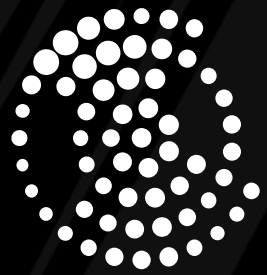
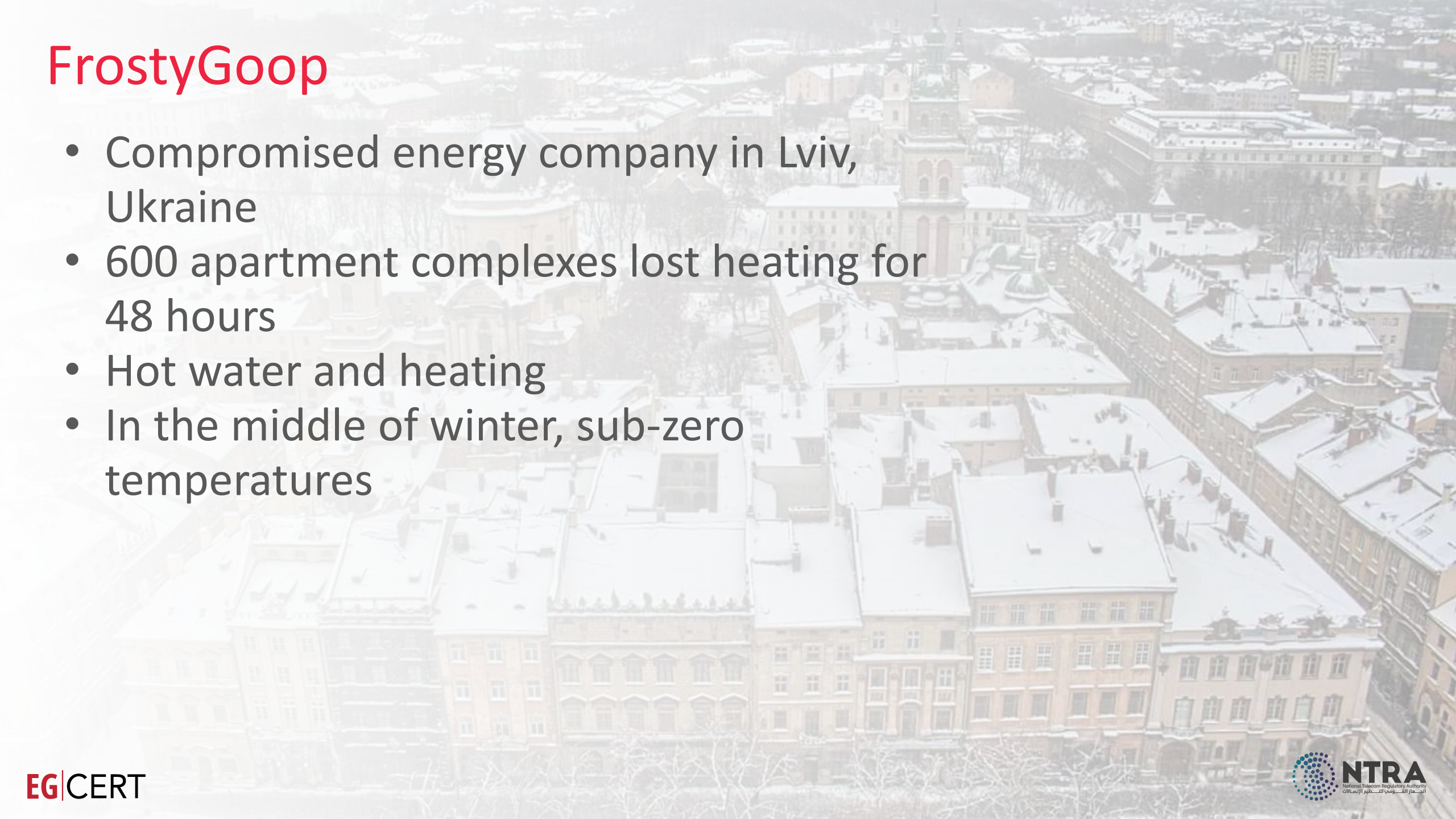
EG|CERT



NTRA
National Telecom Regulatory Authority
الجـــهاز القـــومي لتنـــظيم الإتصـالات

FrostyGoop

- Compromised energy company in Lviv, Ukraine
- 600 apartment complexes lost heating for 48 hours
- Hot water and heating
- In the middle of winter, sub-zero temperatures



FrostyGoop

- Gained initial foothold in IT Network, ~9 months prior
- Exploit Vulnerability in MikroTik Router
- Setup backdoors and remote connections in victim network
- Downgraded ENCO Controller firmware
- Hackers Scans for devices running over Modbus TCP
- Turned off heating

Unitronics Attack

IOCONTROL Malware: Iranian Cyber Attacks on IoT & OT

EG|CERT

NTRA
National Telecom Regulatory Authority

Iranian CyberAv3ngers

- In Feb 2024 CyberAv3ngers targeted devices operating in water treatment facilities in Israel and the United States
- They Leaved behind a message threatening other similar technology made in Israel.
- No other damage was done!!!!!

Why?!!

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Video Live

US sanctions Iranian officials over cyber-attacks on water plants

2 February 2024

Share Save

Azadeh Moshiri
BBC News

The US has imposed sanctions on six officials in Iran's powerful Islamic Revolutionary Guard Corps (IRGC) which it says are responsible for the cyber-

TECH / SECURITY

Cyberattacks are targeting US water systems, warns EPA and White House

The Municipal Water Authority of Aliquippa, PA (pictured) was targeted by a cyber attack last year. Image: AP Photo / Gene J. Puskar

/ States a
assess vulnerabilities at water
utilities following attacks linked to
the Chinese and Iranian
governments.

by Jess Weatherbed
Mar 20, 2024, 5:12 PM GMT+2

3 Comments (3 New)

posed Water PLCs Are Easy
Iran

ted Unitronics Devices

February 9, 2024

Tweet Share Credit Eligible Get Permission

Screen of a Unitronics device hacked in Aliquippa, Pennsylvania, on Nov. 25, 2023 (Image: Municipal Water Authority of Aliquippa)

Here's one reason why Iranian state hackers may have been able to target Israeli-made pressure-monitoring controllers used by American water systems: Nearly 150 of the controllers are exposed to the internet - and some still use the default password 1111

Unitronics Vision

- Unitronics vision is a PLC + HMI
- Vendor : Israel
- Uses PCOM communication protocol (proprietary protocol designed by Unitronics)
- Ok, how to hack it , We need to
  - Download the engineering workstation software (Visilogic)
  - Connect to the unitronics through the IP address
  - Authentication using password
  - Upload the new logic

The only way to connect the devices remotely is to be publicly facing the internet.

Indeed, this PLC is not facing the internet

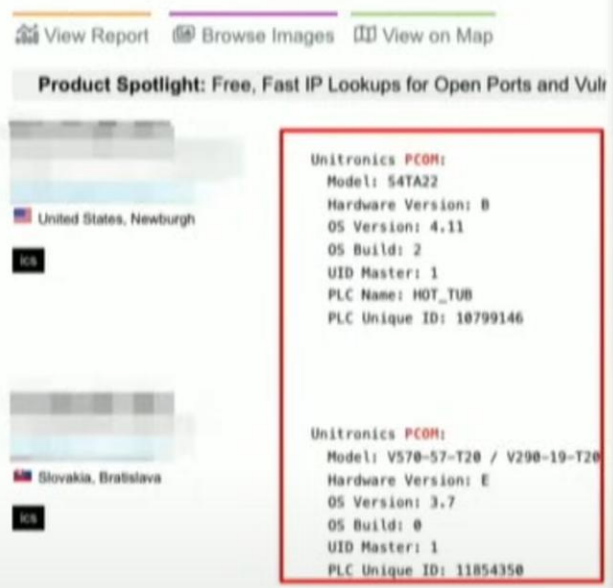
Right???

NO

How they get the IP address?

- there are **890 unitronics devices publicly facing the internet**
- Most of these device have **old version of PCOM** protocol which has no password protection

- Using shodan.io:
  - 900 devices
  - PCOM exported
- Unpatched devices have no authentication!



From Process to Cloud

Navigating ICS/OT Security in a Converged World

EG|CERT

NTRA
National Telecom Regulatory Authority

Chapter 1

ICS/OT Security

From Process to Cloud

- ICS/OT Environments
- ICS Architecture, Attacks and Threats
- Frameworks and Standards
- Defensive Architecture
- Incident Response and Monitoring

Chapter 1

ICS/OT Security

From Process to Cloud

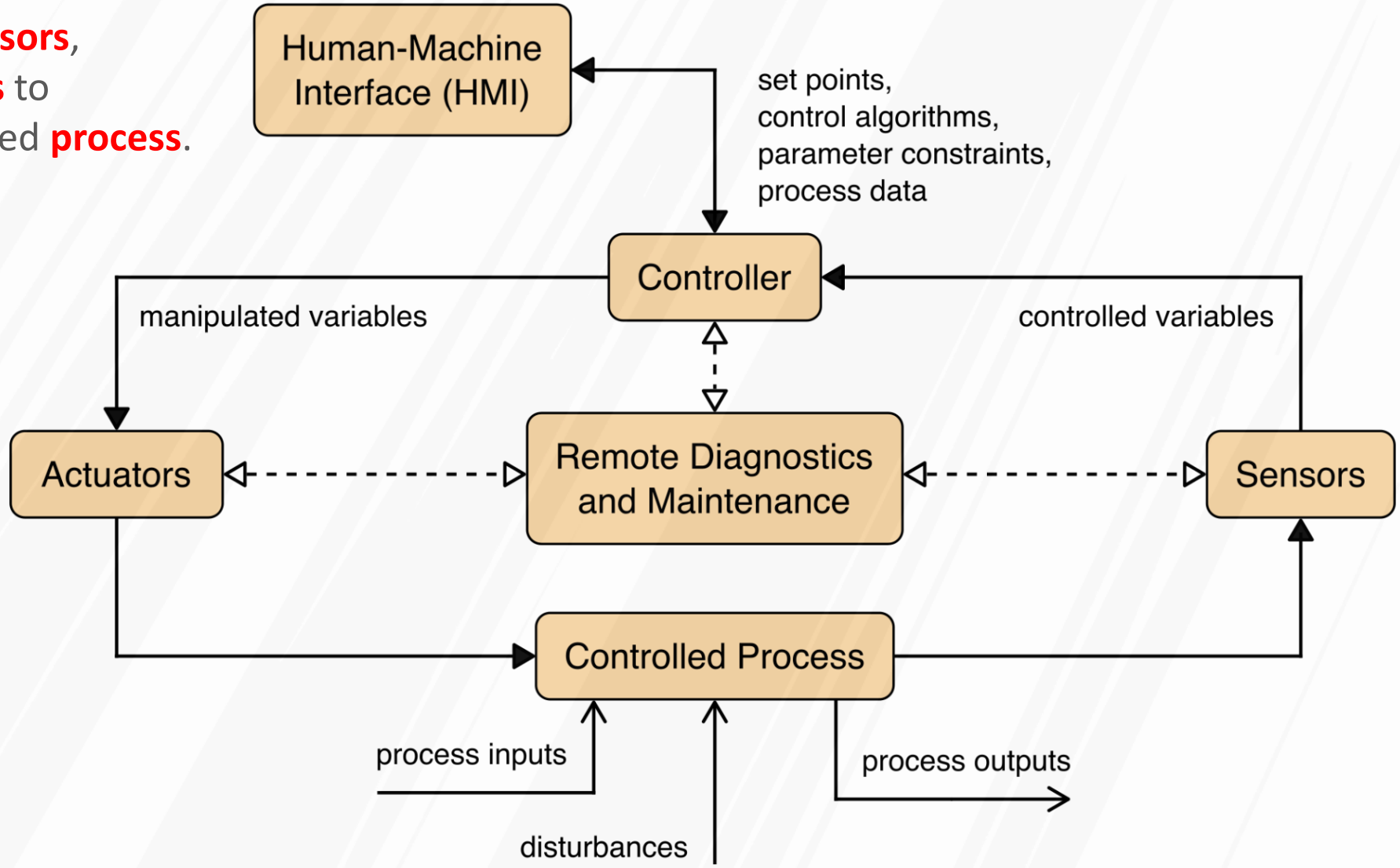
- ICS/OT Environments
- ICS Architecture, Attacks and Threats
- Frameworks and Standards
- Defensive Architecture
- Incident Response and Monitoring

EG|CERT

NTRA National Telecom Regulatory Authority

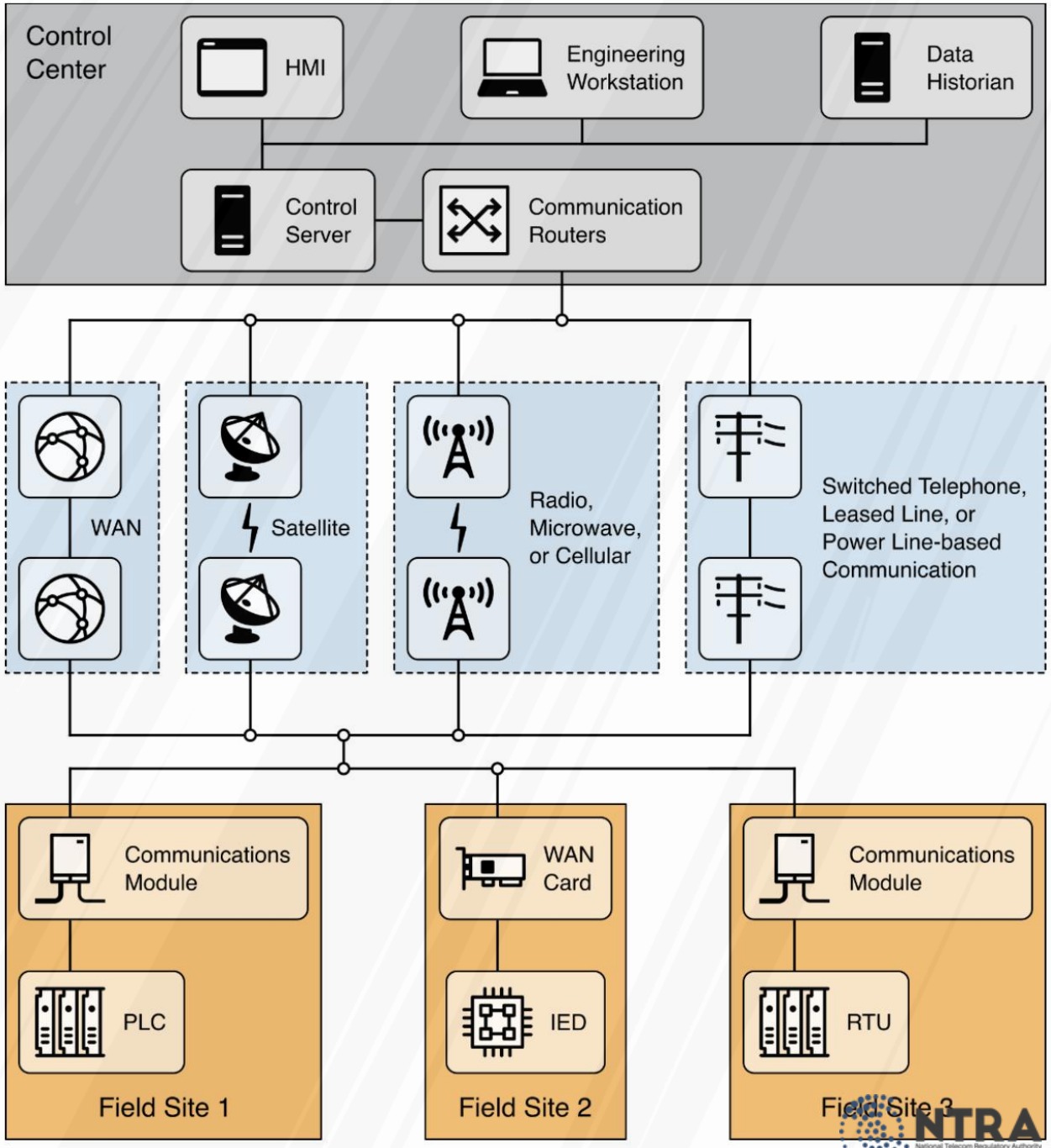
Typical OT system

- A control loop utilizes **sensors**, **actuators**, and **controllers** to manipulate some controlled **process**.



General SCADA system

- The control contains **control server** and the **communications routers**, **HMI**, **engineering workstations**, and the **data historian**,
- All of these components are connected by a **local area network (LAN)**.
- The control center
  - Collects and logs information [gathered by the field sites]
  - Displays information to the HMI
  - Generate actions based on detected events.
  - Responsible for centralized alarming,
  - Trend analyses
  - Reporting.



OT Vs IT System Security

Category	Information Technology (IT)	Operational Technology (OT)
Primary Concern	**Data protection** and **information security** (CIA triad).	**Safety, reliability**, and process **continuity**.
Systems Managed	Servers, databases, business apps, and user endpoints.	PLCs, RTUs, HMIs, sensors, and control systems.
Update Frequency	Frequent updates, patches, and upgrades.	**Rare updates** downtime must be minimized.
Tolerance to Downtime	Some downtime acceptable.	**Downtime can halt production** or cause hazards.
Protocols Used	Standard IT protocols (TCP/IP, HTTP, DNS).	Industrial protocols (**Modbus, DNP3, OPC UA**).
Lifecycle	Short (3–5 years typical).	Long (**10–20+** years operational).
Security Approach	Focus on confidentiality and integrity.	Focus on availability and safety.
Incident Impact	Data loss, financial loss, or reputation damage.	May cause equipment damage or safety hazards

Chapter 1

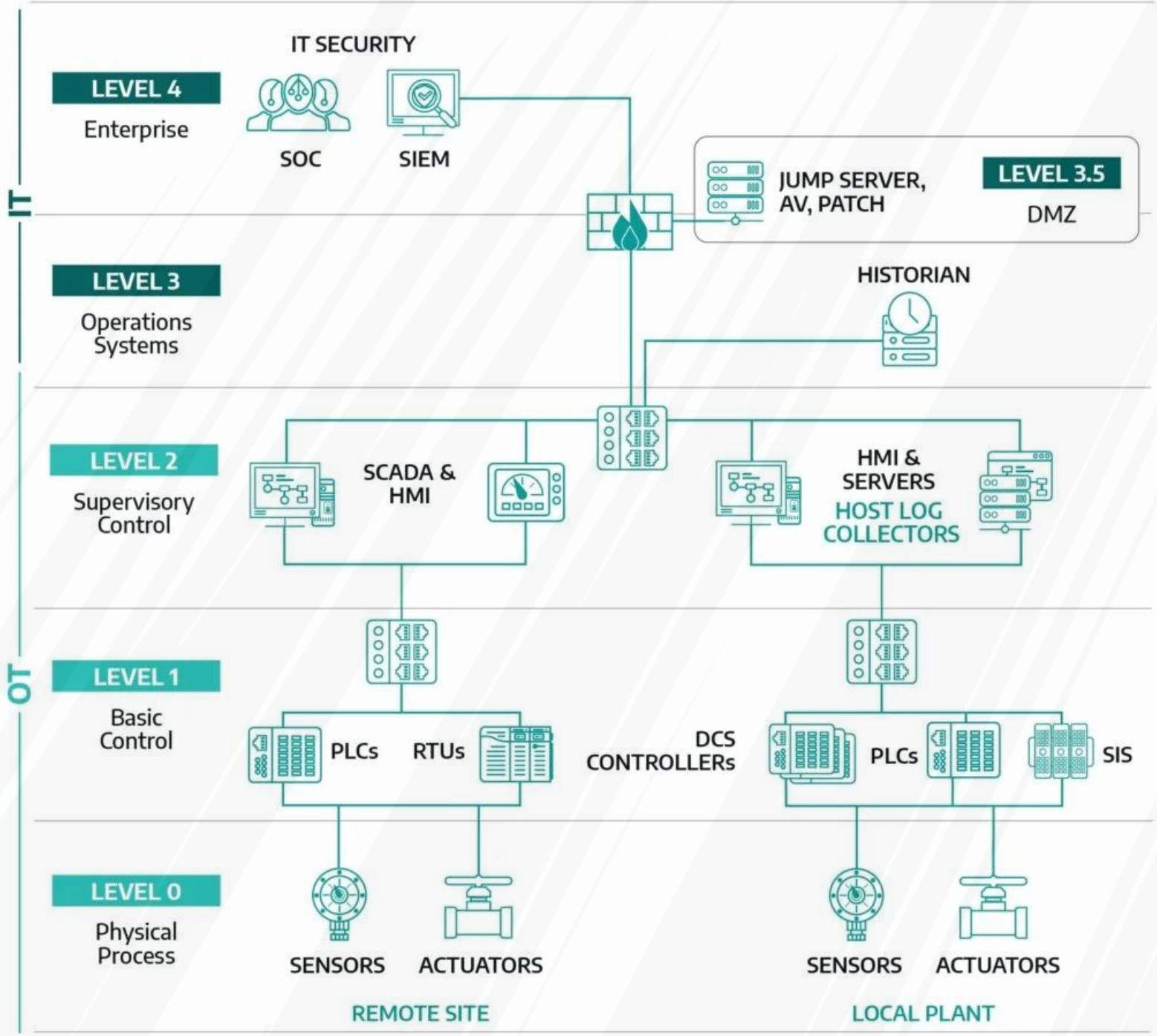
ICS/OT Security

From Process to Cloud

- ICS/OT Environments
- **ICS Architecture, Attacks and Threats**
- Frameworks and Standards
- Defensive Architecture
- Incident Response and Monitoring

Purdue Enterprise Reference Architecture

- Created in the early 1990s at Purdue University
- Used To define best practices for the relationship between industrial control systems and business networks
- Purdue levels are the most common security zone naming scheme used
- Purdue model is first and foremost a linguistical tool!!!
- Purdue Model have six network levels of the environment

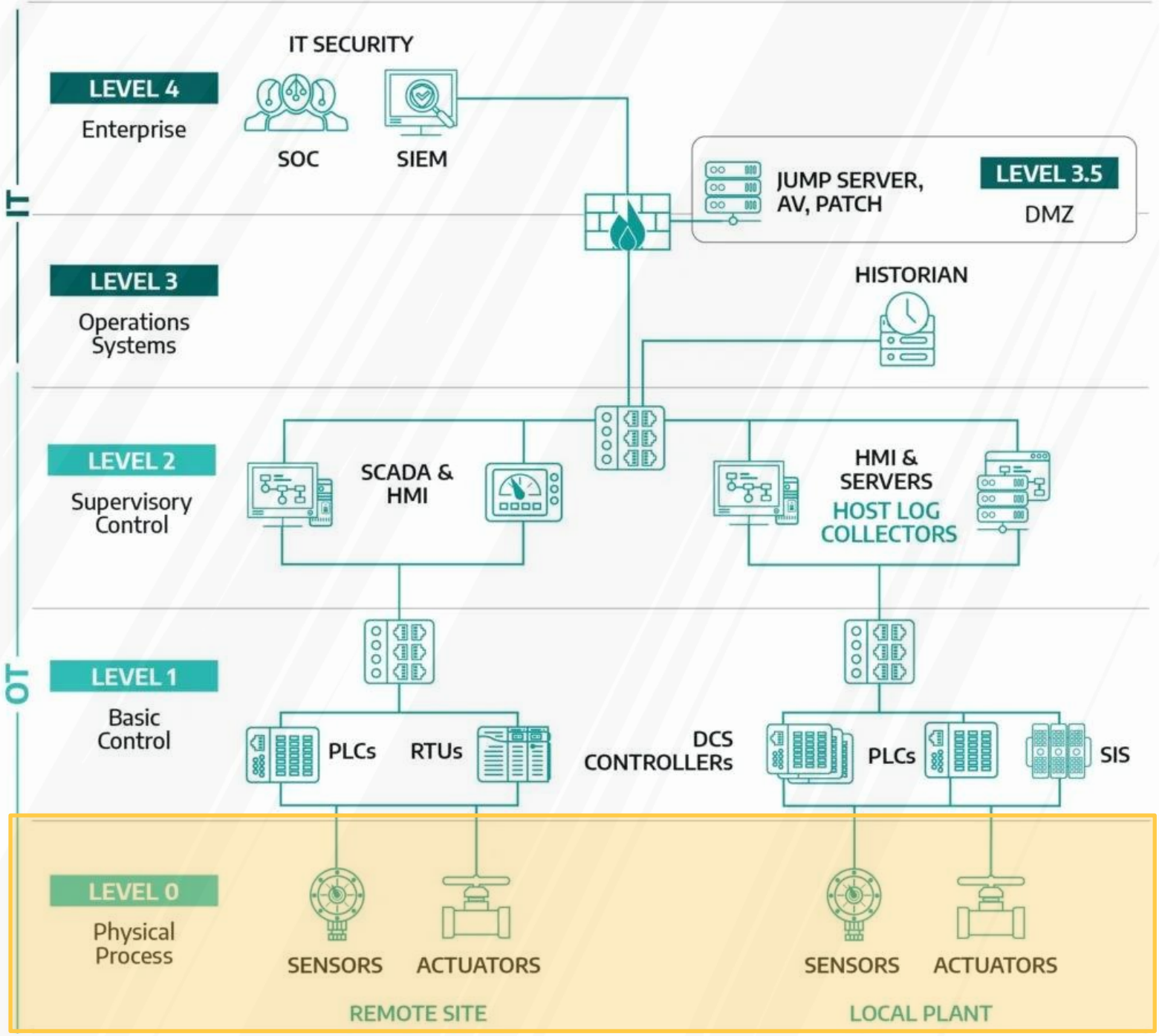


EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Physical Process

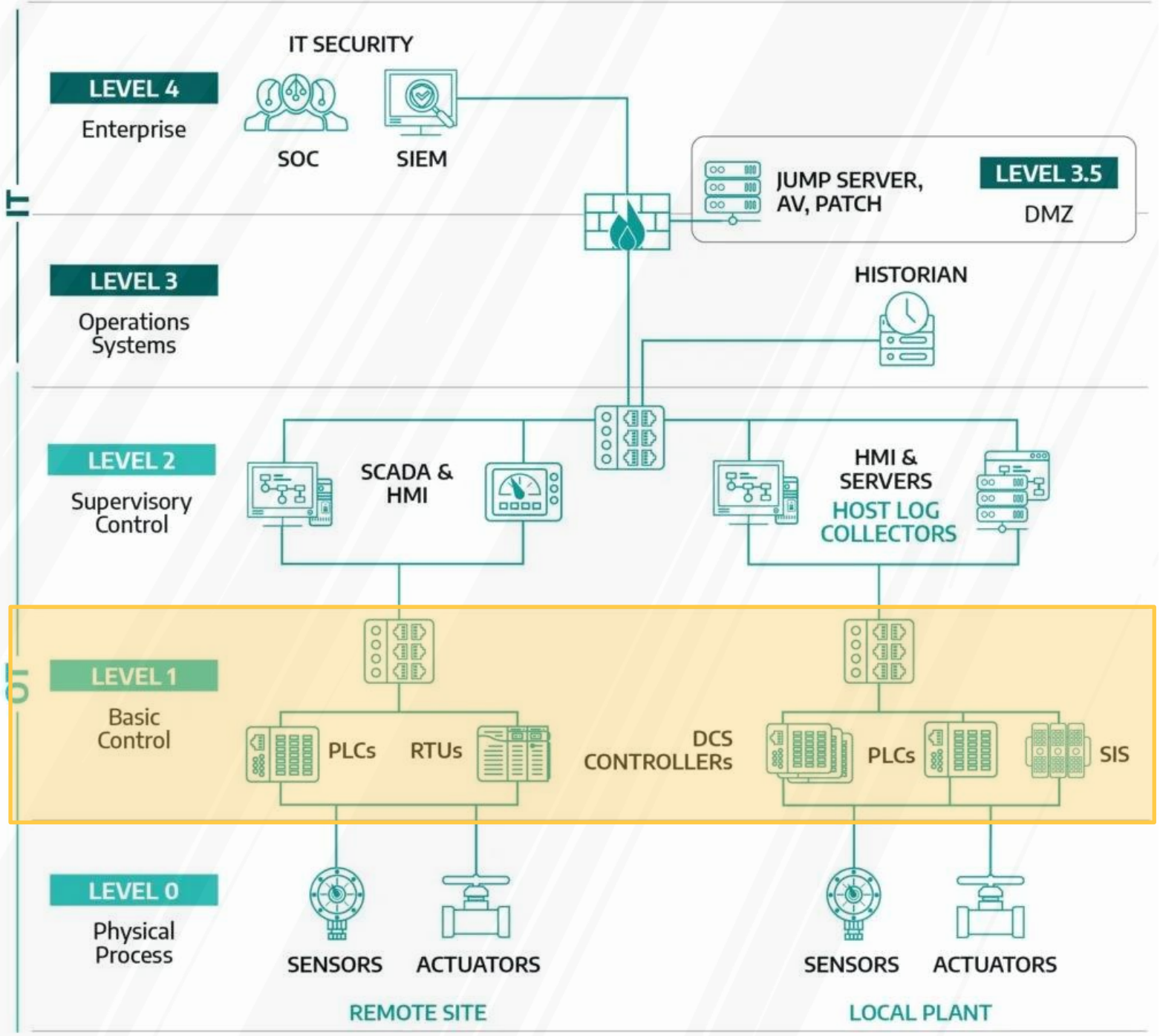
- Sensors and actuators for the cell, line, process, or DCS solution.
- Often combined with Level 1.
- This level includes:
  - Basic sensors and actuators
  - Smart sensors/actuators speaking fieldbus protocols
  - Intelligent Electronic Devices (IEDs)
  - Industrial Internet-of-Things (IIoT) devices
  - Communications gateways
  - Other field instrumentation



EG|CERT

Basic Control

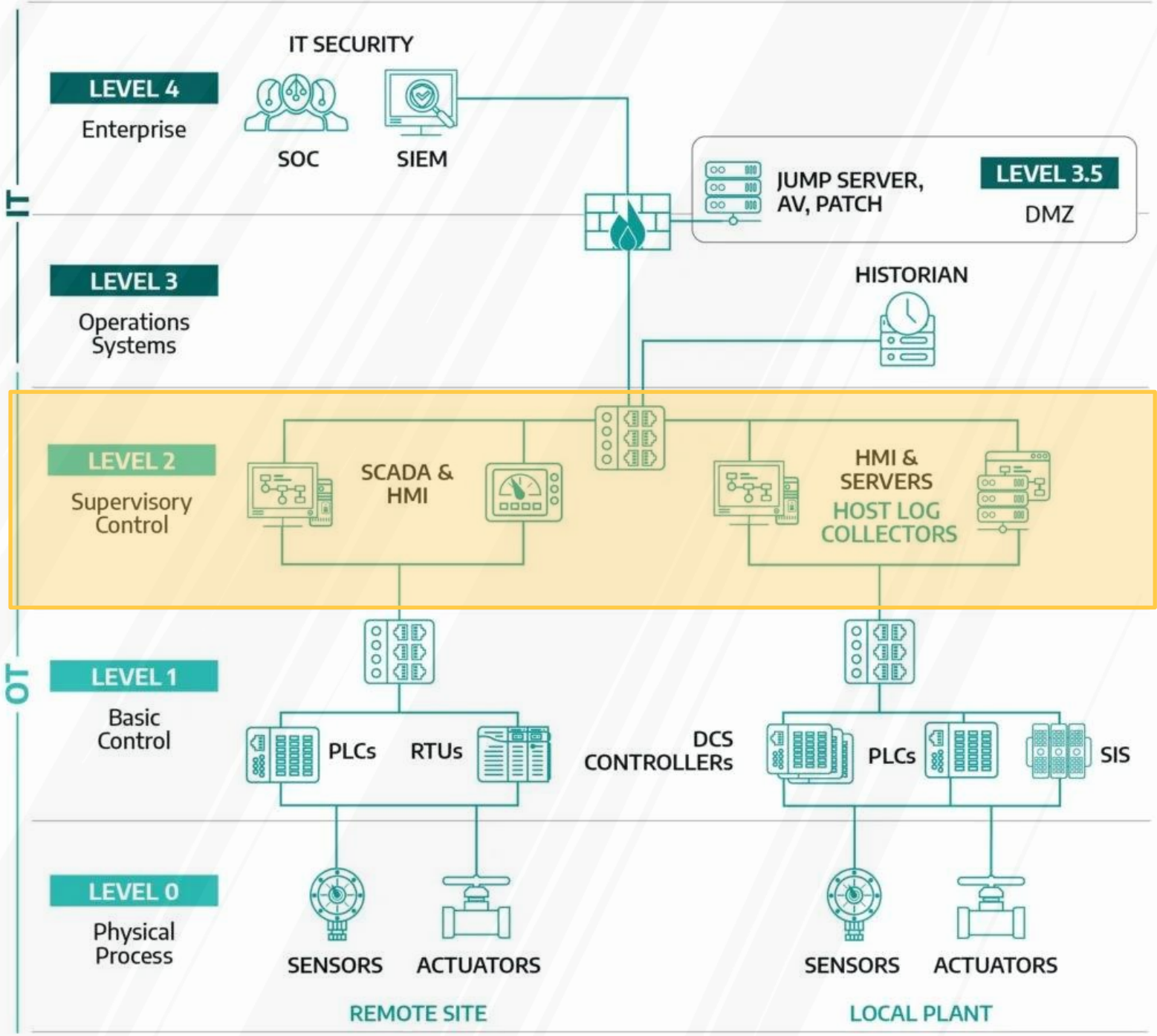
- Devices and systems to provide automated control of a process, cell, line, or DCS solution.
- Modern ICS solutions often combine Levels 1 and 0.
- This Level Includes:
  - Programmable Logic Controllers (PLCs)
  - Control processors
  - Programmable relays
  - Remote terminal units (RTUs)
  - Process-specific microcontrollers



EG CERT

Supervisory Control

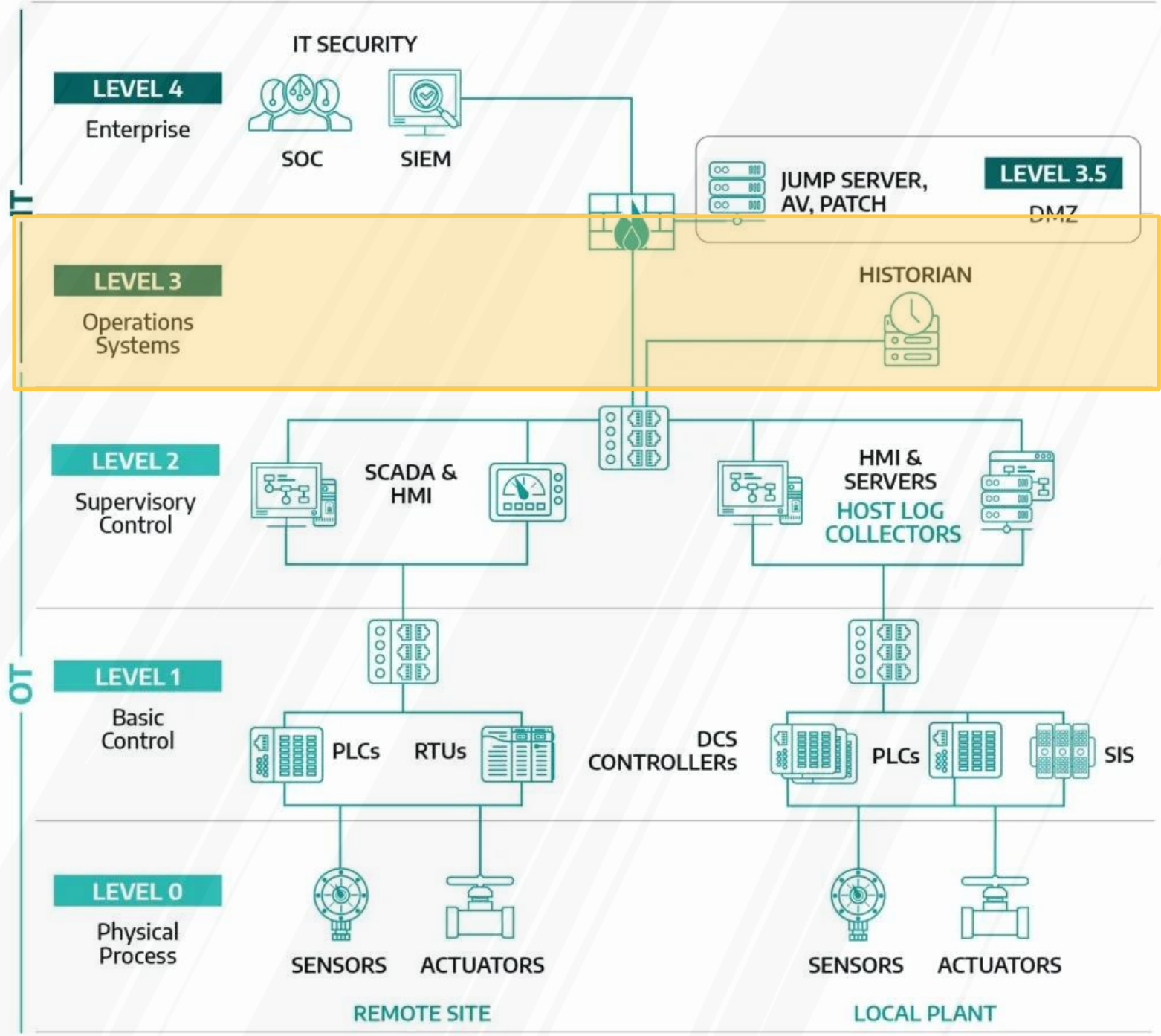
- Monitoring and supervisory control for a single process, cell, line, or distributed control system (DCS) solution. Isolate processes from one another, grouping by function, type, or risk.
- This level includes:
  - HMIs
  - Alarm servers
  - Process analytic systems
  - Historians
  - Control room (if scoped for a single process and not the site/region)



EG|CERT

Operation System

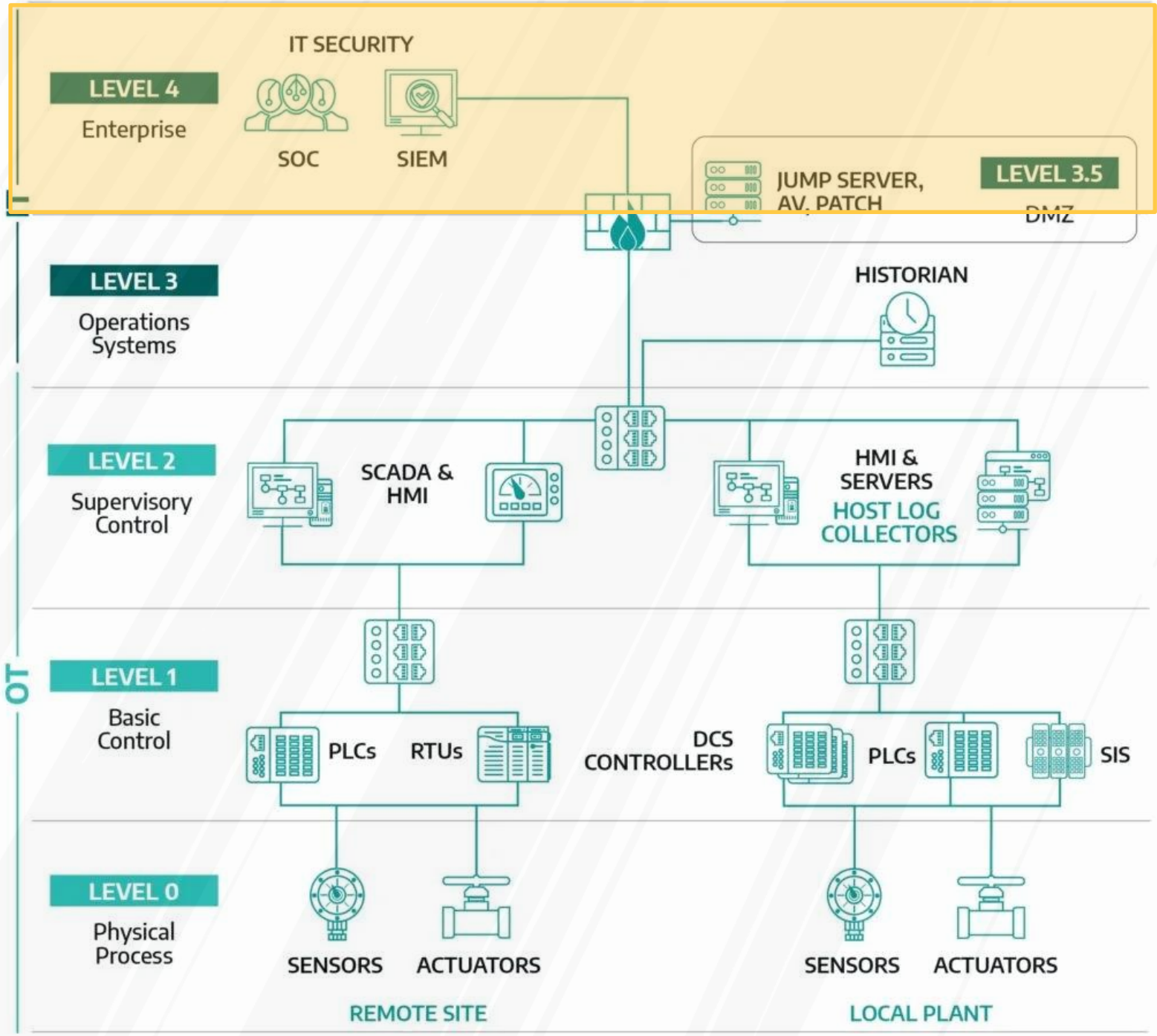
- Monitoring, supervisory, and operational support for a site or region.
- This level includes:
  - Management servers
  - Human-machine interfaces (HMIs)
  - Alarm servers
  - Analytic systems
  - Historians (if scoped for an
  - entire site or region)



EG CERT

Enterprise

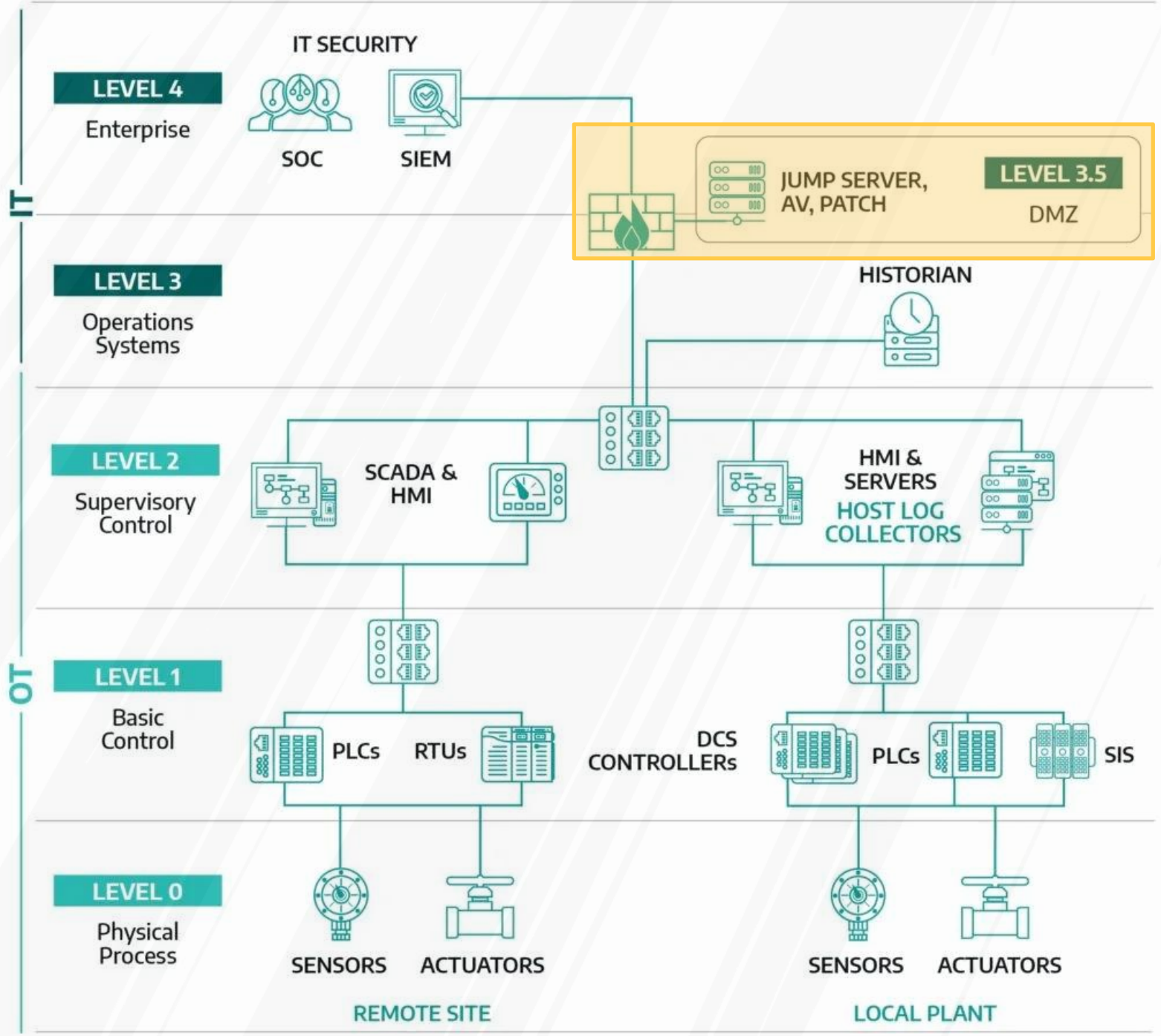
- IT networks for business users at local sites. Connectivity to Enterprise wide area network (WAN) and possibly local Internet access. Direct Internet access should not extend below this level.
- This level includes:
  - Business workstations
  - Local file and print servers
  - Local phone systems
  - Enterprise AD replicas



EG CERT

Enforcement Boundaries

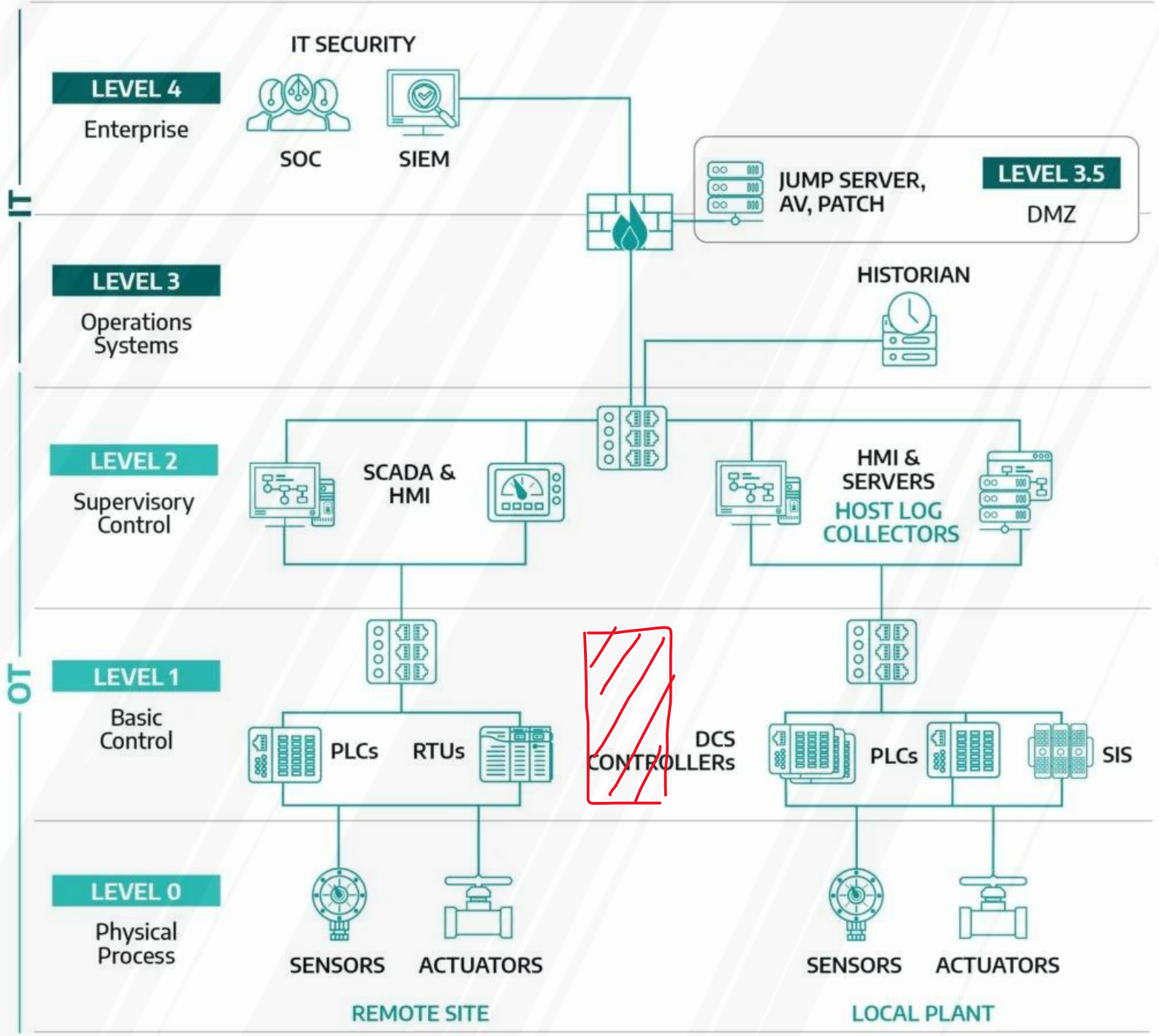
- Between some Purdue levels, we place enforcement boundaries.
- These includes the functions necessary to segment and protect the various Purdue levels within an ICS environment.
- Items typically found in this boundary include
  - Firewalls
  - outers (with ACLs)
  - Application firewalls
  - Data diodes.



EG CERT

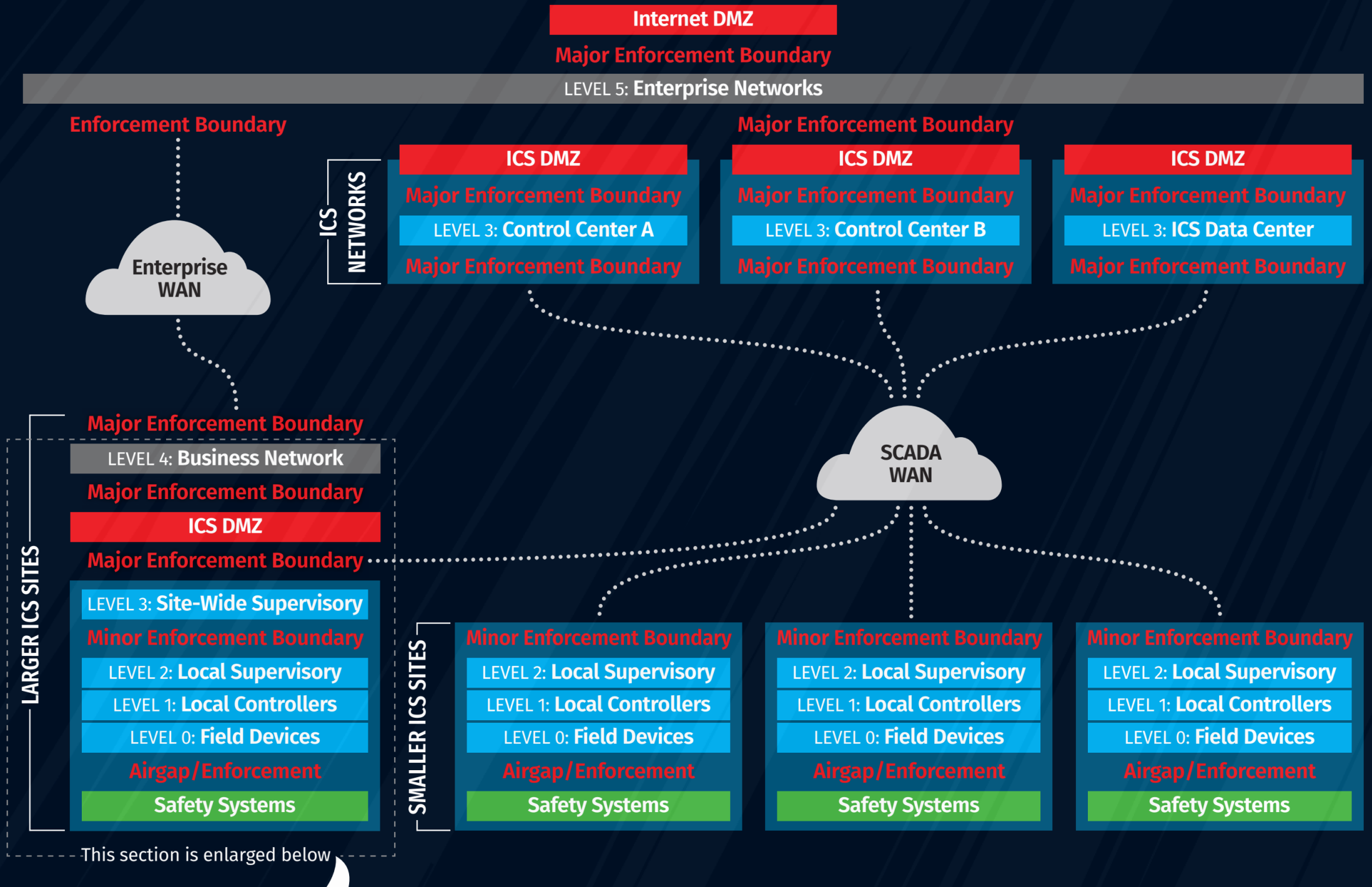
Problem with purdue model

- Each **level in the purdue** model has **different components, services, and functions**
- A **single Purdue level should contain multiple subnets** to prevent lateral movement
- **Network defenses** can be placed **between subnets in the same Purdue level**



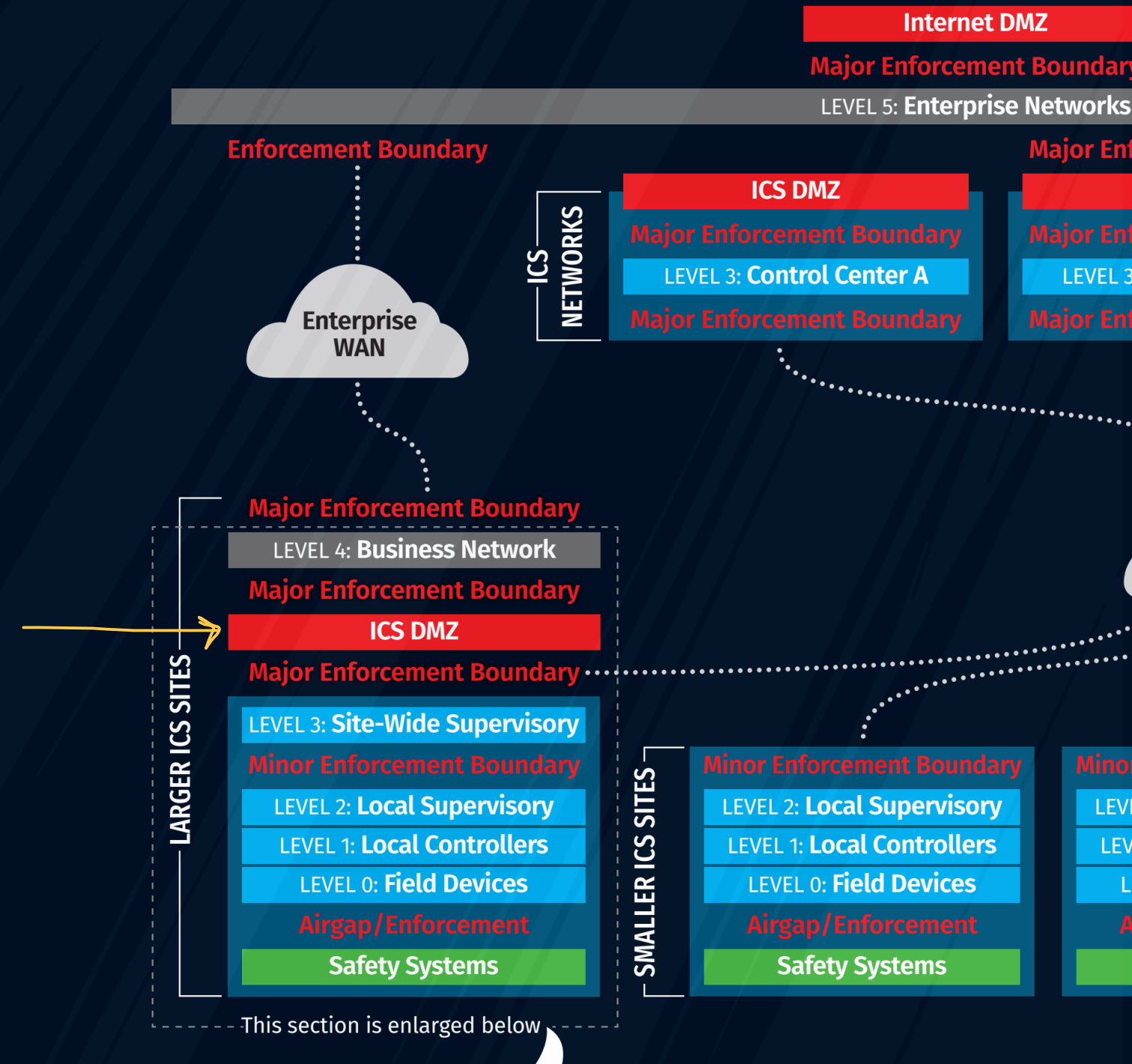
EG CERT

ICS 410 Model


Internet DMZ
Major Enforcement Boundary
LEVEL 5: Enterprise Networks
Enforcement Boundary
Major Enforcement Boundary
ICS NETWORKS
ICS DMZ
Major Enforcement Boundary
LEVEL 3: Control Center A
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LEVEL 3: Control Center B
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LEVEL 3: ICS Data Center
Major Enforcement Boundary
Enterprise WAN
SCADA WAN
Major Enforcement Boundary
LEVEL 4: Business Network
Major Enforcement Boundary
ICS DMZ
Major Enforcement Boundary
LARGER ICS SITES
LEVEL 3: Site-Wide Supervisory
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
This section is enlarged below
SMALLER ICS SITES
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems
Minor Enforcement Boundary
LEVEL 2: Local Supervisory
LEVEL 1: Local Controllers
LEVEL 0: Field Devices
Airgap/Enforcement
Safety Systems

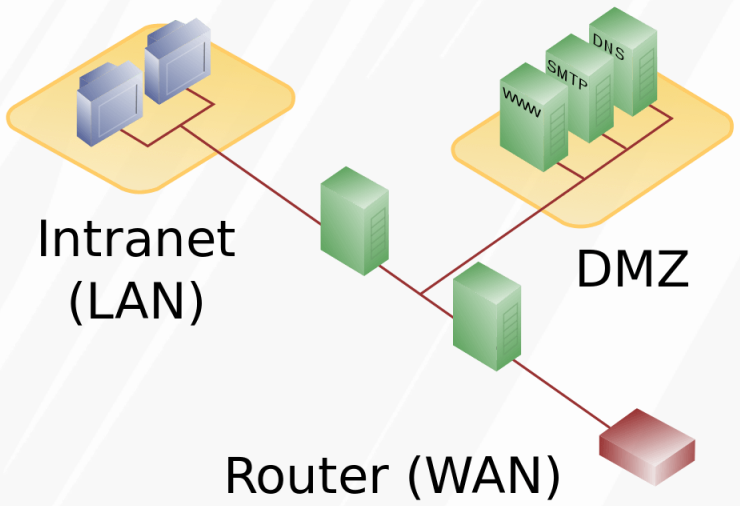
ICS DMZ

- ICS **DMZ allows you to inspect twice**
- DMZ **decrease** the chance of attacker's **bidirectional tunnels**
- ALL **inbound and outbound** traffic **must stop at a server** in the DMZ



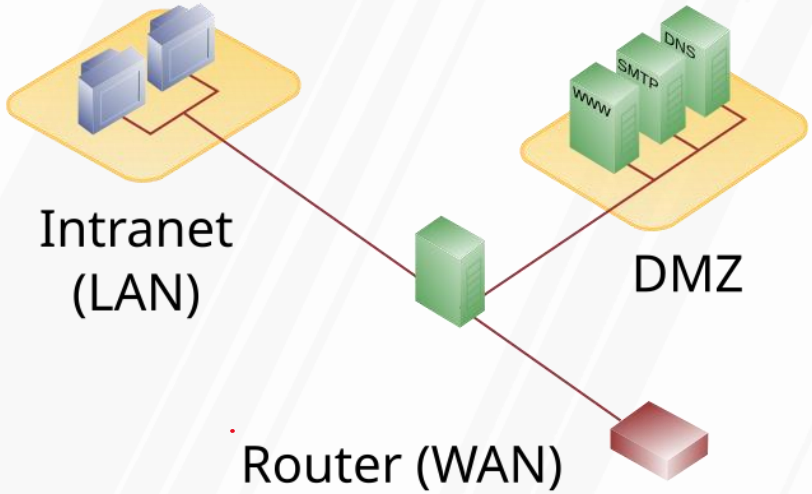
Two-firewall solution

- Two-firewall solution
  - Firewall rulesets **require all traffic to terminate in the Control System** DMZ
  - Allows **business and control to each manage a firewall**, even different vendors
  - **Often the best political decision**



Single-firewall solution

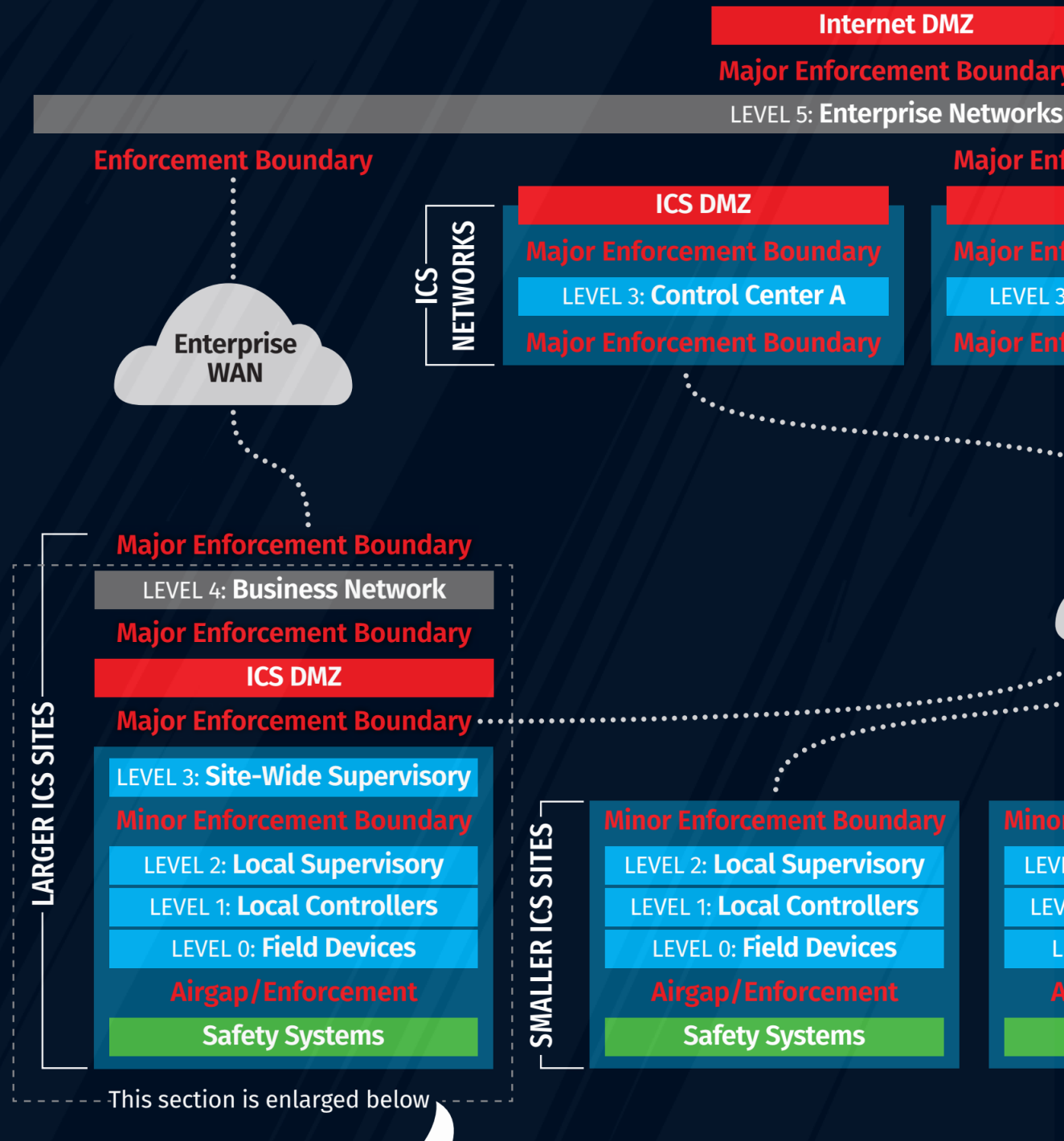
- • Single-firewall solution
  - **3-legged firewall** with Control System DMZ on a third port
  - **Managed from the Control System** side
  - **No rule permits traffic directly between business and control**



ICS DMZ

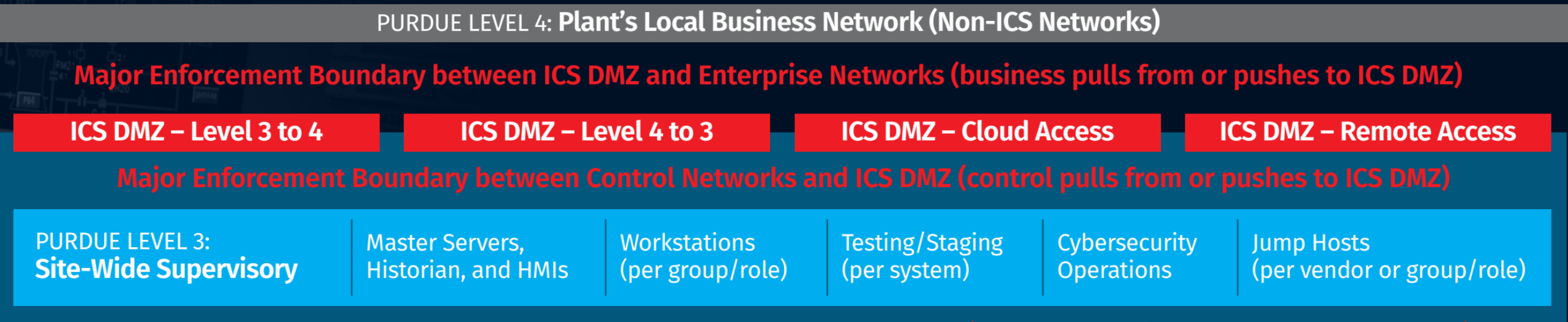
- The **most secure communications** should look like this
  - Inbound communication
    - Level 4/5 pushes to this DMZ
    - Level 3 pulls from it
  - Outbound communication
    - Level 3 pushes to this DMZ
    - Level 4/5 pulls from it

Larger sites can use **multiple DMZ** to separate traffic further and mitigate risk



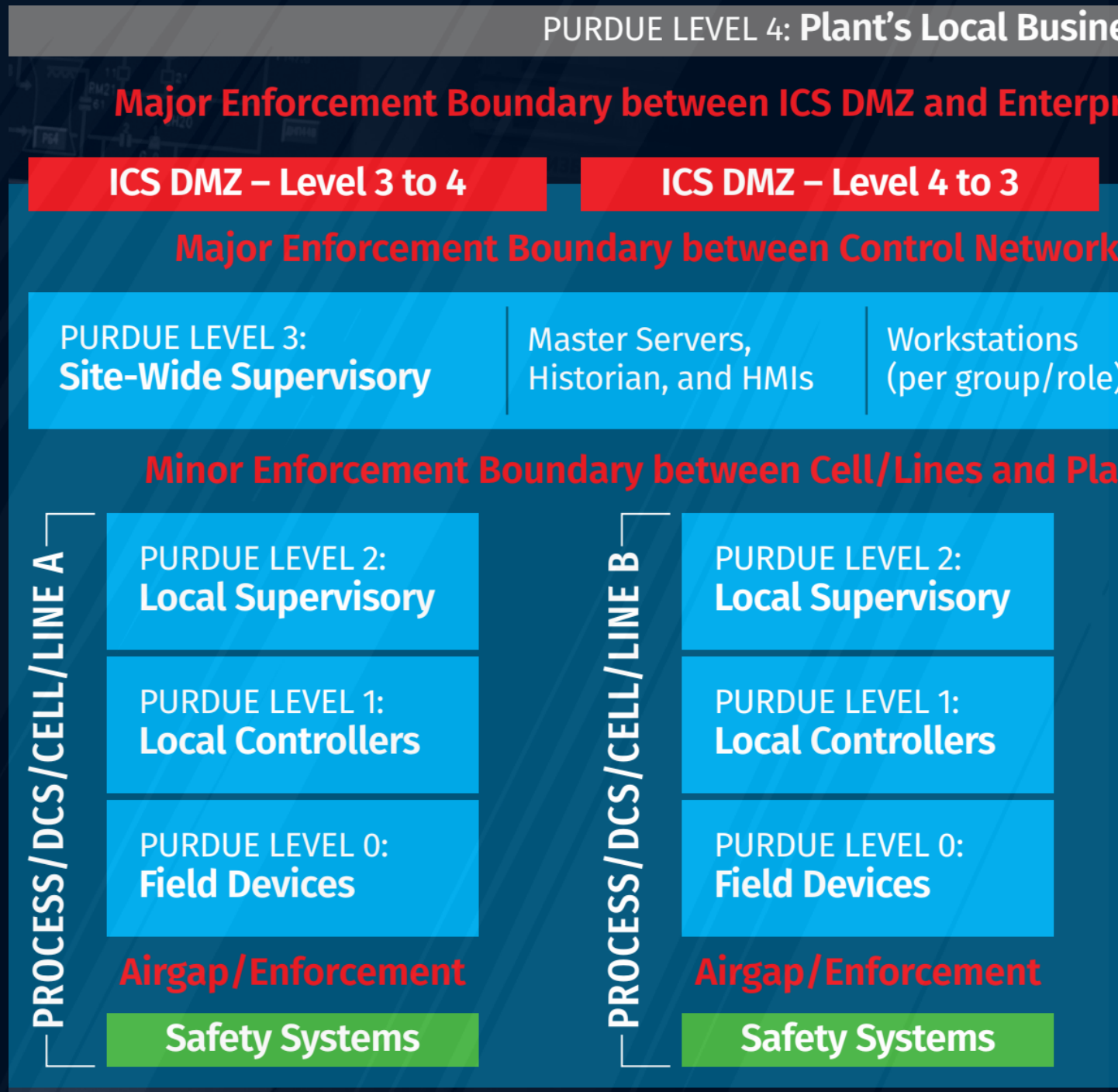
Level 3 Subnets

- **Level 3** should be **broken into multiple subnets**
- **Group systems by function** and role, which simplifies network security controls
- System **must have ICS cybersecurity operations subnet**
  - To manage SIEM, patches, and endpoint security solutions
  - Have ACLs to prevent compromise of this subnet from other Level 3 subnets
  - Patches and endpoint updates should be fed through ICS DMZ



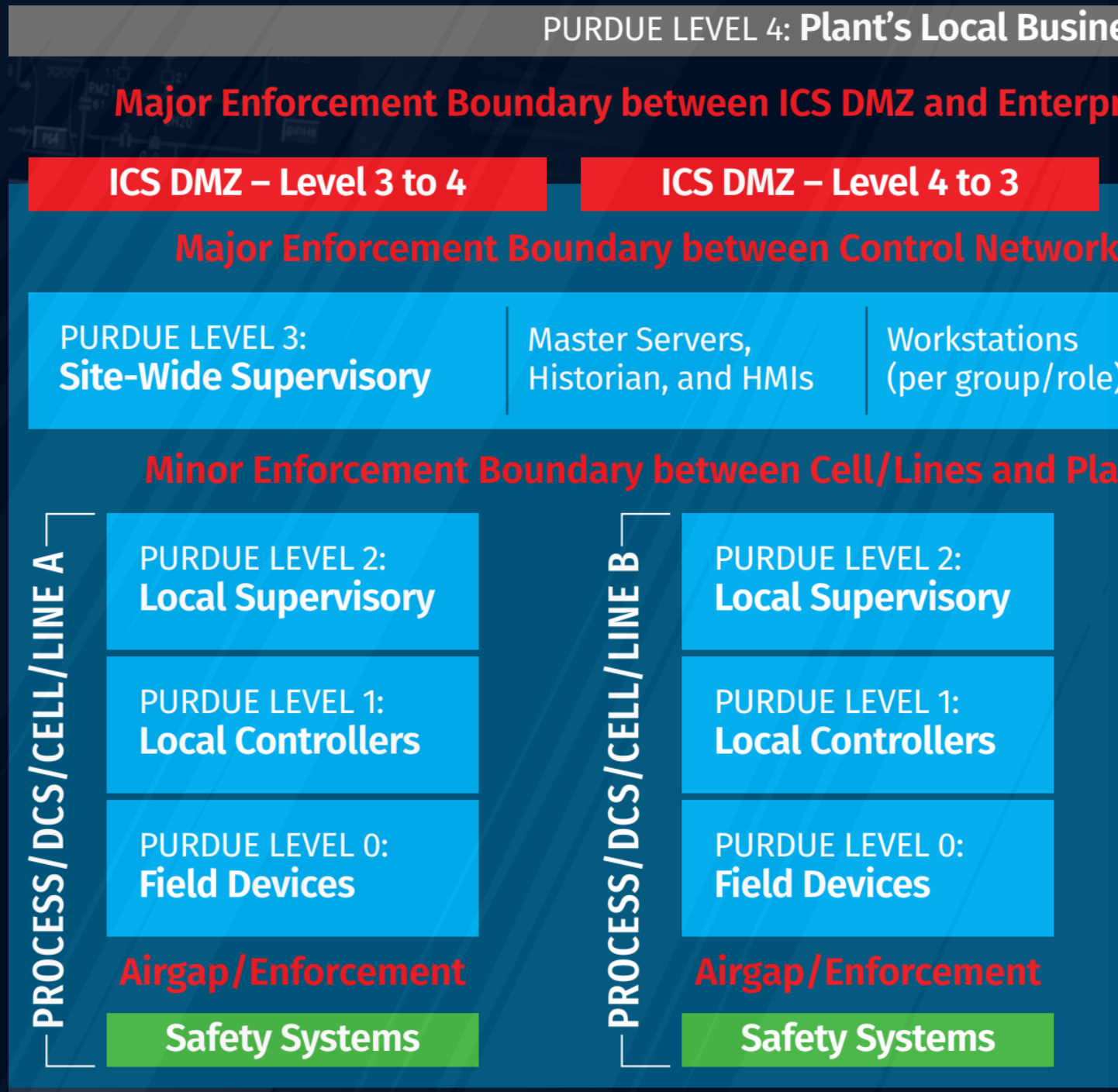
Level 3 and Processes

- Identify **major process groups** at each site
- Consider **minor enforcement** boundary between **Layer 2** and **Level 3**
- **Isolate any safety system** communication from the rest of the ICS network



Level 3 and Processes

- Each manufacturing cell, line, or **process should be able to operate** for a limited time **without communications to Level 3**
- This allows us to **island each process** in the case of **Level 3 compromise**.



Chapter 1

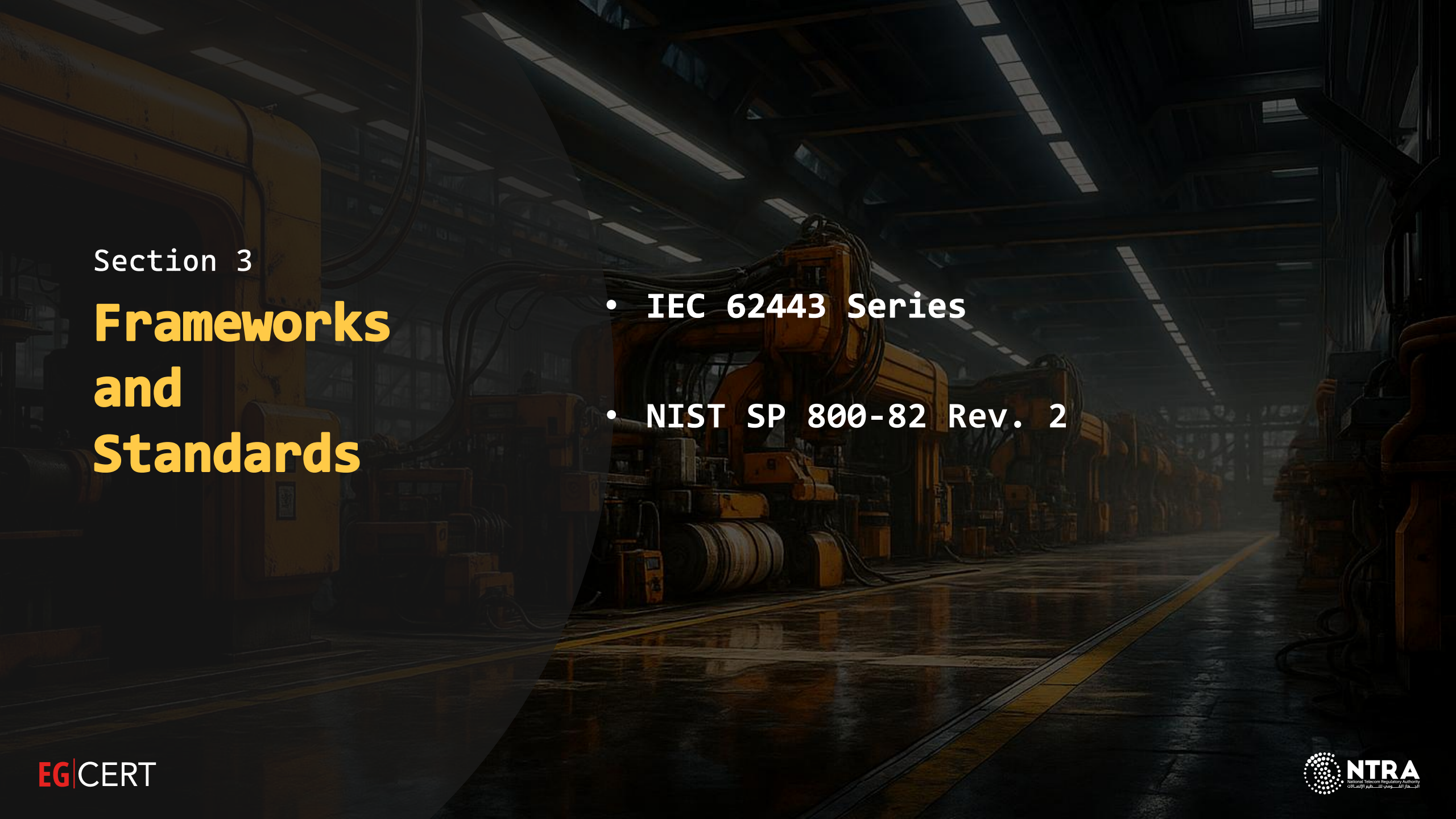
ICS/OT Security

From Process to Cloud

- ICS/OT Environments
- ICS Architecture, Attacks and Threats
- Frameworks and Standards
- Defensive Architecture
- Incident Response and Monitoring

EG|CERT

NTRA
National Telecom Regulatory Authority



Section 3

Frameworks and Standards

- IEC 62443 Series
- NIST SP 800-82 Rev. 2

Section 3

Frameworks and Standards

- IEC 62443 Series
- NIST SP 800-82 Rev. 2

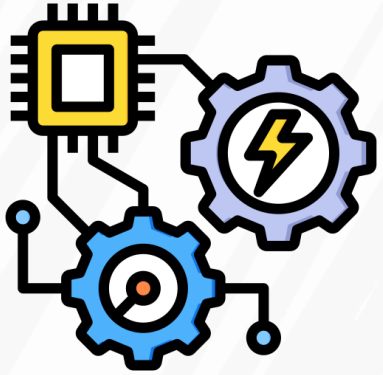
IEC 62443 Series

- IEC 62443 is designed to reduce the risk of deploying and operating an Industrial Automation Control System “IACS”.
- provides a realistic and achievable model to mitigate security threats.
- define the roles of organizations, the policies and processes which are applicable to each one

Roles of Organizations

Asset Owner

Individual or Organisation responsible for one or more IACSs Typically the Asset Owner is the end user.



System Integrator

builds IACSs for the Asset Owners by integrating hardware and software from multiple Product Manufacturers.

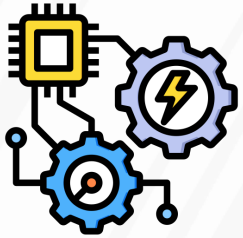
Product Manufacturer

designs and creates the individual components that the System Integrator uses to build the automation system.

How IEC62443 helps each stakeholder

Asset Owner

- IEC 62443 enables Asset Owners to define a required security level, with reference to a threat level
- Asset owner don’t have to define the security function required from each individual component.
- If a network already exists
  - the Asset Owner can use the standard as a benchmark to determine the current security level.



System Integrator

- IEC62443 provides an unambiguous statement of the Asset Owner's security requirements.
- offers confirmation that the IACS meets the required security level.

Product Manufacturer

- IEC62443 offers a simple way to describe the security functionality of the product.
- Which is much better than a long list of features.
- It also offers an easy way for customers to compare products from different manufacturers.

EG|CERT

NTRA

IEC 62443 Series 4 categories

GENERAL

IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	IEC 62443-1-4
Concepts and models	Master Glossary of Topics and Abbreviations	System security compliance metrics	IACS Security Lifecycle and Use Cases

POLITICS AND PROCEDURES

IEC 62443-2-1	IEC 62443-2-2	IEC 62443-2-3	IEC 62443-2-4
Requirements for the IACS security management system	Implementation guide for the IACS security management system	Patch management in the IACS environment	Requirement for IACS Solution Providers

SYSTEM

IEC 62443-3-1	IEC 62443-3-2	IEC 62443-3-3
Security technologies for IACS	Evolution of security risks and system design	System security requirements and security levels

COMPONENTS

IEC 62443-4-1	IEC 62443-4-2
Product development requirements	Safety technical requirements for IACS components

Additional Relevant BV Services

- Management system services, e.g. ISO 27001
- Security Testing / Requirement of .....

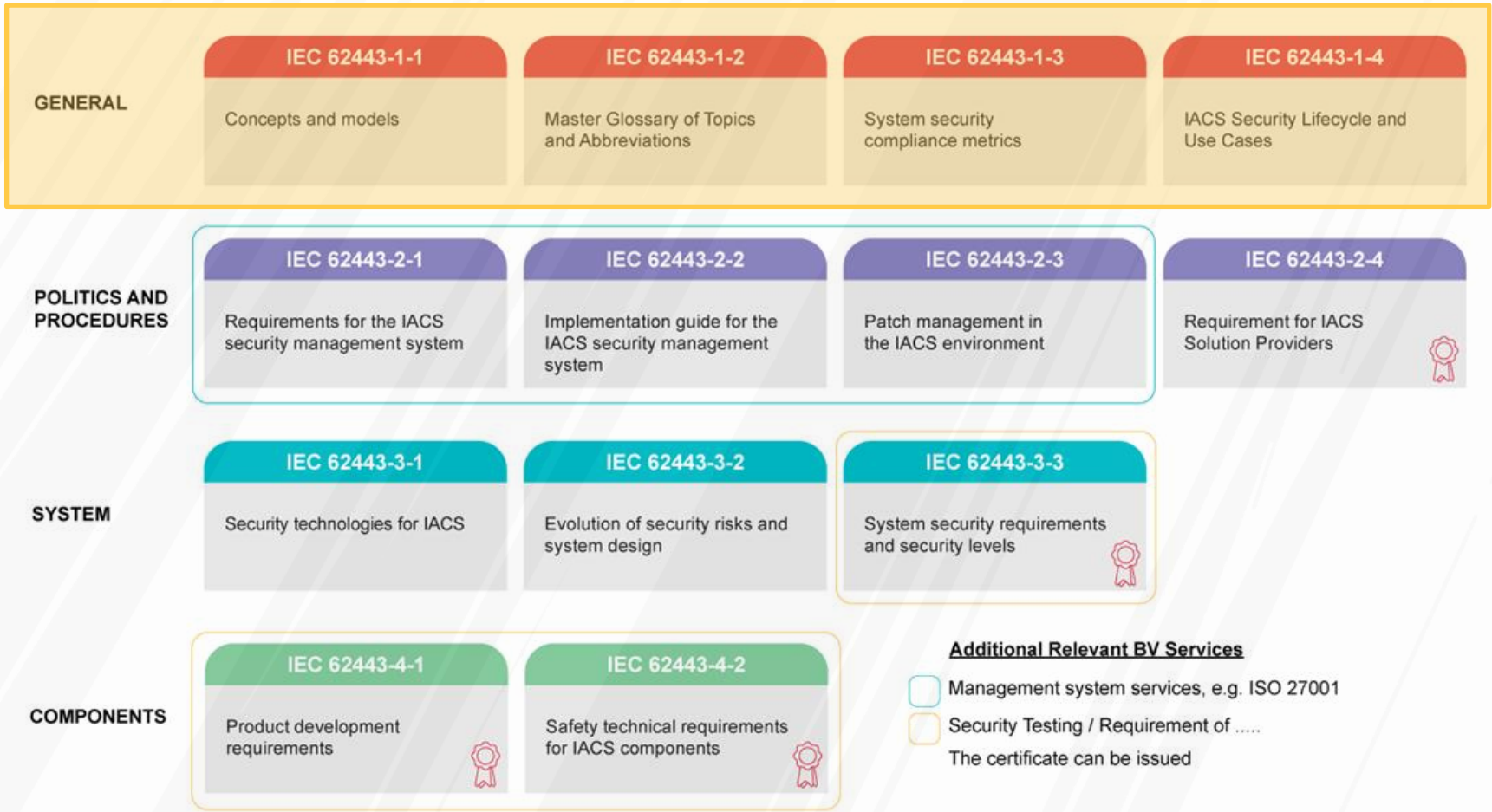
The certificate can be issued

EG CERT

NTRA National Telecom Regulatory Authority

General

- The General standards provide an overview of the IEC 62443 security process, and introduce concepts which are found throughout the series of standards.
- They form the foundation for the other categories.

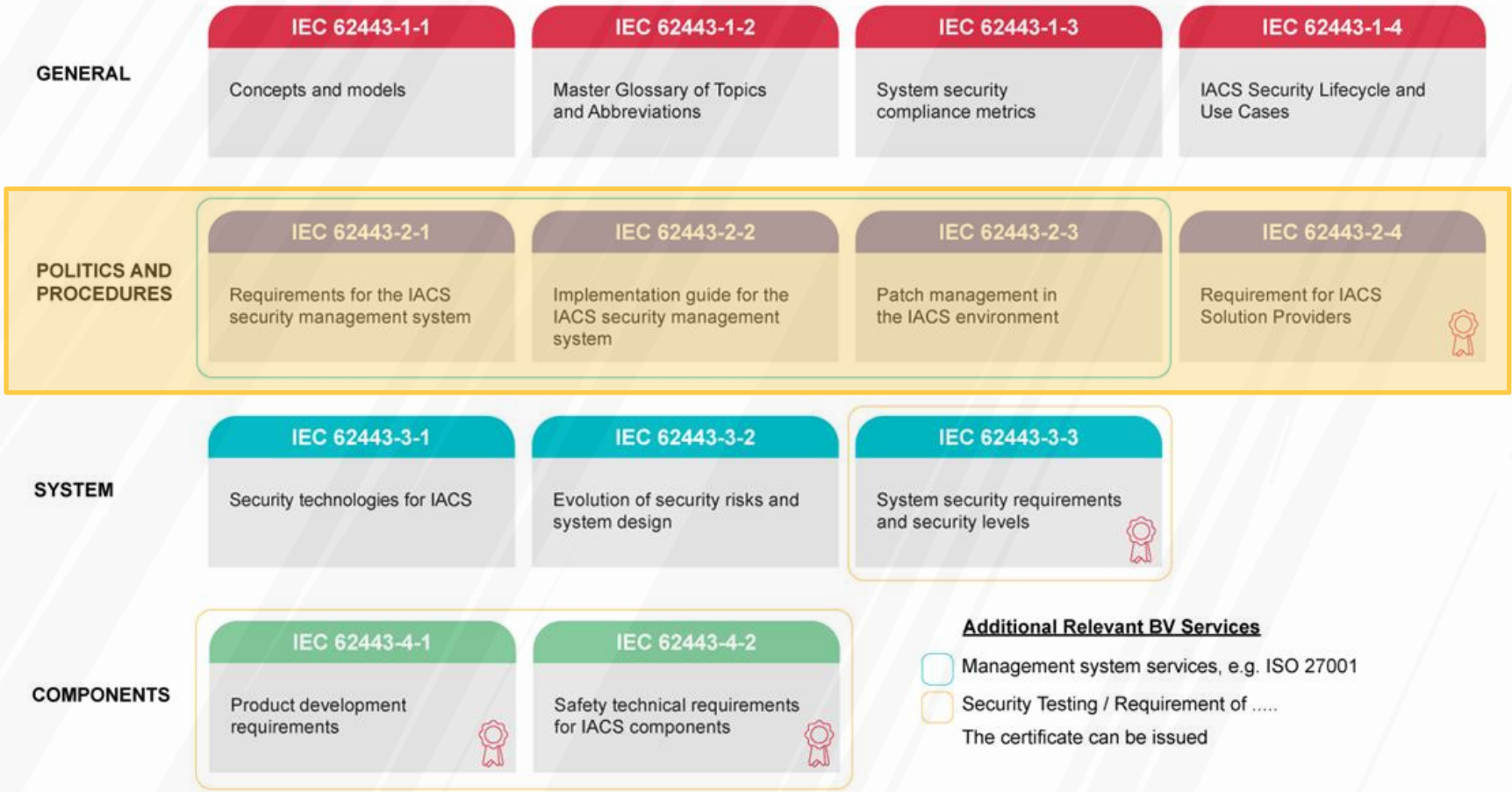


EG CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Policies and Procedures

- The Policies and Procedures standards provide guidance on creating and maintaining a secure system, including security policies and risk management.

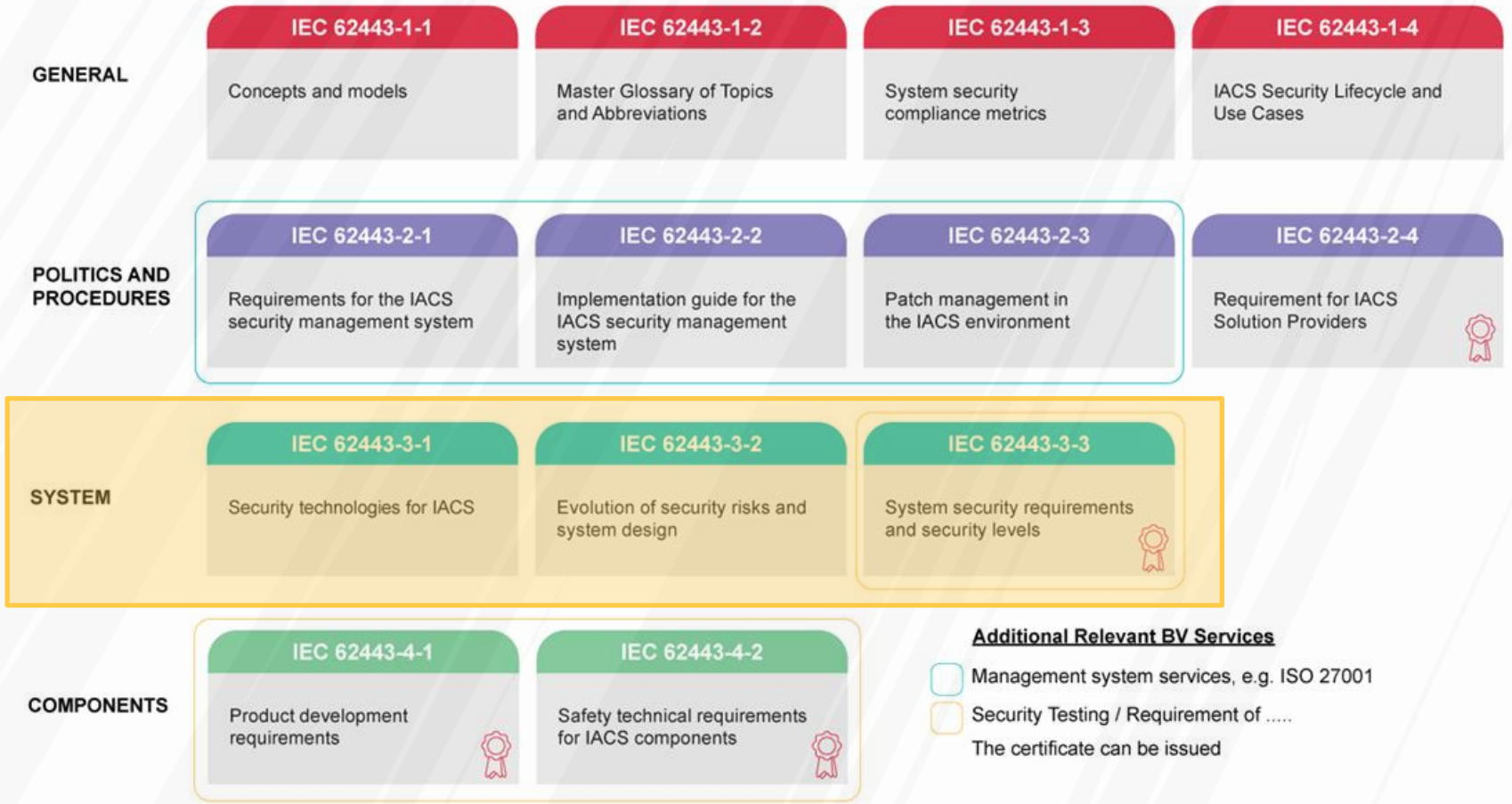


EG CERT

NTRA

System

- The System standards provide guidance on designing and implementing a secure IACS, including cyber security technologies and mitigation methods.

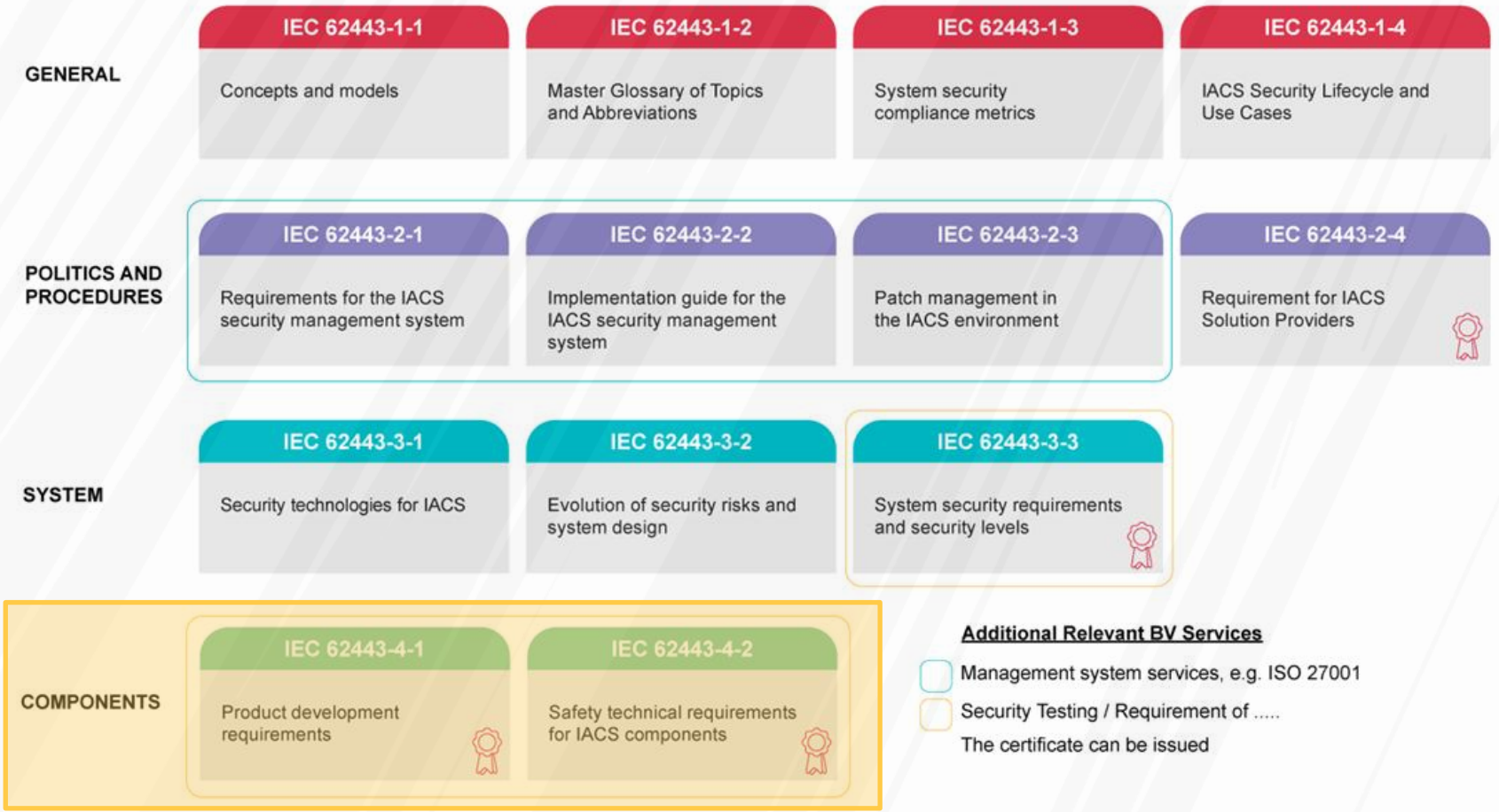


EG CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

Component

- The Component standards describe the development life cycle requirements and technical functionality levels for industrial network components.



EG CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

IEC 62443 Series 4 categories

		IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3	IEC 62443-1-4
	GENERAL	Concepts and models	Master Glossary of Topics and Abbreviations	System security compliance metrics	IACS Security Lifecycle and Use Cases
Asset Owner	**POLITICS AND PROCEDURES**	IEC 62443-2-1: Requirements for the IACS security management system	IEC 62443-2-2: Implementation guide for the IACS security management system	IEC 62443-2-3: Patch management in the IACS environment	IEC 62443-2-4: Requirement for IACS Solution Providers
System Integrator	**SYSTEM**	IEC 62443-3-1: Security technologies for IACS	IEC 62443-3-2: Evolution of security risks and system design	IEC 62443-3-3: System security requirements and security levels	
Product Manufacturer	**COMPONENTS**	IEC 62443-4-1: Product development requirements	IEC 62443-4-2: Safety technical requirements for IACS components		

Additional Relevant BV Services

- Management system services, e.g. ISO 27001
- Security Testing / Requirement of .....

The certificate can be issued

IEC 62443 Series 4 categories

		IEC 62443-1-1	IEC 62443-1-2	IEC 62443-1-3
	GENERAL	Concepts and models	Master Glossary of Topics and Abbreviations	System security compliance metrics
Asset Owner	POLITICS AND PROCEDURES	IEC 62443-2-1: Requirements for the IACS security management system	IEC 62443-2-2: Implementation guide for the IACS security management system	IEC 62443-2-3: Patch management in the IACS environment
System Integrator	SYSTEM	IEC 62443-3-1: Security technologies for IACS	IEC 62443-3-2: Evolution of security risks and system design	IEC 62443-3-3: System security requirements and security levels
Product Manufacturer	COMPONENTS	IEC 62443-4-1: Product development requirements	IEC 62443-4-2: Safety technical requirements for IACS components	

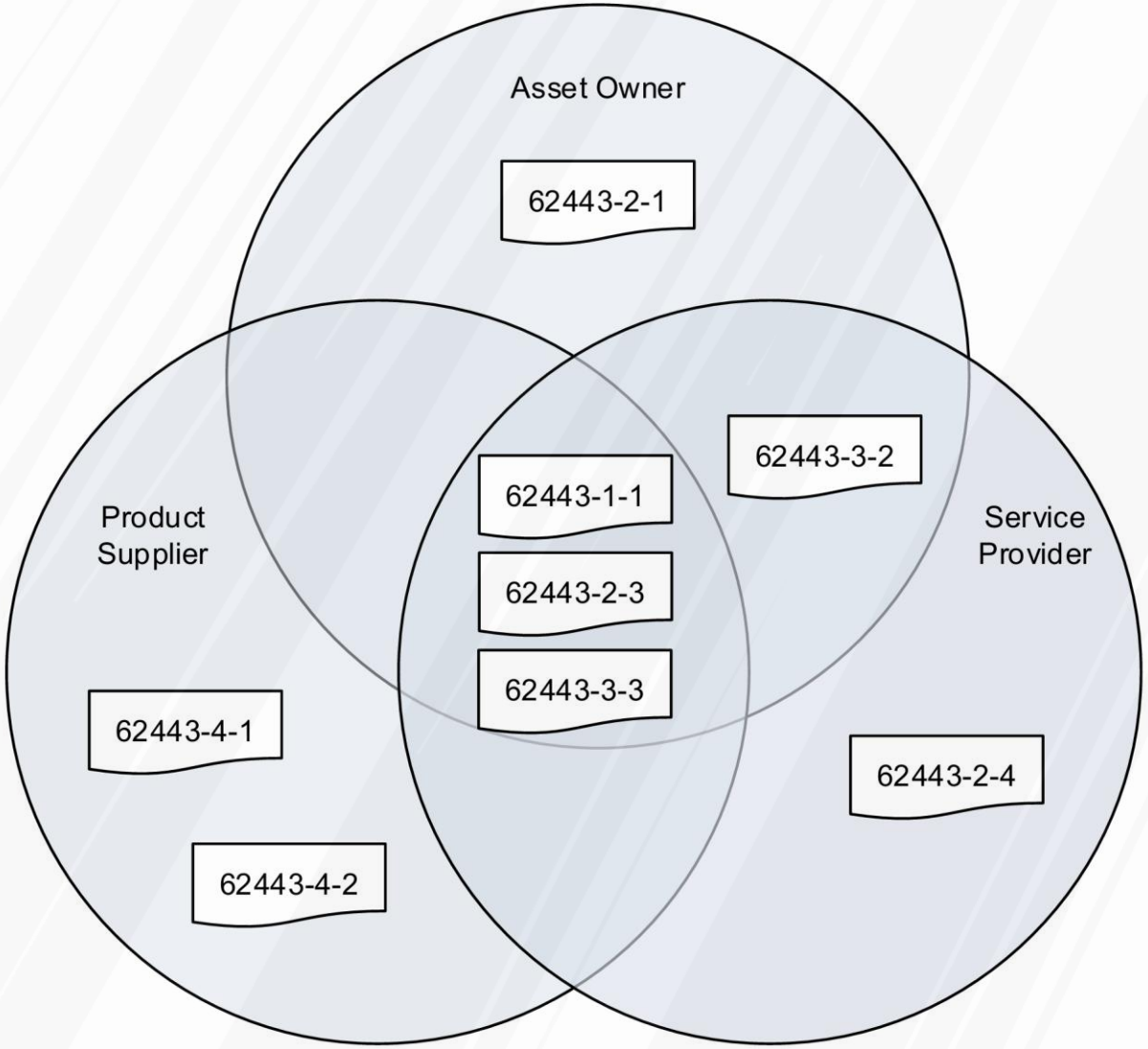
Additional Relevant B
- Management system se
- Security Testing / Requi

The certificate can be is

requirements

solution

IEC 62443 Series 4 categories



Security levels

- Level of security functionality provided by a component.
- IEC 62443-4-2 (components) includes 4 security levels
- The Security level matchs to the skills, resources, knowledge and motivation of an attacker
- This allows products to be selected based on the threat level from an adversary.

Security Level (SL)	Misuse	Means	Resources	Knowledge	Motivation
SL0 (no security)	—	—	—	—	—
SL1	Accidental	—	—	—	—
SL2	Intentional	Simple	Few	General	Low
SL3	Intentional	Complex	Moderate	IACS-specific	Moderate
SL4	Intentional	Complex	Extensive	IACS-specific	High

- Security levels are based on the concept of requirements

Types of Security levels

- **Target Security Levels (SL-T)**
  - the desired level of security for a particular Automation Solution.
  - Define how much protection the Asset Owner needed to protect the system
  - An Asset Owner determines and documents the appropriate SL-T in Cybersecurity Requirements Specification.
- **Capability Security Levels (SL-C)**
  - The native technical security countermeasures available within a system
- **Achieved Security Levels (SL-A)**
  - The actual, measured SLs for a particular Automation Solution
  - Determined after the Automation Solution is in operation.

Security Requirements

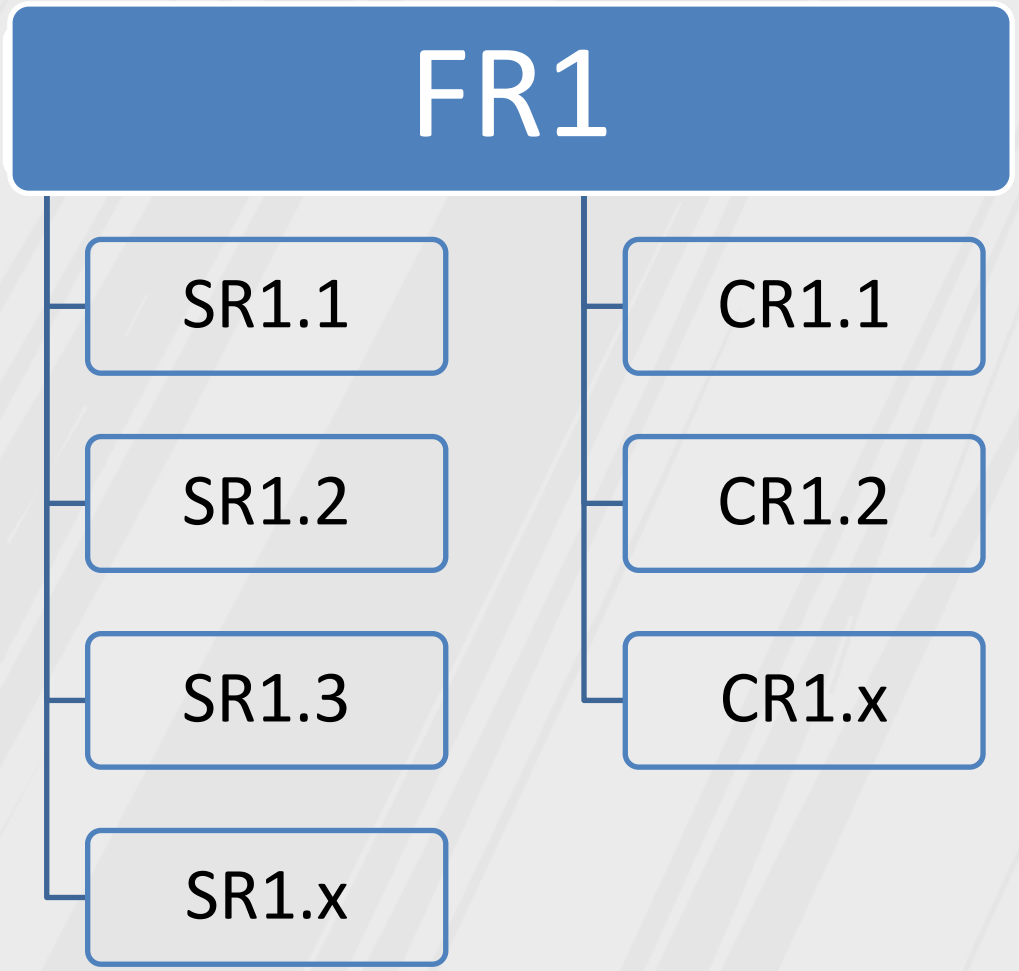
- A Corrective process (mitigation , policy, etc.) for a specific security weakness
- Security Requierments can be categorized into 3 categories
  - Foundational
  - System
  - Component.
- Each category maps to the security levels defined in the standard

The 7 Foundational Requirements

No.	Name	Label	Description
FR-1	**Identification and Authentication Control**	**IAC**	The Asset or Control System (ACS) shall provide the necessary capabilities to reliably identify and authenticate all users (humans, software processes, and devices) attempting to access the ICS.
FR-2	**Use Control**	**UC**	Asset or Control System (ACS) shall provide the necessary capabilities to enforce the assigned privileges of an authenticated user (human, software process, or device) to perform the requested action on the system or assets and monitor the use of these privileges.
FR-3	**System Integrity**	**SI**	Asset or Control System (ACS) shall provide the necessary capabilities to ensure the integrity of the ACS to prevent unauthorized manipulation.
FR-4	**Data Confidentiality**	**DC**	Asset or Control System (ACS) shall provide the necessary capabilities to ensure the confidentiality of information on communication data flows and in data repositories to prevent unauthorized disclosure.
FR-5	**Restricted Data Flow**	**RDF**	Asset or Control System (ACS) shall provide the necessary capabilities to segment the control system via security zones and security conduits to limit unnecessary data flow.
FR-6	**Timely Response to Events**	**TRE**	Asset or Control System (ACS) shall provide the necessary capabilities to respond to security violations by notifying the proper authority, reporting needed evidence of the violation, and taking timely corrective action when incidents are discovered.
FR-7	**Resource Availability**	**RA**	Asset or Control System (ACS) shall provide the necessary capabilities to ensure the availability of the control system against the degradation or denial of essential services.

Requirements Hierarchy

- System Requirements
  - defines the security capability required of a complete system.
- Component Requirements
  - define the security capability offered by individual components.
- The security capabilities of the system is build upon the capabilities of the components used in the system
- There is a direct correlation between the numbering of System and Component requirements.



Requirements Hierarchy

FR-1
Identification and Authentication Control

◇ CR 1.1 – Requirement

Components shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

◇ SR 1.1 – Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

Component Requirements

- Component Requirements are categorized into four subgroups
  - software application requirements (SAR)
  - embedded devices requirements (EDR)
  - host devices requirements (HDR)
  - network devices requirements (NDR)

Section 3

Frameworks and Standards

- IEC 62443 Series
- **NIST SP 800-82 Rev. 2**

Chapter 1

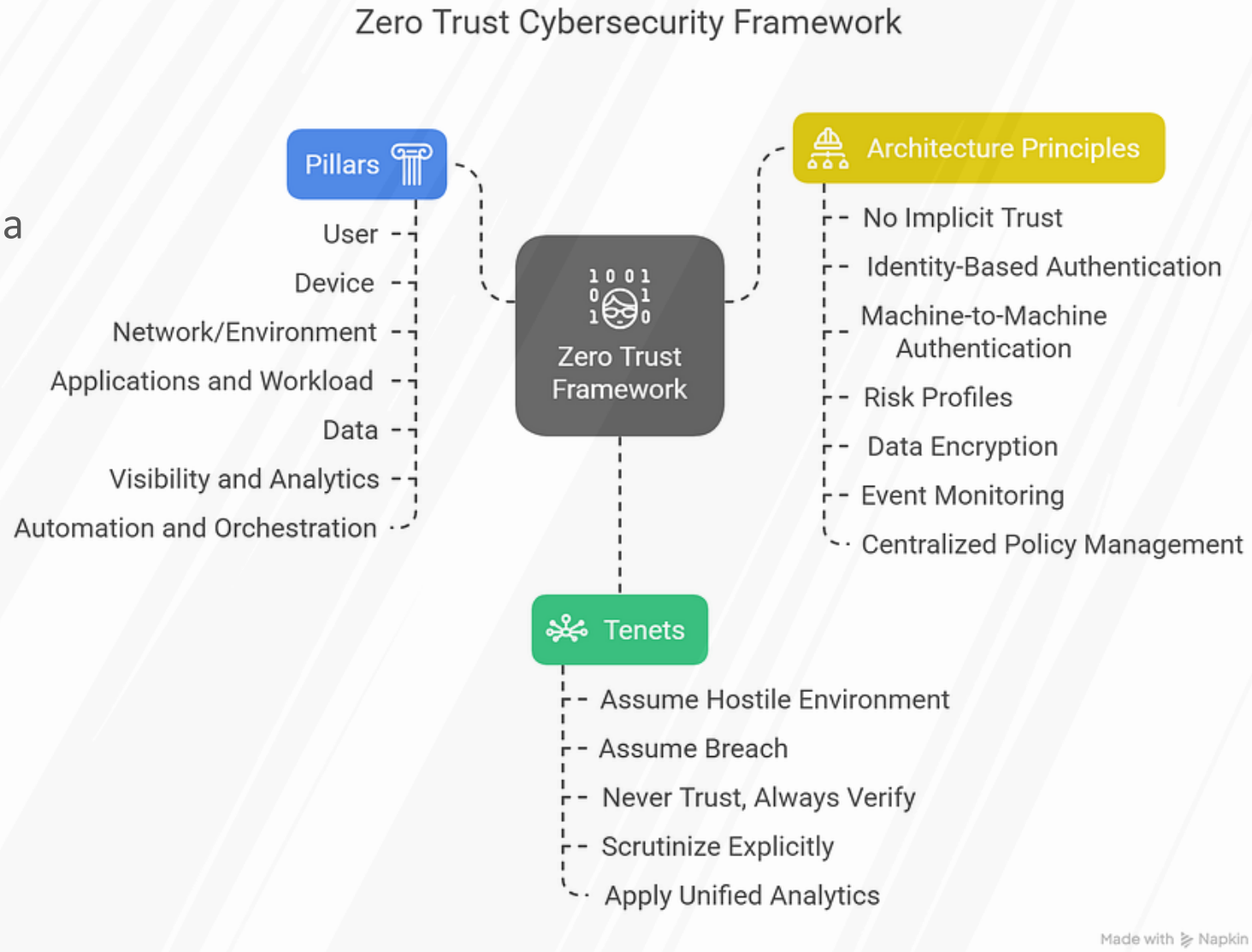
ICS/OT Security

From Process to Cloud

- ICS/OT Environments
- ICS Architecture, Attacks and Threats
- Frameworks and Standards
- **Defensive Architecture**
- Incident Response and Monitoring

Zero Trust Architecture

- with the **increase of distributed systems**, **wireless** and **cellular networks**, and **cloud** or hybrid environments, the traditional idea of a **clear network perimeter is becoming less relevant**.
- In these cases, **organizations should consider applying Zero Trust principles** to strengthen their overall security architecture.



Zero Trust Architecture

- In traditional network security, the **main focus is on network segmentation** and perimeter defenses.
- **Once a user or device gains access inside** the network boundary, they are often **considered “trusted”** and given wide access to internal resources.
- Because of this, security **controls between network zones do not prevent attackers from moving laterally** within the same zone.

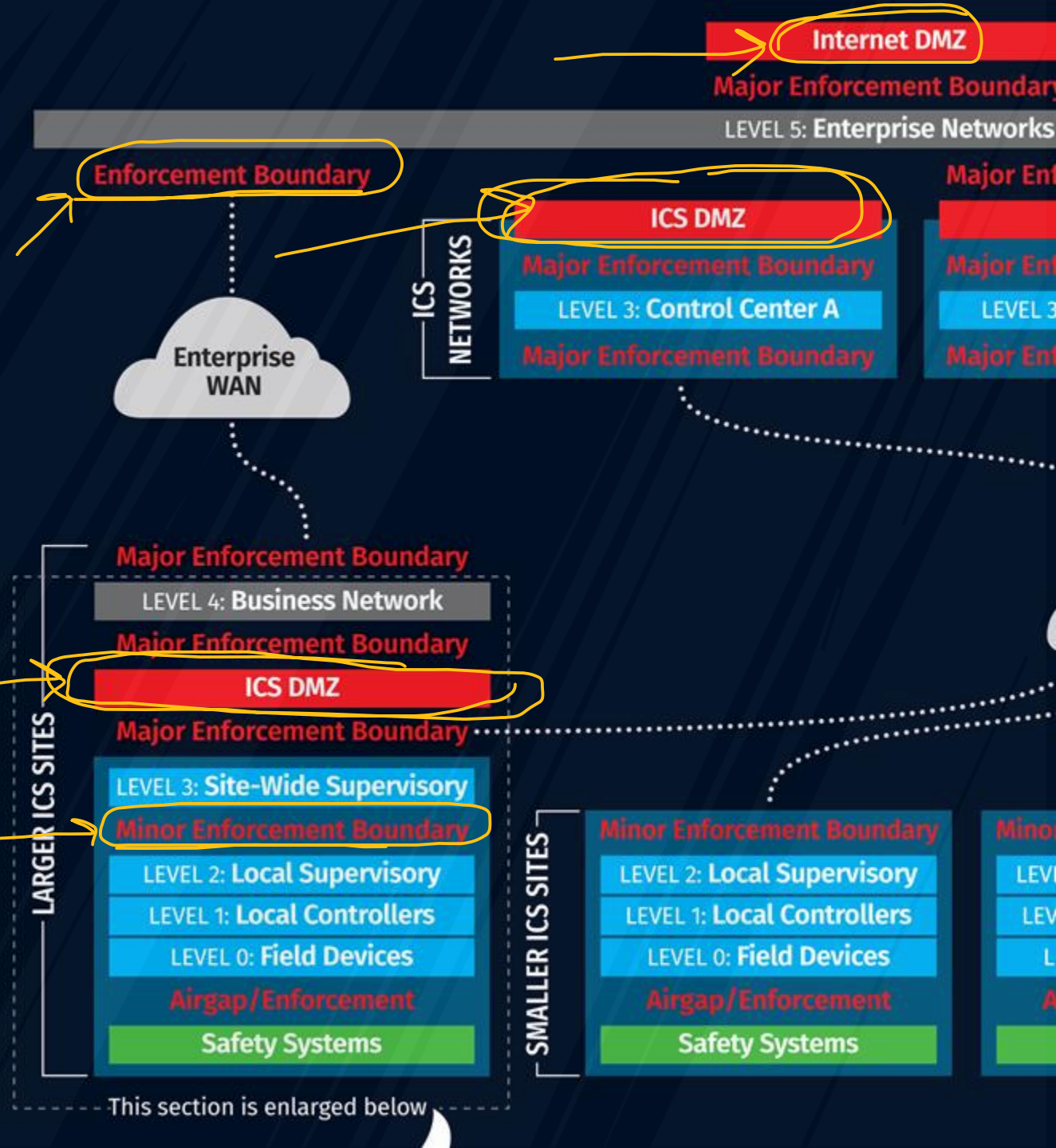
- **ZTA focus** on each resource **Data, Services, Applications**
- **Access decisions should be checked as close as possible to the resource itself**
- **Don’t trusted any other device** even in the same betwork.

NIST SP 800-82

Some OT components (e.g., PLCs, controllers, HMI) may not support the technologies or protocols required to fully integrate with a ZTA implementation.
As a result, a ZTA implementation might not be practical for some OT devices.
Instead, organizations should consider applying a ZTA to compatible devices, such as those typically found at the functionally higher levels of the OT architecture (e.g., Purdue model Levels 3, 4, 5, and the OT DMZ).
Organizations may also want to consider whether any adverse impacts might occur, such as if the ZTA solution increases the latency to respond to resource requests or if one or more ZTA components become unavailable. Based on this analysis, organizations should consider

Enforcement Boundary

- We typically define two primary types of enforcement boundaries:
  - **Major boundaries** separating IT and OT networks
  - **Minor boundaries** placed within OT environments, providing segmentation between different process zones or critical subsystems.



Devices and solutions

- To effectively restrict and monitor ICS communications, a combination of security devices and solutions can be employed:

- **Next-Generation Firewalls (NGFWs)** and **Unified Threat Management (UTM)** systems for advanced traffic inspection and policy enforcement.
- Network **Intrusion Detection and Prevention** Systems (NIDS/NIPS) to identify or block malicious network activity.
- **Data Diodes** for enforcing one-way communication where data integrity and confidentiality are critical.
- Network **Monitoring and Anomaly Detection tools** to establish baselines and detect unusual patterns in OT traffic.
- **Traditional firewalls** for basic segmentation and access control between network zones.
- **Honeypots** to attract, study, and detect unauthorized activity.
- **USB control and file-scanning solutions** to prevent malware introduction through removable media.

Firewall

- **Control traffic** between different **network segments**.
- **Filter communications** by content to block offensive, malicious, or sensitive data transfers.
- Perform Network Address Translation **(NAT) to obscure** internal network structure.
- **Encrypt communications**, e.g., using **VPN (IPSec)** for secure remote connections.
- Aid in **intrusion detection** and **forensics** when properly **logging** allowed and denied traffic.
- Use **Default Deny**: Only explicitly permitted traffic is allowed (recommended).
- **Reduce risks from both incoming and outgoing** exploitation attempts.
- **Preventing network reconnaissance** or intelligence gathering.
- Provide **detailed logs for use in incident handling** and forensic investigations.
- **Multiple firewalls** of different types or brands **can be cascaded** to strengthen security
  (Defense-in-Depth).

Data Diodes

- **Modern operational requirements**:
  - Site replication
  - Remote support
  - Asset performance monitoring
  - Business intelligence
  - Management visibility

- This **increases the connectivity** between control systems and external networks.

- Directly connecting IDS sensors to multiple networks can **bypass security controls**.

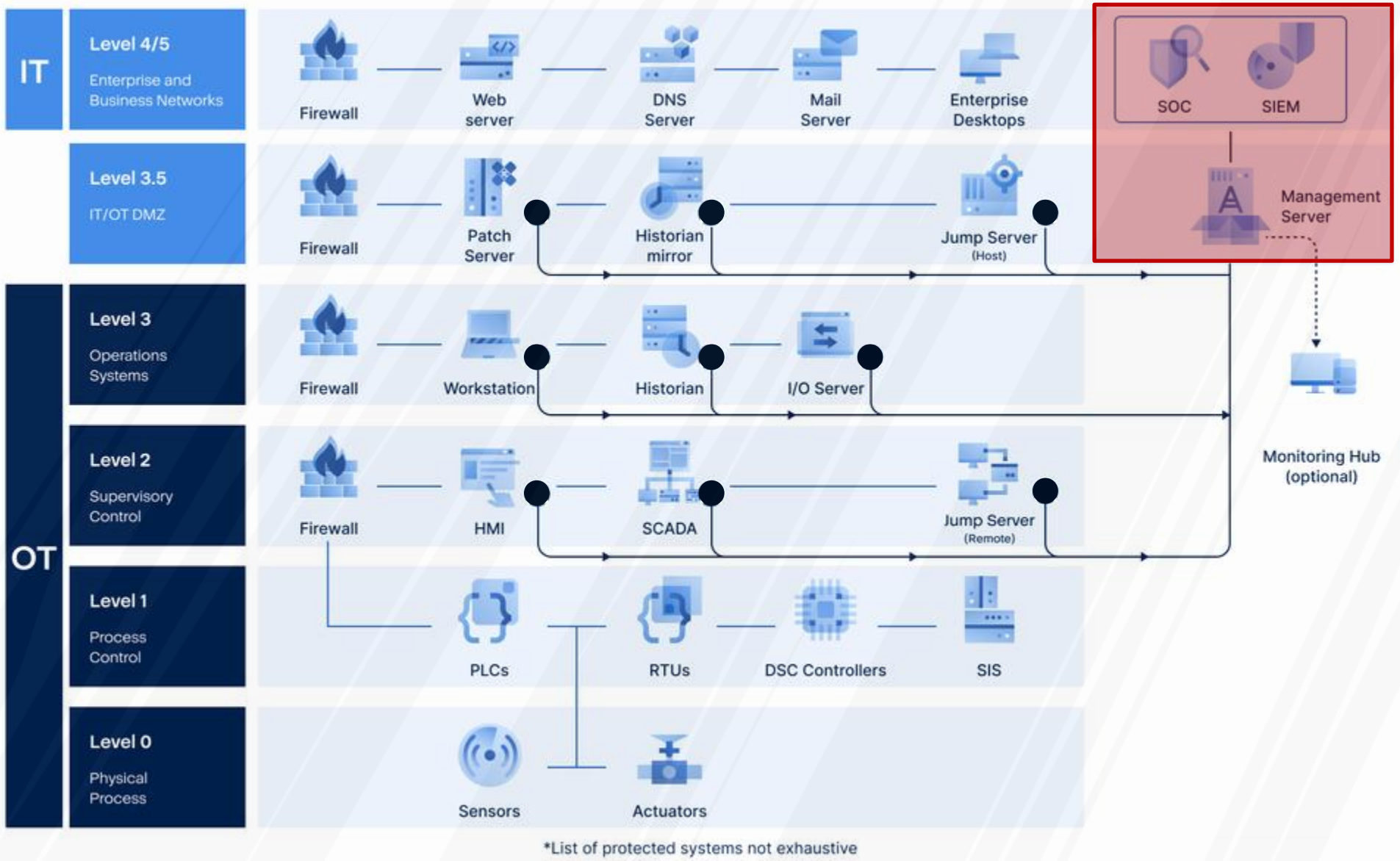
- The challenge is to **send data outward** for visibility or analytics **without allowing inbound communication** from less secure networks.

Possible solutions include

Deploying separate IDS collectors per network

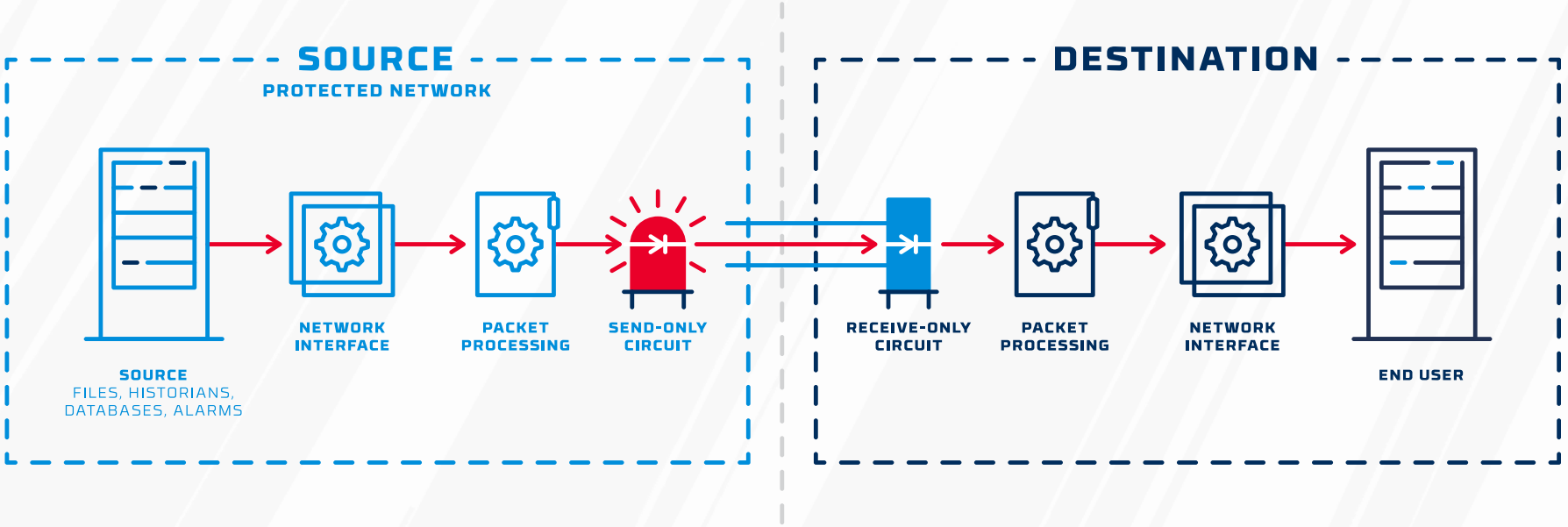
Or

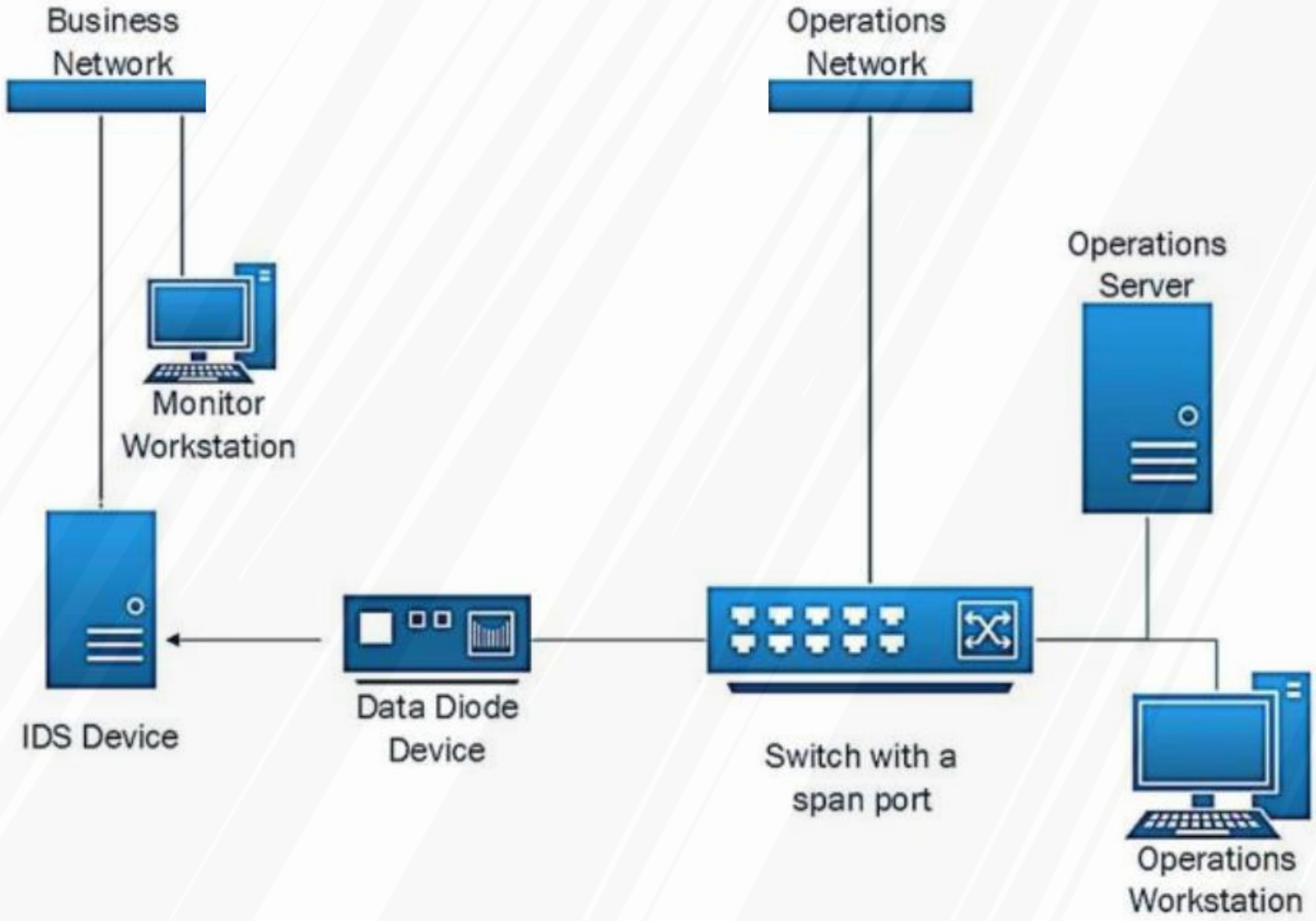
Using data diodes to allow one-way data flow from the secure network to the

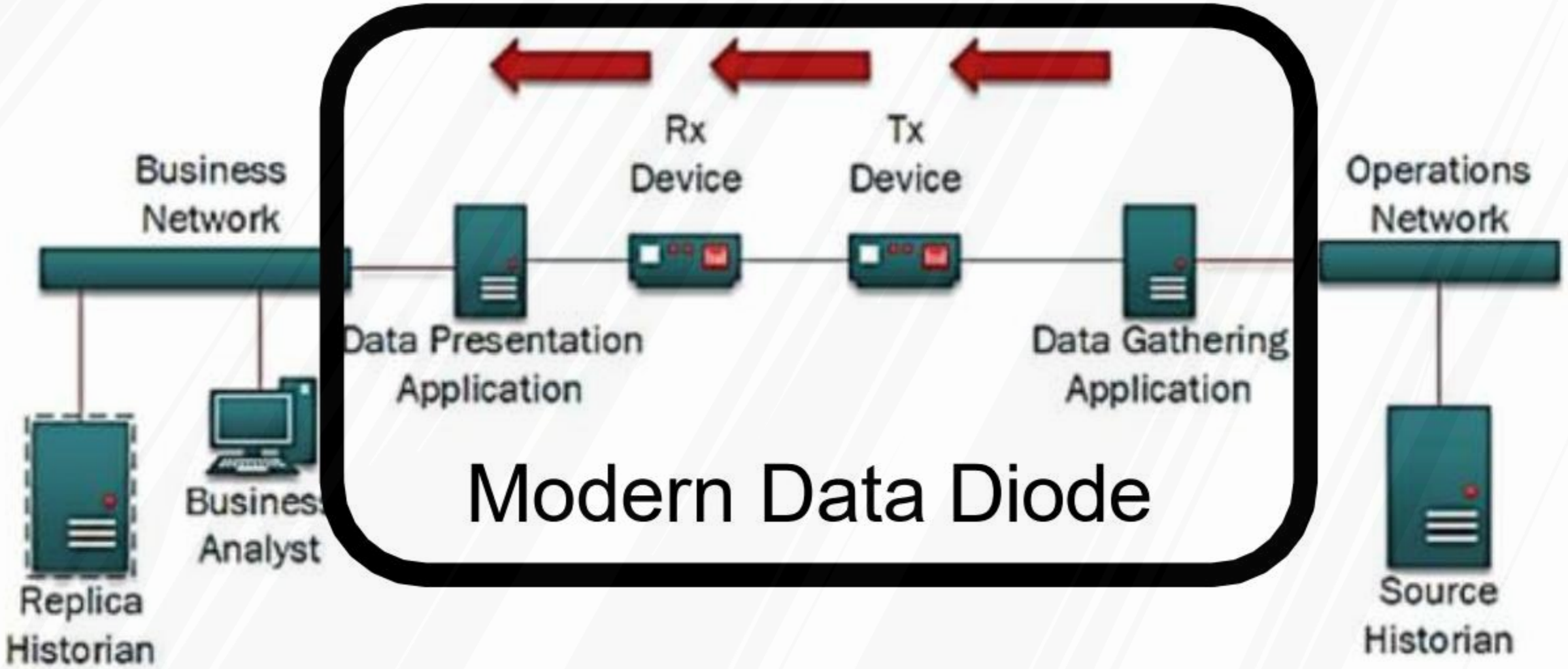

IT
Level 4/5
Enterprise and Business Networks
Firewall
Web server
DNS Server
Mail Server
Enterprise Desktops
SOC
SIEM
Level 3.5
IT/OT DMZ
Firewall
Patch Server
Historian mirror
Jump Server (Host)
Management Server
OT
Level 3
Operations Systems
Firewall
Workstation
Historian
I/O Server
Monitoring Hub (optional)
Level 2
Supervisory Control
Firewall
HMI
SCADA
Jump Server (Remote)
Level 1
Process Control
PLCs
RTUs
DSC Controllers
SIS
Level 0
Physical Process
Sensors
Actuators
*List of protected systems not exhaustive

Data Diodes

- Data diodes are **hardware-based** solution, primarily **used in military** networks.
- Consisted of a **data-emitting diode** (transmitter) on one side and a **light-receiving diode** (receiver) on the other.
- **No physical path existed** for data to flow backward.
- Support only simple use cases, such as:
  - **Collecting log events** (e.g., via syslog).
  - Protecting networks from **misconfigured SPAN ports**.
  - **Incompatible with TCP-based** protocols [3-way handshakes]
  - Limited UDP support [UDP uses request/response based communication].




Business Network
Operations Network
Operations Server
Monitor Workstation
IDS Device
Data Diode Device
Switch with a span port
Operations Workstation


Business
Network
Rx
Device
Tx
Device
Operations
Network
Data Presentation
Application
Data Gathering
Application
Modern Data Diode
Business
Analyst
Replica
Historian
Source
Historian

Chapter 1

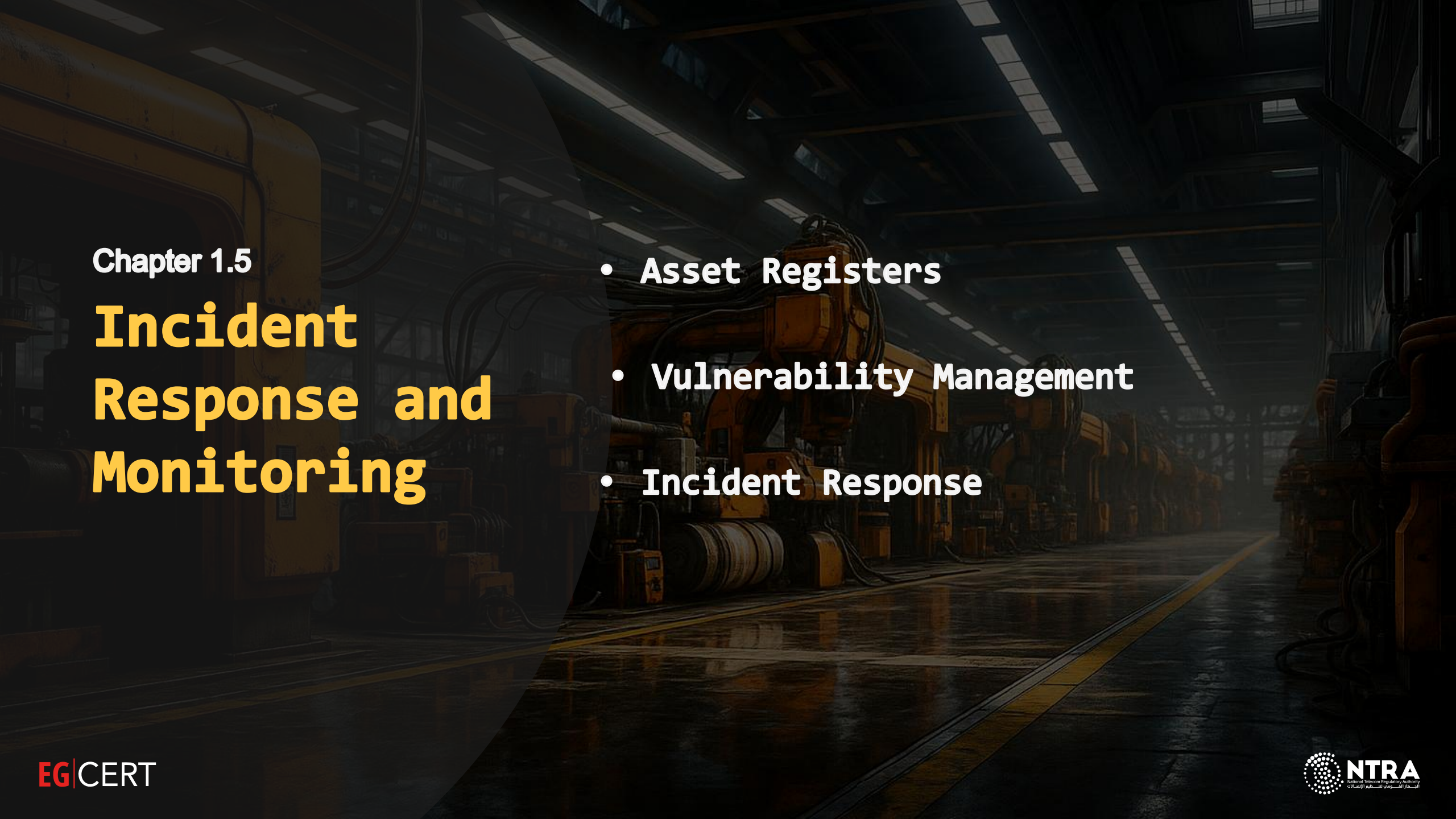
ICS/OT Security

From Process to Cloud

- ICS/OT Environments
- ICS Architecture, Attacks and Threats
- Frameworks and Standards
- Defensive Architecture
- **Incident Response and Monitoring**

EG|CERT

NTRA
National Telecom Regulatory Authority



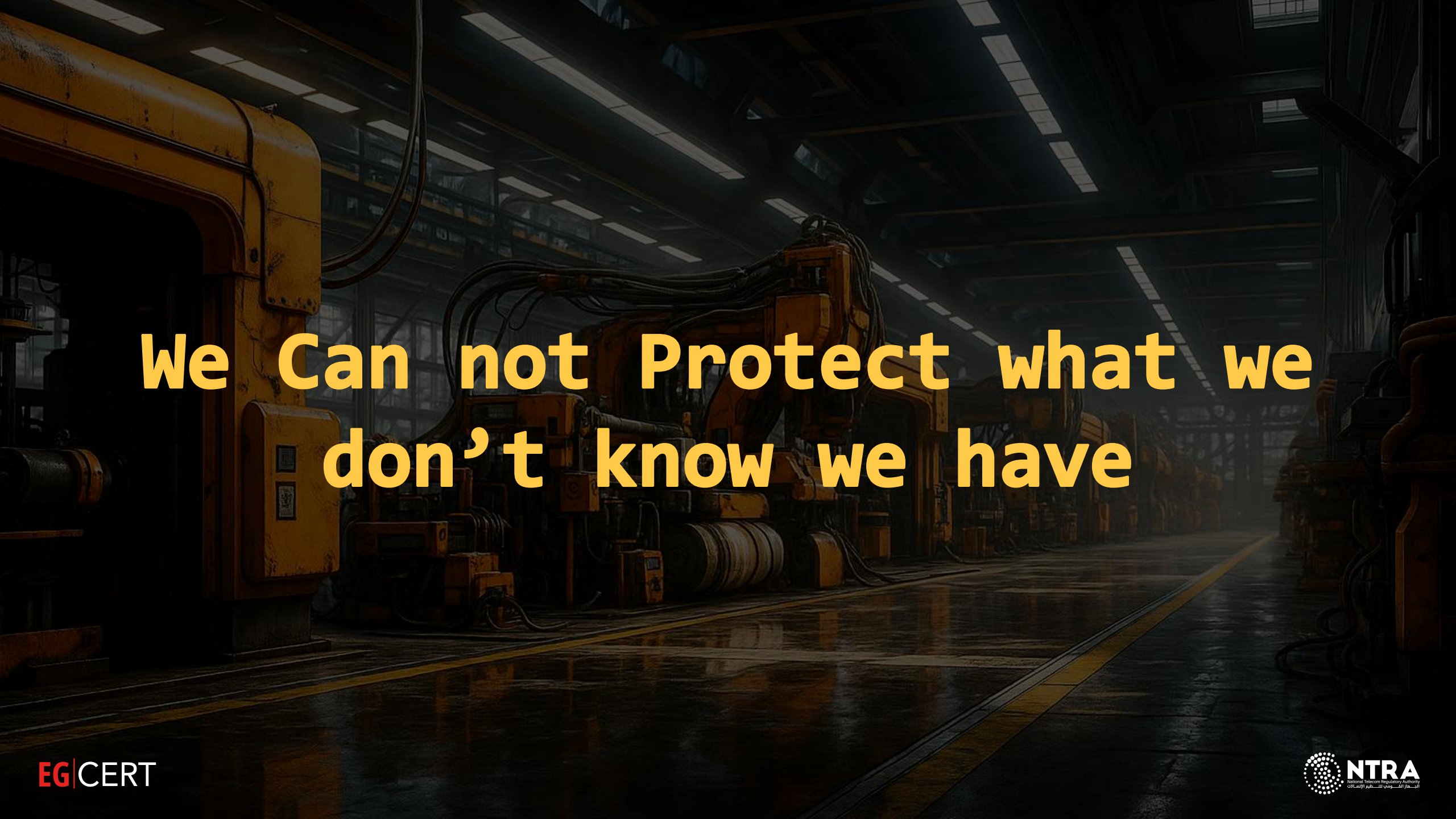
Chapter 1.5

Incident Response and Monitoring

- Asset Registers
- Vulnerability Management
- Incident Response

EG|CERT

NTRA
National Telecom Regulatory Authority



EG|CERT

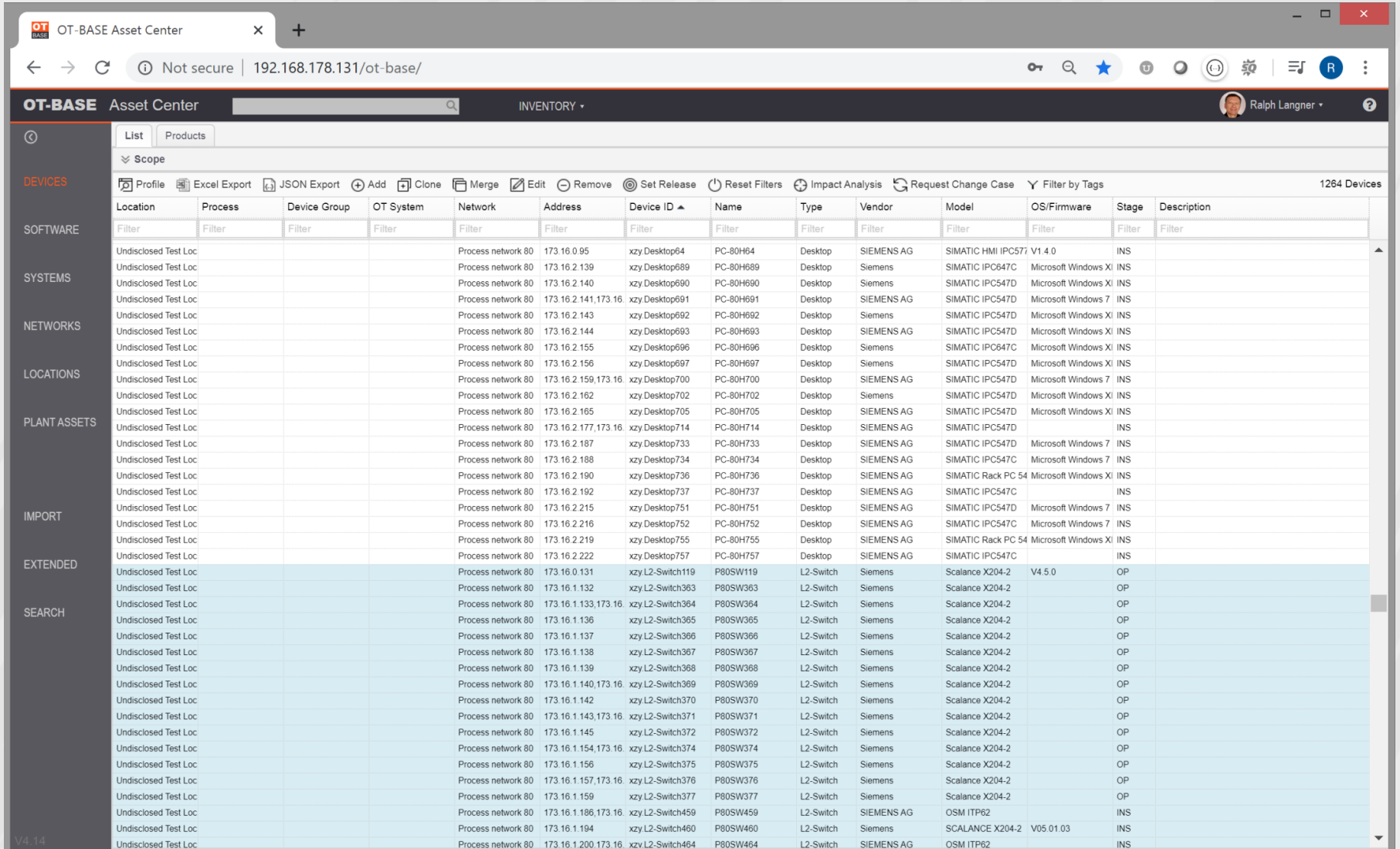
NTRA
National Telecom Regulatory Authority

Asset Registers And System Inventory

- An inventory that **contains all the hardware and software** within the environment
- It also **must include the virtualized assets**
- This will **help us in threat and vulnerability management** programs
- Never Assume the inventory is 100% accurate
  - A **maintenance engineer might add new HW** device
  - A technician **open hotspot** on the field
  - **A bored team connect Xbox** to the network
  - **Attacker connects a device**

Asset Registers And System Inventory

- Most common asset tool is **excel or Database**



Asset Registers And System Inventory

- Asset ID
- Asset Name
- Asset Type
- Location
- Manufacturer
- Model
- Serial Number
- IP Address
- MAC Address
- Installation Date
- Firmware Version
- Software Version
- Last Maintenance Date
- Maintenance Schedule
- Criticality
- Responsible Party
- Status
- Notes
- Zones
- Conduits

Building The Asset Register

- **Walking the environment**
  - Physically trace cables through the environment.
- **Review existing data**
  - Network diagrams, programming data, project files, procurement info.
- Review **network packet captures**
  - Use tools to analyze passively captured network data.
- **Actively scan the environment**
  - Tools can be used to send network packets on the network to test for the presence of assets and additional information gathering techniques.

Note

WARNING Active scanning can be considered harmful in ICS/OT.

Walking the environment

- Considered the **most physically dangerous** option as it requires team members to be exposed
- The **most time consuming** based on the effort required
- Potentially could **cause production issues if a technician interferes**
- Could be done **during basic maintenance** checks such as if a PLC key switch is in ‘Run’ mode

Review existing data

- **Information** about the **assets in the environment** can exist in multiple places, we just need to look for it
  - Project files
  - Network diagrams and configurations
  - System design specifications
  - PLC programming files
  - Asset specifications
  - Project plans and schedules
  - Change management records
  - Purchase records
  - Network appliance configurations
    - ARP tables

```
!
hostname Switch
!
interface VLAN 10
 description Internal Network
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1
 description PLC-1
 switchport access vlan 10
!
interface FastEthernet0/2
 description Firewall-1
 switchport access vlan 10
!
interface FastEthernet0/3
 description Valve-1
 switchport access vlan 10
```

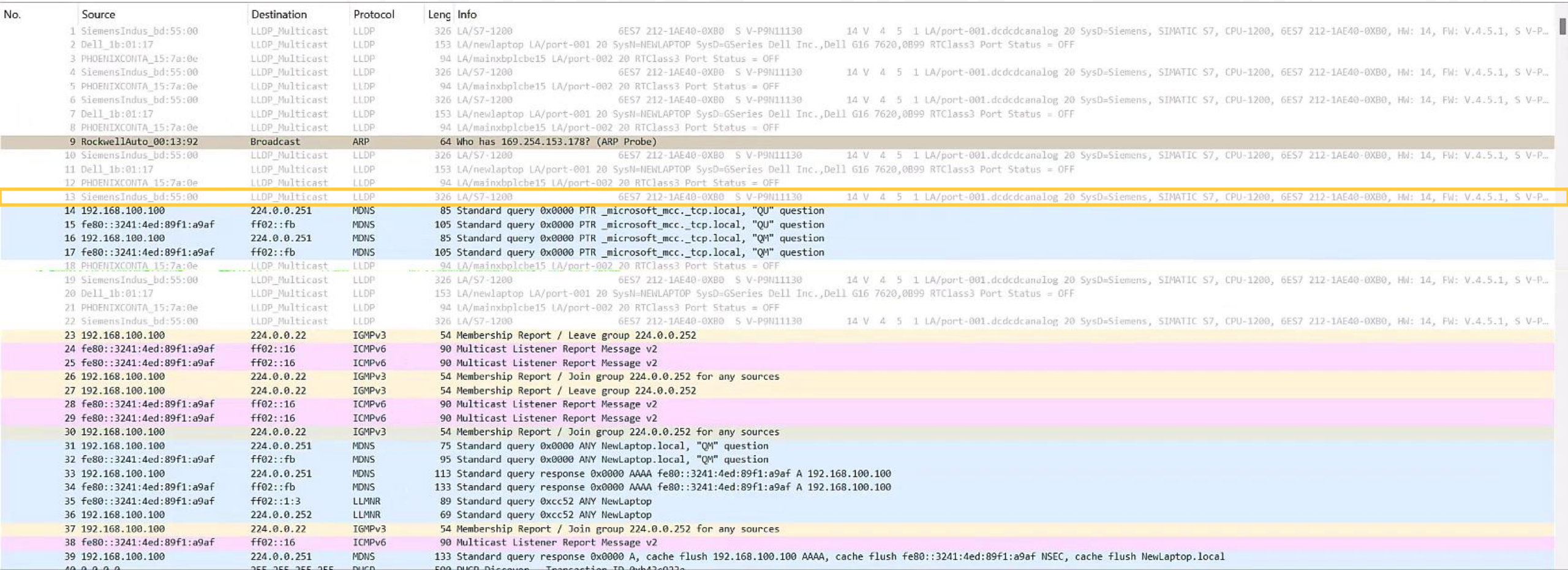
Network configurations

Review Network capture

- Packet captures can be **passively analyzed with Wireshark** to determine live hosts, active ports, services and applications
- Specific vendors, firmware and software versions can be discovered under certain conditions
- **Requires network visibility** for greatest coverage [No visibility, no discovered assets]

2	0.000035	141.81.0.10	141.81.0.86	Modbus/TCP	66
3	0.000574	141.81.0.86	141.81.0.10	Modbus/TCP	327
4	0.001032	141.81.0.10	141.81.0.86	Modbus/TCP	66
5	0.048116	141.81.0.86	141.81.0.10	Modbus/TCP	80
6	0.072663	141.81.0.10	141.81.0.24	Modbus/TCP	66
7	0.073315	141.81.0.24	141.81.0.10	Modbus/TCP	143
8	0.082684	141.81.0.10	141.81.0.24	Modbus/TCP	66
9	0.082747	141.81.0.10	141.81.0.44	Modbus/TCP	66
10	0.082881	141.81.0.10	141.81.0.104	Modbus/TCP	66
11	0.082977	141.81.0.10	141.81.0.144	Modbus/TCP	66
12	0.083193	141.81.0.10	141.81.0.164	Modbus/TCP	66
13	0.083239	141.81.0.24	141.81.0.10	Modbus/TCP	143
14	0.083278	141.81.0.10	141.81.0.24	Modbus/TCP	90
15	0.083465	141.81.0.44	141.81.0.10	Modbus/TCP	143
16	0.083466	141.81.0.144	141.81.0.10	Modbus/TCP	143
17	0.083468	141.81.0.104	141.81.0.10	Modbus/TCP	143
18	0.083563	141.81.0.10	141.81.0.44	Modbus/TCP	90
19	0.083633	141.81.0.10	141.81.0.144	Modbus/TCP	90
20	0.083643	141.81.0.10	141.81.0.104	Modbus/TCP	90
21	0.083831	141.81.0.164	141.81.0.10	Modbus/TCP	143
22	0.083880	141.81.0.10	141.81.0.164	Modbus/TCP	90
23	0.084029	141.81.0.144	141.81.0.10	Modbus/TCP	293
24	0.084038	141.81.0.24	141.81.0.10	Modbus/TCP	293
25	0.084216	141.81.0.104	141.81.0.10	Modbus/TCP	293
26	0.084217	141.81.0.44	141.81.0.10	Modbus/TCP	293
27	0.084456	141.81.0.164	141.81.0.10	Modbus/TCP	293
28	0.127740	141.81.0.10	141.81.0.26	Modbus/TCP	68
29	0.133665	141.81.0.10	141.81.0.24	Modbus/TCP	68
30	0.134282	141.81.0.24	141.81.0.10	Modbus/TCP	84
31	0.144627	141.81.0.26	141.81.0.10	TCP	60
32	0.144628	141.81.0.26	141.81.0.10	Modbus/TCP	66
33	0.144682	141.81.0.10	141.81.0.26	Modbus/TCP	68
34	0.173836	141.81.0.10	141.81.0.66	Modbus/TCP	66
35	0.179846	141.81.0.10	141.81.0.46	Modbus/TCP	68
36	0.182671	141.81.0.10	141.81.0.44	Modbus/TCP	68
37	0.183285	141.81.0.44	141.81.0.10	Modbus/TCP	84
38	0.183339	141.81.0.10	141.81.0.44	Modbus/TCP	68
39	0.183852	141.81.0.44	141.81.0.10	Modbus/TCP	66
40	0.194908	141.81.0.46	141.81.0.10	TCP	60
41	0.194910	141.81.0.46	141.81.0.10	Modbus/TCP	66
42	0.194963	141.81.0.10	141.81.0.46	Modbus/TCP	82
43	0.196380	141.81.0.26	141.81.0.10	Modbus/TCP	66
44	0.196427	141.81.0.10	141.81.0.26	Modbus/TCP	102
45	0.201791	141.81.0.66	141.81.0.10	TCP	60
46	0.201793	141.81.0.66	141.81.0.10	Modbus/TCP	65
47	0.201837	141.81.0.10	141.81.0.66	Modbus/TCP	66
48	0.244030	141.81.0.46	141.81.0.10	Modbus/TCP	78
49	0.244962	141.81.0.26	141.81.0.10	Modbus/TCP	340
50	0.245497	141.81.0.10	141.81.0.86	TCP	54
51	0.246309	141.81.0.10	141.81.0.26	Modbus/TCP	66
52	0.252460	141.81.0.66	141.81.0.10	Modbus/TCP	65
53	0.252514	141.81.0.10	141.81.0.66	Modbus/TCP	82
54	0.252828	141.81.0.10	141.81.0.86	Modbus/TCP	66
55	0.260110	141.81.0.10	141.81.0.64	Modbus/TCP	68

Review network packet captures



No.	Source	Destination	Protocol	Leng	Info
1	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
2	Dell_1b:01:17	LLDP_Multicast	LLDP	153	LA/newlaptop LA/port-001 20 SysN=NEWLAPTOP SysD=GSeries Dell Inc.,Dell G16 7620,0B99 RTClass3 Port Status = OFF
3	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
4	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
5	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
6	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
7	Dell_1b:01:17	LLDP_Multicast	LLDP	153	LA/newlaptop LA/port-001 20 SysN=NEWLAPTOP SysD=GSeries Dell Inc.,Dell G16 7620,0B99 RTClass3 Port Status = OFF
8	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
9	RockwellAuto_00:13:92	Broadcast	ARP	64	Who has 169.254.153.178? (ARP Probe)
10	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
11	Dell_1b:01:17	LLDP_Multicast	LLDP	153	LA/newlaptop LA/port-001 20 SysN=NEWLAPTOP SysD=GSeries Dell Inc.,Dell G16 7620,0B99 RTClass3 Port Status = OFF
12	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
13	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
14	192.168.100.100	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
15	fe80::3241:4ed:89f1:a9af	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
16	192.168.100.100	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
17	fe80::3241:4ed:89f1:a9af	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
18	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
19	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
20	Dell_1b:01:17	LLDP_Multicast	LLDP	153	LA/newlaptop LA/port-001 20 SysN=NEWLAPTOP SysD=GSeries Dell Inc.,Dell G16 7620,0B99 RTClass3 Port Status = OFF
21	PHOENIXCONTA_15:7a:0e	LLDP_Multicast	LLDP	94	LA/mainxbplcbe15 LA/port-002 20 RTClass3 Port Status = OFF
22	SiemensIndus_bd:55:00	LLDP_Multicast	LLDP	326	LA/S7-1200 6ES7 212-1AE40-0XB0 S V-P9N11130 14 V 4 5 1 LA/port-001.dcdcdcanalog 20 SysD=Siemens, SIMATIC S7, CPU-1200, 6ES7 212-1AE40-0XB0, HW: 14, FW: V.4.5.1, S V-P…
23	192.168.100.100	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
24	fe80::3241:4ed:89f1:a9af	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
25	fe80::3241:4ed:89f1:a9af	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
26	192.168.100.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
27	192.168.100.100	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
28	fe80::3241:4ed:89f1:a9af	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
29	fe80::3241:4ed:89f1:a9af	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
30	192.168.100.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
31	192.168.100.100	224.0.0.251	MDNS	75	Standard query 0x0000 ANY NewLaptop.local, "QM" question
32	fe80::3241:4ed:89f1:a9af	ff02::fb	MDNS	95	Standard query 0x0000 ANY NewLaptop.local, "QM" question
33	192.168.100.100	224.0.0.251	MDNS	113	Standard query response 0x0000 AAAA fe80::3241:4ed:89f1:a9af A 192.168.100.100
34	fe80::3241:4ed:89f1:a9af	ff02::fb	MDNS	133	Standard query response 0x0000 AAAA fe80::3241:4ed:89f1:a9af A 192.168.100.100
35	fe80::3241:4ed:89f1:a9af	ff02::1:3	LLMNR	89	Standard query 0xcc52 ANY NewLaptop
36	192.168.100.100	224.0.0.252	LLMNR	69	Standard query 0xcc52 ANY NewLaptop
37	192.168.100.100	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
38	fe80::3241:4ed:89f1:a9af	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
39	192.168.100.100	224.0.0.251	MDNS	133	Standard query response 0x0000 A, cache flush 192.168.100.100 AAAA, cache flush fe80::3241:4ed:89f1:a9af NSEC, cache flush NewLaptop.local

Active Scanning

- Active scanning **sends network packets** to **discover the live hosts** and **associated services**

> Note
>
> Active Scanning is not allowed for use in ICS/OT … Why?
> Active scanning can cause OT assets to reset, crash or damage

- Use Nmap carefully to scan the OT network
  - Live hosts
  - Open ports
  - Services and apps
  - Versions
  - Vulnerabilities

Active Scanning Using Nmap

Nmap QuickStart Guide for ICS/OT

insecure.org

What is Nmap?

Nmap is the world's most popular port scanner which has additional capabilities added over time. Created by Gordon "Fyodor" Lyon in 1997, Nmap runs on most operating systems.

You can find Nmap at insecure.org.

WARNING

Port scanning can have unintended consequences in network environments, particularly in ICS/OT networks. Ensure you have authorization and understand the potential ramifications of scanning a particular network before doing so.

Finding Hosts (Safest to Least Safest)

DNS Lookup – Lookup hostnames by IP
Example: **nmap -sL 192.168.1.0/24**

ARP Scan – Find hosts with ARP broadcasts
Example: **nmap -PR 192.168.1.0/24**

Ping Sweep – Find hosts with ICMP responses
Example: **nmap -sP 192.168.1.0/24**

Performance Settings

Controlling how fast Nmap sends packets on the network can help to reduce the risk of negatively impacting an ICS/OT network or asset.

- Use the –scan-delay option to force a limit on how often network probes are sent.
- Set --max-parallelism to 1 to ensure only one packet is sent at a time.

Example: **nmap 192.168.1.0/24 --scan-delay 5s --max-parallelism 1**

Port Scanning

Scan a Single Host – Default TCP Ports
Example: **nmap 192.168.1.5**

Scan a Single Host – Default UDP Ports
Example: **nmap -sU 192.168.1.5**

Scan a Single Host – All TCP ports
Example: **nmap 192.168.1.5 -p-**

Default TCP Port Scan On All Hosts on Subnet
Example: **nmap 192.168.1.0/24**

Scan for Most Common ICS/OT TCP Protocols
Example: **nmap 192.168.1.5 -p 102,502,789,1911,1962,2455,5007,9600,18245, 20000,20547,44818**

Scan for Most Common ICS/OT UDP Protocols
Example: **nmap 192.168.1.5 -p 5006,5094, 44818,47808**

Common ICS/OT Protocols & Ports

There are several common ICS/OT protocols that run on default ports to be familiar with.

Modbus	TCP 502	**GE-STRP**	TCP 18245
S7	TCP 102	**Hart**	UDP 5094
DNP3	TCP 20000	**PCWorx**	TCP 1962
BACnet	UDP 47808	**Omron**	TCP 9600
CODESYS	TCP 2455	**Red Lion**	TCP 789
Tridium	TCP 1911	**ProConOS**	TCP 20547
EthernetIP	TCP 44818	**MELSEC-Q**	TCP 5007
EthernetIP	UDP 44818	**MELSEC-Q**	UDP 5006

Service Scans

Service scans can be used to determine the actual service/application running on an open port.

Conduct a Service Scan on Default TCP Ports
Ex: nmap -sV 192.168.1.5

The Nmap Scripting Engine (NSE)

The Nmap Scripting Engine (NSE) provides additional capabilities beyond port scanning and service detection. Scripts can be written in LUA and stored in the Nmap /scripts folder.

Conduct a Script Scan with Default Scripts
Ex: nmap -sV -sC 192.168.1.5

Conduct a Script Scan with Only a Specific Script
Ex: nmap 192.168.1.5 -p 502 --script modbus-discover

Other included ICS/OT protocol enumeration scripts include **bacnet-info, enip-info,fox-info, iec-identify, modbus-discover, omron-info, pcworx-info and s7info.nse.**

Nmap Output

Nmap can save its output in several formats.

-oN: Normal text format
-oX: XML format
-oG: Grepable format
-oA: All three of the above at one time
-oS: s|<rIpt kIddi3 format

Ex: nmap 192.168.1.0/24 -oN results.txt

Special thanks to Gordon "Fyodor" Lyon for an incredible tool over the last 25 years!

linkedin.com/in/mikeholcomb

Asset Inventory update

- Establish **regular schedule to update the asset register** e.g., monthly, quarterly, annually
- Ensure **change management procedures** include updating the asset register as required
  - Adding assets as they are connected to the plant network
  - Removing assets as each is removed and/or decommissioned
- **If an asset is discovered** on the plant network that is not in the asset register, initiate **incident response procedures** to determine its origin

Chapter 1.5

Incident Response and Monitoring

- Asset Registers
- Threat & Vulnerability Management
- Incident Response

EG|CERT

NTRA
National Telecom Regulatory Authority

Threat and vulnerability management

- It is about How the business sees Risk
  - What would happen when this process goes down

$$Risk = threat\ x\ vulnerability\ x\ probability\ x\ impact$$

- Risk: the overall damage happens when vulnerability is exploited
- Threat: Potential source(script kiddy, state sponsored)
- Vulnerability: weakness or flaw that when exploited results negative impact
- Probability: how difficult this vulnerability could be exploited
- Impact: the damage done to the system (the business impact)

Vulnerability management Process

01. Find
Detecting vulnerabilities through scanning and testing

02. Prioritize
Understanding which issues are the most worthwhile to fix

Assign Risk

03. Fix
Patching, blocking, or otherwise fixing vulnerabilities at scale and in real-time

04. Monitor
Monitoring projects and code for newly discovered vulnerabilities

Vulnerability management Process

- **Critical**
  Easy to remotely exploit; provides full admin control.
- **High**
  Fairly easy to exploit; could provide full or limited control. Could be limited due to requiring local access (privilege escalation).
- **Medium**
  Difficult to exploit; even if so, associated impact would be limited.
- **Low**
  Very difficult to exploit; even if so, associated impact would be extremely limited.
- **Informational**
  Provides additional context but not assigned risk.

Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

Vulnerability management Process

CNA: Zero Day Initiative

Published: 2025-06-25 **Updated:** 2025-06-25
Title: Mikrotik RouterOS VXLAN Source IP Improper Access Control Vulnerability

Description

Mikrotik RouterOS VXLAN Source IP Improper Access Control Vulnerability. This vulnerability allows remote attackers to bypass access restrictions on affected installations of Mikrotik RouterOS. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of remote IP addresses when processing VXLAN traffic. The issue results from the lack of validation of the remote IP address against configured values prior to allowing ingress traffic into the internal network. An attacker can leverage this vulnerability to gain access to internal network resources. Was ZDI-CAN-26415.

CWE 1 Total

Learn more

- CWE-284: CWE-284: Improper Access Control

CVSS 1 Total

Learn more

Score	Severity	Version	Vector String
7.2	HIGH	3.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

Product Status

Learn more

Vendor
Mikrotik

Product
RouterOS

Versions 1 Total

Default Status: *unknown*
Affected

- affected at 7.15.3. 7.16.2

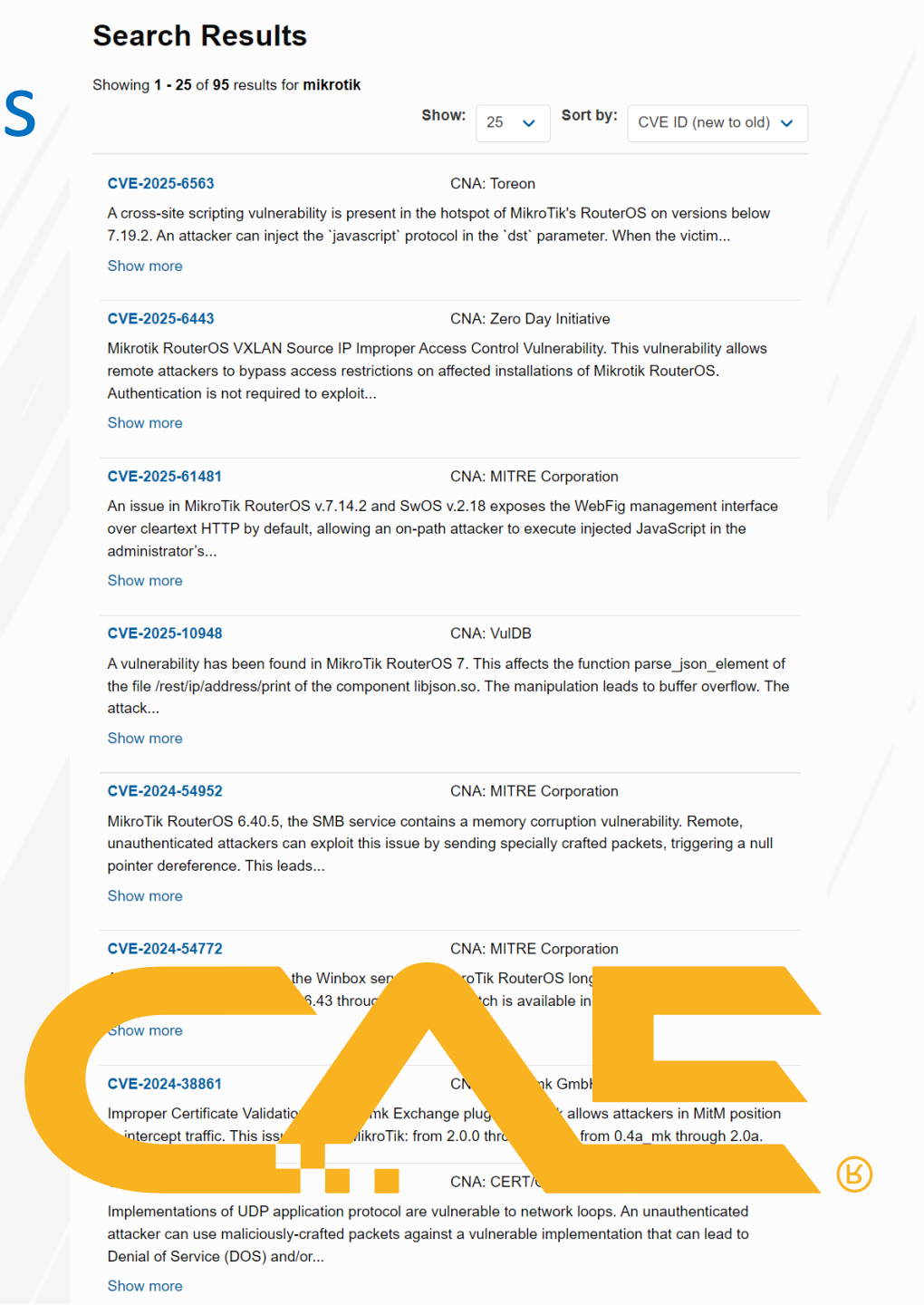
References 1 Total

- zerodayinitiative.com: ZDI-25-424 x_research-advisory

Vulnerability management Process

- CVE™'s Mission is to **identify, define, and catalog publicly disclosed cybersecurity vulnerabilities**.

- The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program.



Search Results

Showing **1 - 25** of **95** results for **mikrotik**

Show: 25 **Sort by:** CVE ID (new to old)

CVE-2025-6563 CNA: Toreon

A cross-site scripting vulnerability is present in the hotspot of MikroTik's RouterOS on versions below 7.19.2. An attacker can inject the `javascript` protocol in the `dst` parameter. When the victim...

Show more

CVE-2025-6443 CNA: Zero Day Initiative

Mikrotik RouterOS VXLAN Source IP Improper Access Control Vulnerability. This vulnerability allows remote attackers to bypass access restrictions on affected installations of Mikrotik RouterOS. Authentication is not required to exploit...

Show more

CVE-2025-61481 CNA: MITRE Corporation

An issue in MikroTik RouterOS v.7.14.2 and SwOS v.2.18 exposes the WebFig management interface over cleartext HTTP by default, allowing an on-path attacker to execute injected JavaScript in the administrator's...

Show more

CVE-2025-10948 CNA: VulDB

A vulnerability has been found in MikroTik RouterOS 7. This affects the function parse_json_element of the file /rest/ip/address/print of the component libjson.so. The manipulation leads to buffer overflow. The attack...

Show more

CVE-2024-54952 CNA: MITRE Corporation

MikroTik RouterOS 6.40.5, the SMB service contains a memory corruption vulnerability. Remote, unauthenticated attackers can exploit this issue by sending specially crafted packets, triggering a null pointer dereference. This leads...

Show more

CVE-2024-54772 CNA: MITRE Corporation

Show more

CVE-2024-38861

Show more

CNA: CERT/

Implementations of UDP application protocol are vulnerable to network loops. An unauthenticated attacker can use maliciously-crafted packets against a vulnerable implementation that can lead to Denial of Service (DOS) and/or...

Show more

CVSS SCORE METRICS

A CVSS score is composed of three sets of metrics (**Base**, **Temporal**, **Environmental**), each of which have an underlying scoring component.

BASIC METRIC GROUP

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope

Impact Metrics

- Compatibility Impact
- Integrity Impact
- Availability Impact
- Scope

TEMPORAL METRIC GROUP

The Changing Landscape

- Exploit Code Maturity
- Remediation Level
- Report Confidence

ENVIRONMENTAL METRIC GROUP

Enterprise-Specific Factors

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement
- Modified Base Metrics

Chapter 1.5

Incident Response and Monitoring

- Asset Registers
- Threat & Vulnerability Management
- **Incident Response**

EG|CERT

NTRA
National Telecom Regulatory Authority

Considerations for ICS Incident Response

- Unique Systems:
  - Involve nontraditional computer systems using industrial and proprietary protocols not found in standard IT environments.
- Dependence on External Vendors:
  - Many engineering systems require specialized vendor support and secure remote access for troubleshooting or maintenance.
- Legacy Equipment:
  - Includes outdated devices that cannot be easily patched or updated, often relying on infrequent maintenance windows.
- Non-Traditional Operating Systems:
  - Use of purpose-built embedded or proprietary OSs, where traditional IT security tools and defenses may not apply.
- Human Safety First:
  - In ICS environments, safety of personnel is the top priority, followed by integrity (trusting operations) and availability.
- Protection of Physical Assets:
  - Since ICS directly controls physical processes, cyber incidents can lead to equipment damage, safety hazards, and environmental impacts.

Incident Response Process

- Preparation & Planning
  - **Expand your traditional IT incident response** to ensure that site safety teams are involved in cyber incident response planning.
  - External organizations such as **ICS peers**, **government agencies**, **Information Sharing and Analysis Centers** (ISACs), and **Computer Emergency Response Teams** (CERTs) will also need to be part of the overall plan.
  - **Tools** for those teams in the control system are to be **tested in development environments** at this stage.

Incident Response Process

- Integrated Detection and Identification
  - Collaboration: **Incident Response** and **ICS engineering** teams work together for continuous network monitoring.
  - Threat Intelligence: **Utilize known threat data** to detect suspicious or malicious activity early.
  - Operational Impact Awareness: **Identify threats that could affect control systems** or ongoing industrial processes.

Incident Response Process

- Evidence Acquisition
  - Teams will **use already-tested and deployed** or **available tools** to quickly acquire meaningful forensics data from critical ICS assets to help determine threats.

Incident Response Process

- Time Critical Analysis
  - **Quickly analyze threats** to determine their impact on operations and safety.
  - **Provide stakeholders with immediate, safe response options** such as system isolation or controlled shutdown.

Incident Response Process

- Containment Considering Safety
  - **Ensuring safety will be prioritized** and considered **at each step of containment** or change in the industrial environment, operational technology. or engineering systems.

Incident Response Process

- Eradication, Recovery Considering Safety
  - This will involve **removing threats** such as **malware**, **adversary remote access**, etc. in order to **reestablish a safe and trusted industrial process**.
  - This could require
    - rebuilding the operating system
    - reloading industrial software,
    - uploading controller logic, etc.

Incident Response Process

- Lessons Learned
  - This will involve **applying knowledge**, technology, personnel resourcing, and **process gaps** to the ICS or IT/OT converged Cyber Incident Response Plan.

Incident Response Process

- Information Sharing
  - Sharing key takeaways from incidents with the ICS community and peers in the sector will **help maintain the safety** and reliability of operations in facilities across other sectors globally.
  - Key information would be in the form of **adversary attack TTP**, **indicators of compromise** of a specific attack, and the **campaign** of **malware capability** used.

> whoami

- Mohamed Salah-el-den
- Cyber Security Technical Team Lead @ EG|CERT
- 4 Years of experience in Emerging technologies Cybersecurity Department
- IoT/OT and Embedded systems Pentester

Resources

EG|CERT | NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

THE END