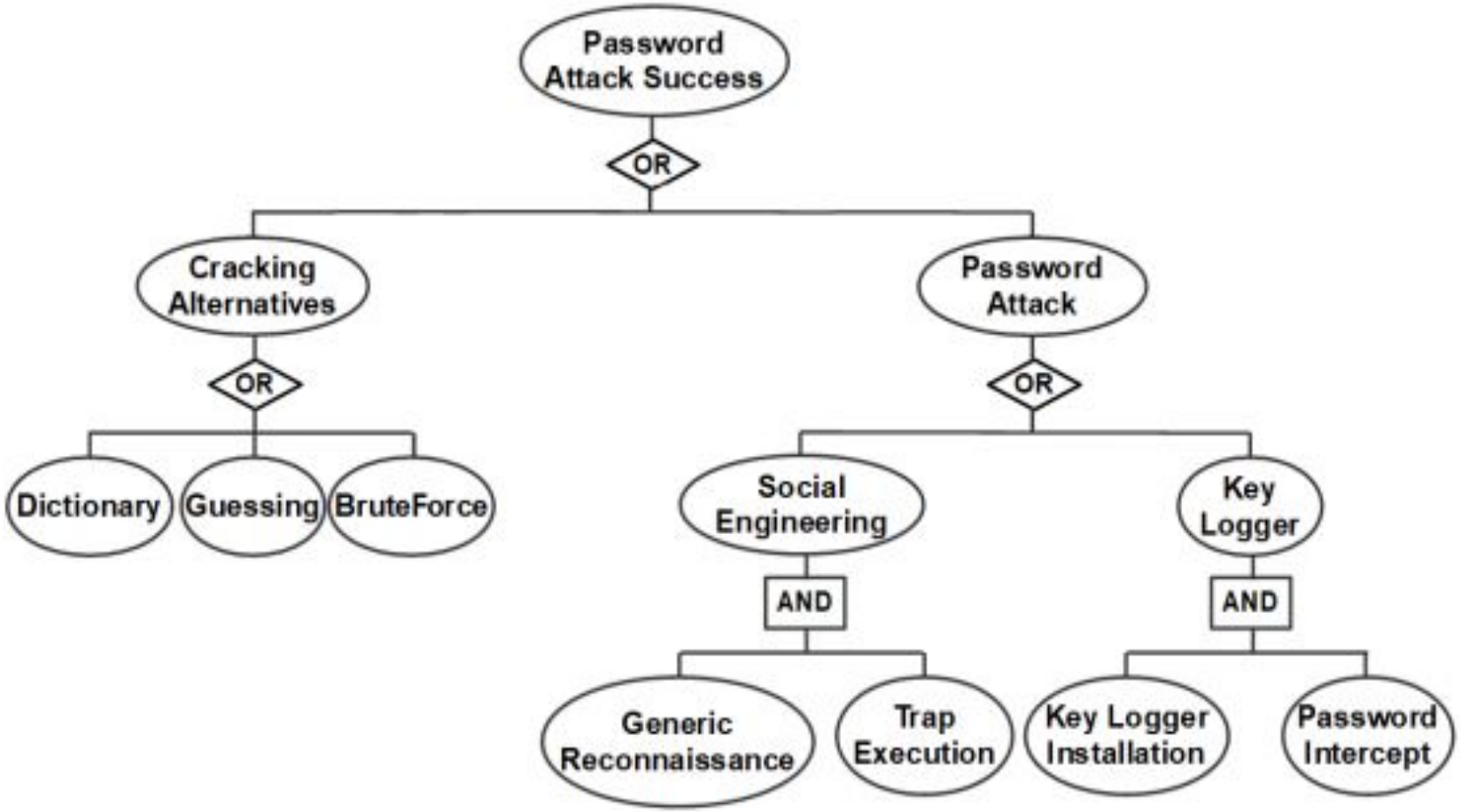
CIVIL INFRASTRUCTURE PLATFORM

STRIDE: Standard Mitigations

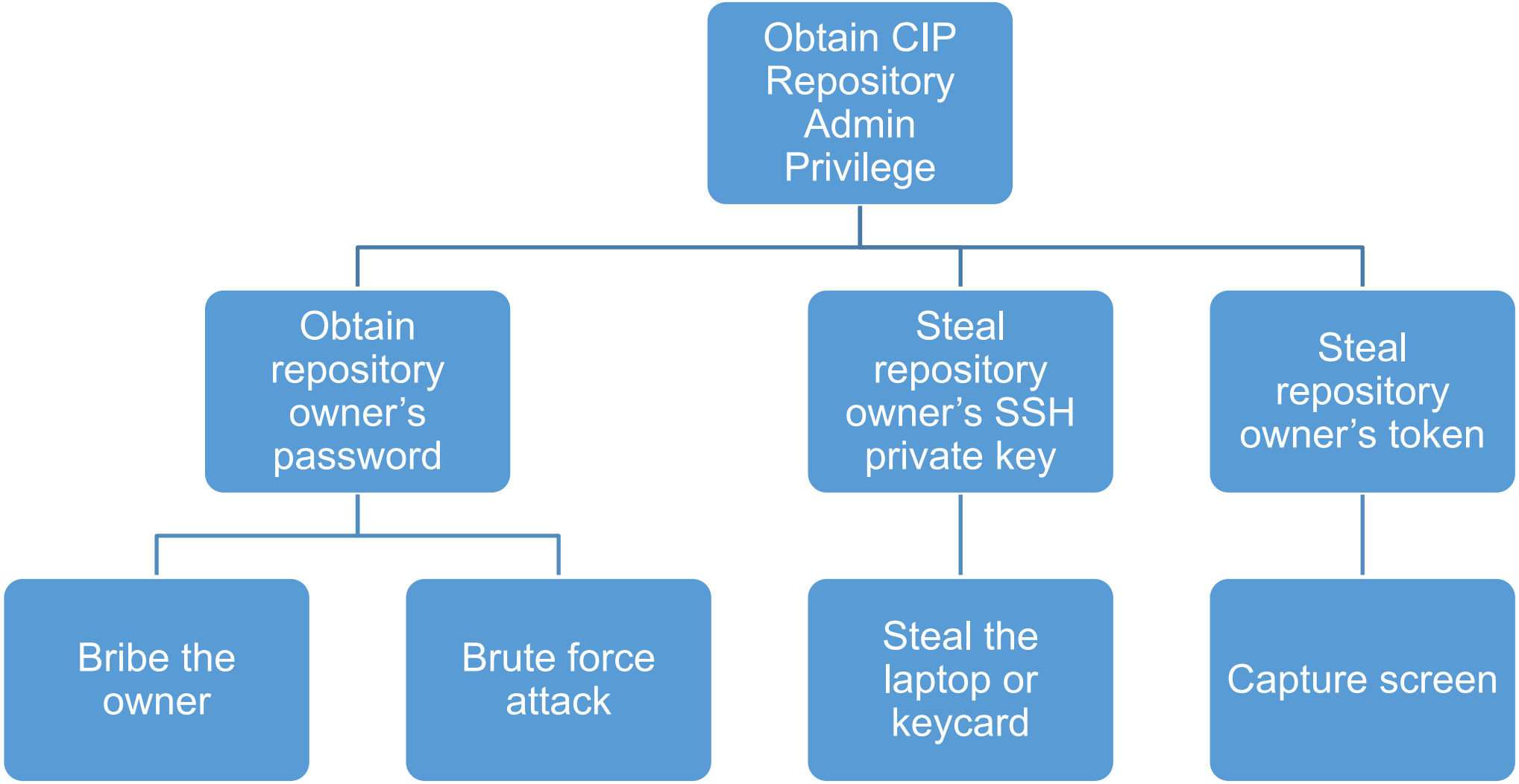
Threat	Security property	Mitigation methods	CIP feature to address standard Threats
Spoofing	Authentication	-Kerberos authentication -PKI Systems, SSL, TLS -Digital signatures	-shadow, pam, -libpam_google_authenticator, -openssl
Tempering	Integrity	-MAC(Mandatory Access Control) -ACLs -Digital Signatures -Checksum	-acl -openssl(digital signature verification) -Sha256, sha512
Repudiation	Non Repudiation	-Secure logging & auditing -Digital signatures	-auditd -rsyslog
Information disclosure	Confidentiality	-Encryption -ACLs	-openssl -acl
Denial of service	Availability	-ACLs -Security policies -Quota	-pam -openssh -acl
Elevation of privileges	Authorization	-ACLs -Group of Role membership -Input Validation	-acl -security policies published via application rules

Generic Attack Tree example

- Root node of the tree is the global goal of the attacker
- Each node represents one attack
- An attack tree defines a collection of possible attacks
- An attack described in a node may require one or more of many attacks described in child nodes to be satisfied

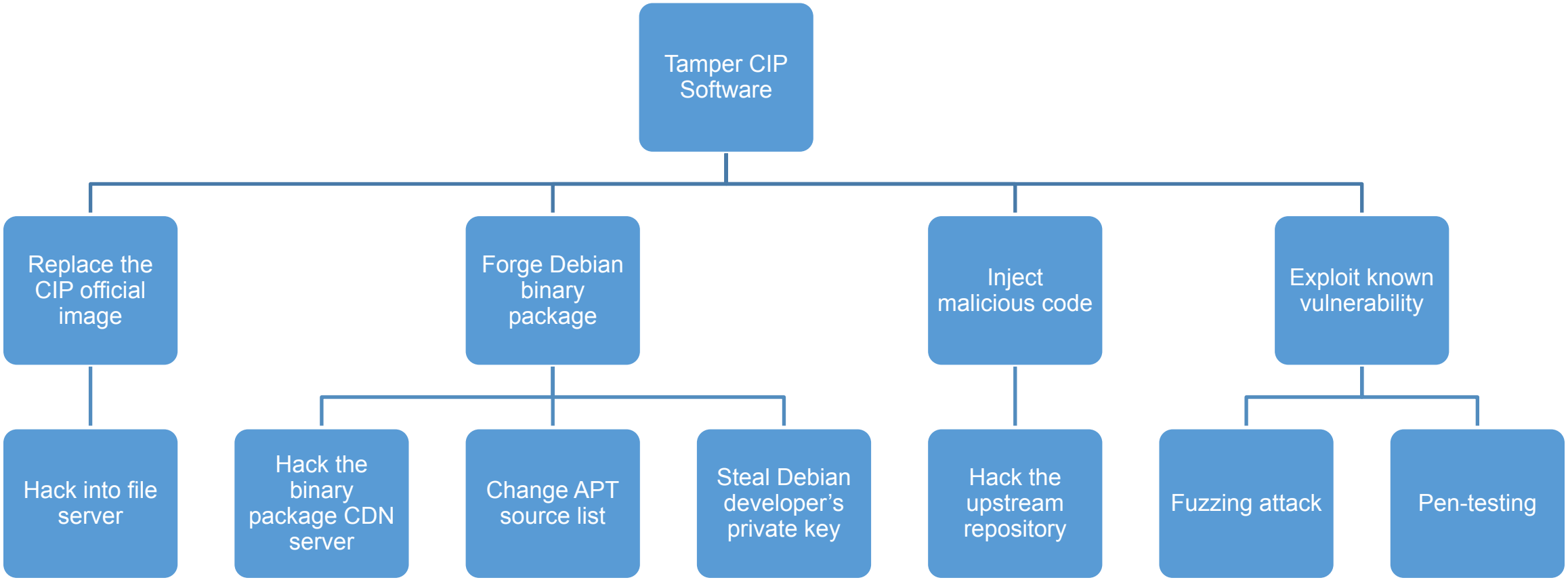


Attack Tree for CIP Repositories



CIVIL INFRASTRUCTURE PLATFORM

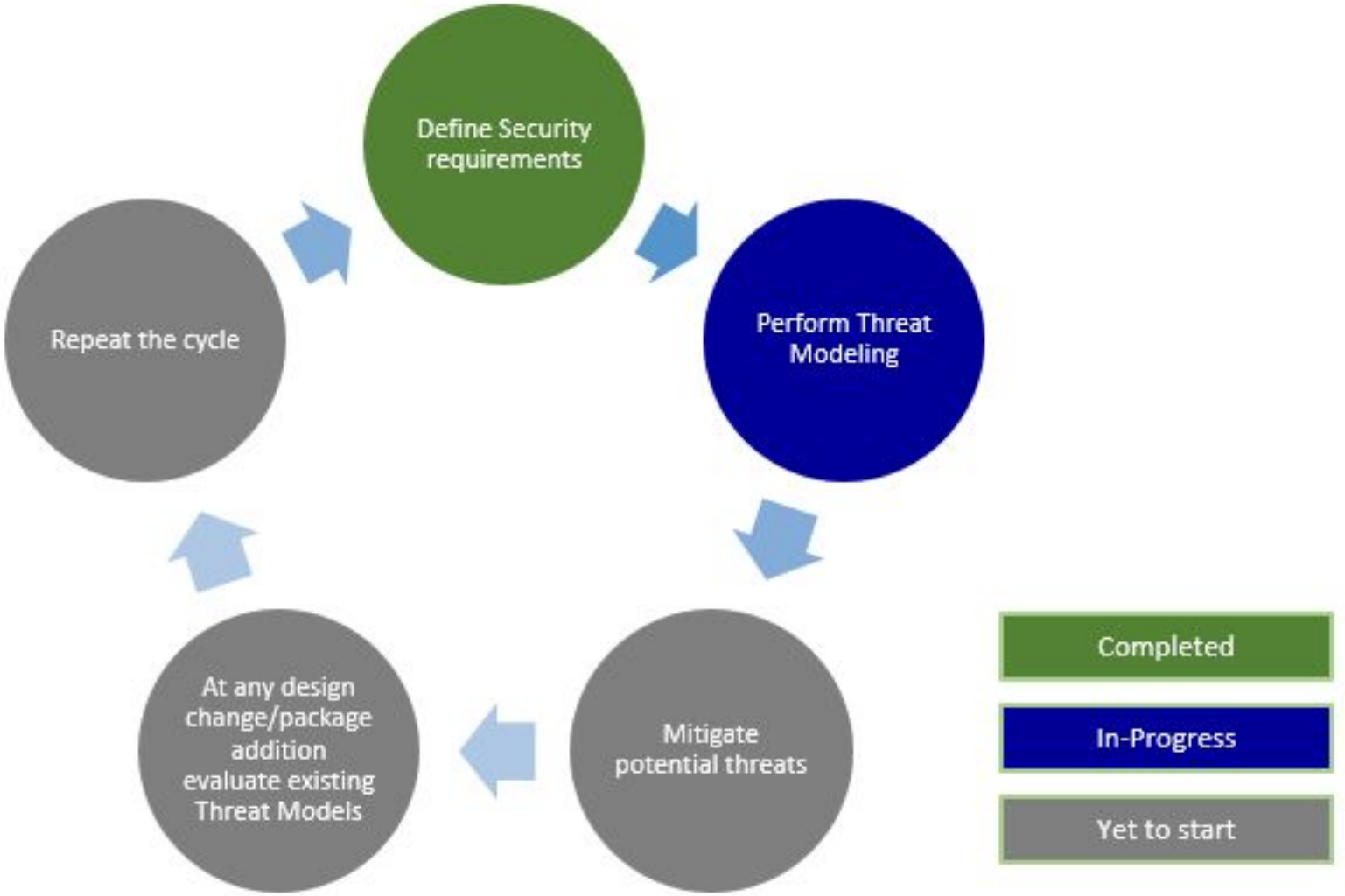
Attack Tree for CIP based systems



Validating Threat Models

- Validate whole threat model
  - Does diagram match the final code or final system implementation?
  - Are all threats enumerated
  - Minimum: STRIDE per element that touches a trust boundary
  - Has test/QA reviewed the model
    - Tester often finds issues with threat models or uncover something not considered during threat modelling
  - Is each threat mitigated
  - Are mitigations done right

Next Step for CIP Threat Modelling



Reference for CIP resources

- CIP Home page
  - https://www.cip-project.org/
- CIP Work Groups wiki page
  - https://wiki.linuxfoundation.org/civilinfrastructureplatform/start
- CIP membership page
  - https://www.cip-project.org/about/join
- CIP Core gitlab
  - https://gitlab.com/cip-project/cip-core
- CIP Kernel gitlab
  - https://gitlab.com/cip-project/cip-kernel/linux-cip
- CIP Documents
  - https://gitlab.com/cip-project/cip-documents

Threat Modelling Tools

- **Draw.io libraries for threat modelling**
  - https://github.com/michenriksen/drawio-threatmodeling
- **OWASP-Threat-Dragon**
  - https://threatdragon.org/login
- **threatspec**
  - https://threatspec.org/
- **pytm**
  - https://github.com/izar/pytm
- **Microsoft Threat Modelling Tool**
  - https://docs.microsoft.com/en-gb/azure/security/develop/threat-modeling-tool

CIP Talks at ELCE, and CIP Mini Summit

- October 26
  - CIP Kernel: Upstream first is our principle
- October 27
  - CIP Security: Threat Modelling
  - Real time Linux virtualization, Embedded systems building, bridging communities
- October 28
  - CIP Security: The international effort to establish Base Layer
- October 30
  - CIP Mini-summit

Please Visit CIP Virtual Booth!

"CIP mini-summit" will be held on Oct. 30th (Frid)"
thank you!

Join us

CIP for sustainable Smart Cities with Open Source Software

RENESAS SIEMENS TOSHIBA

Codethink cybertrust HITACHI Inspire the Next

MOXA Plat' Home There, we are. Internet of Things

Question?

Thank you

CIVIL
INFRASTRUCTURE
PLATFORM

References

- NIST Special Publication 800-30r1 Guide for Conducting Risk Assessments
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- NIST Special Publication 800-39 Managing Information Security Risk
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- Secure Code, Threat modeling sessions
  - https://www.youtube.com/watch?v=gDtS68DPm6Q