PRO-TECH SYSTEMS GROUP

Cybersecurity

For the Water Industries

PRESENTER

Jason Rayle

OT Solution Specialist

OVERVIEW

Overview

- Oldsmar Water Plant Hack
- Cybersecurity in Operational Technologies Background
  - OT/IT Network Structure Basics
  - Types of attacks
    - Basic
    - Advanced
- Planning a Multilayered Protection

Oldsmar, FL Hack

EVENTS

February 5, 2021 / 8 AM

Operator notices the mouse cursor moving across the screen and navigating to a controls screen. Supervisor has remote setting to monitor the system.

February 5, 2021 / Few hours Later

Operator notices the mouse cursor moving across without him using it. He assumes that a This time he sees the setting for the sodium hydroxide change from 100 to 11100 ppm and realizes that this was not a Supervisor, but someone who was trying to do harm.

Cybersecurity

Oldsmar, FL Hack

Investigation Discoveries

2017 Compilation of breaches included 11 pairs of credentials

Feb 2 Compilation of breaches included 13 pairs of credentials

All computers were unsupported Windows 7 (32 bit) operating software

Team Viewer was the remote access software

All remote access shared the same password

Cybersecurity

OT Network Basics

Old Infrastructure- Lower Risk

- Isolation
- Manual processes for data collection and operations
- Unique Protocols

New Infrastructure- Higher Risk

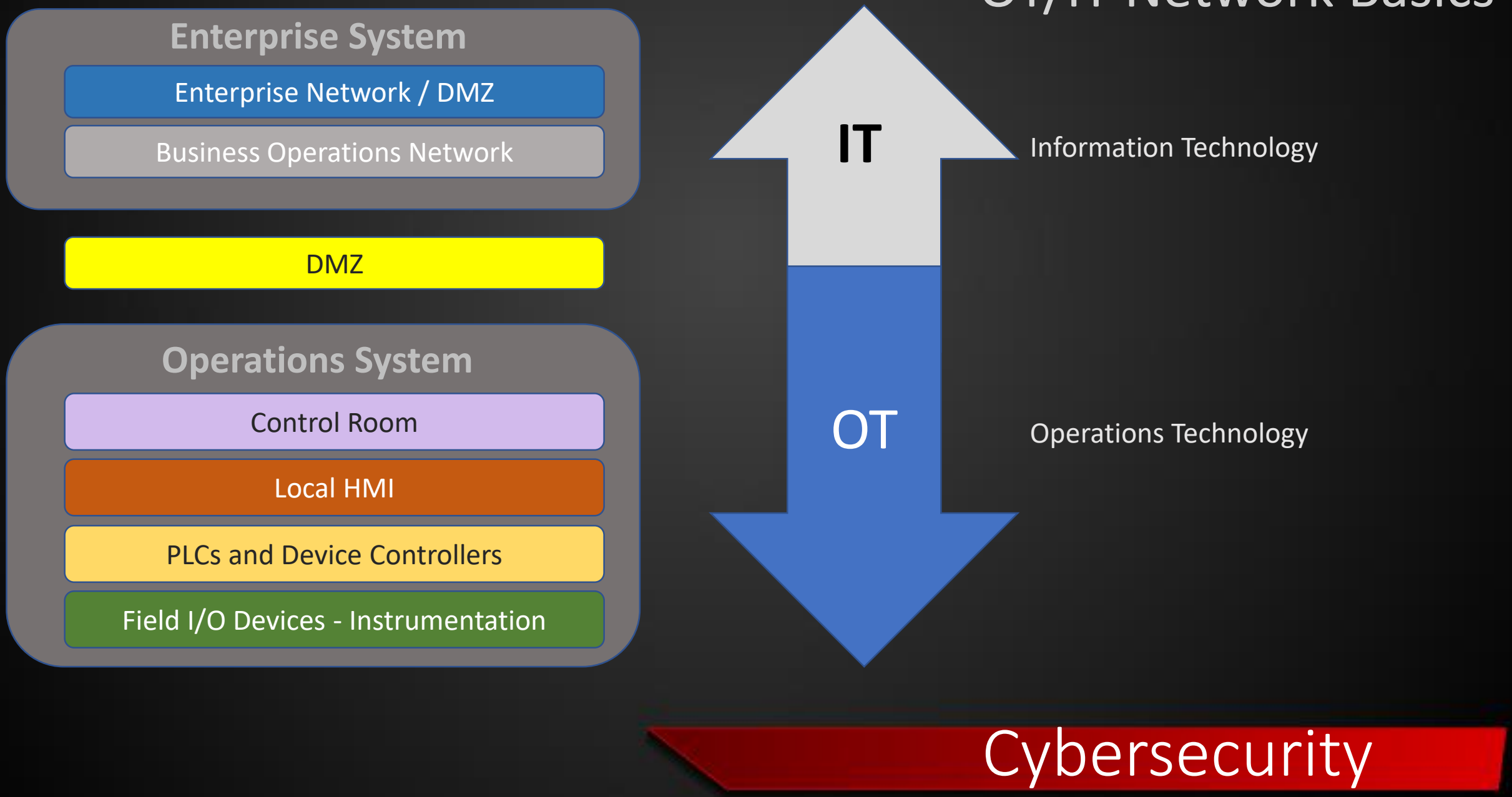
- Connected processes
- Increased automation
- Universal Protocols (e.g., Modbus)
- Remote access
- Business integrations

OT Network Basics

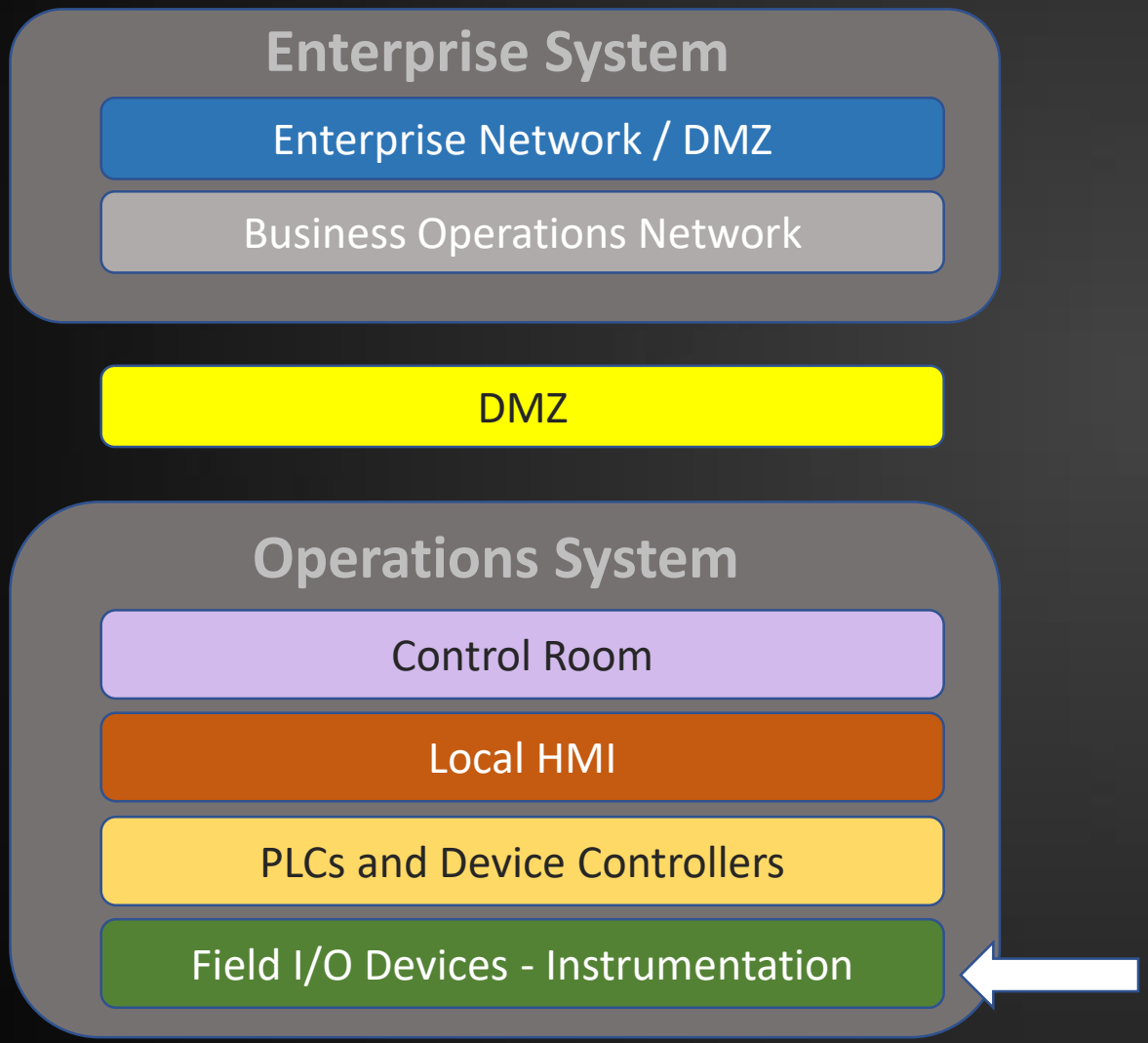
Risk Factors

- Connected Systems and Devices
- Common methods of communication
  - Protocols
  - Network Structure and Components
- Increased number of domestic and foreign activity
- Advanced tools for attackers

OT/IT Network Basics

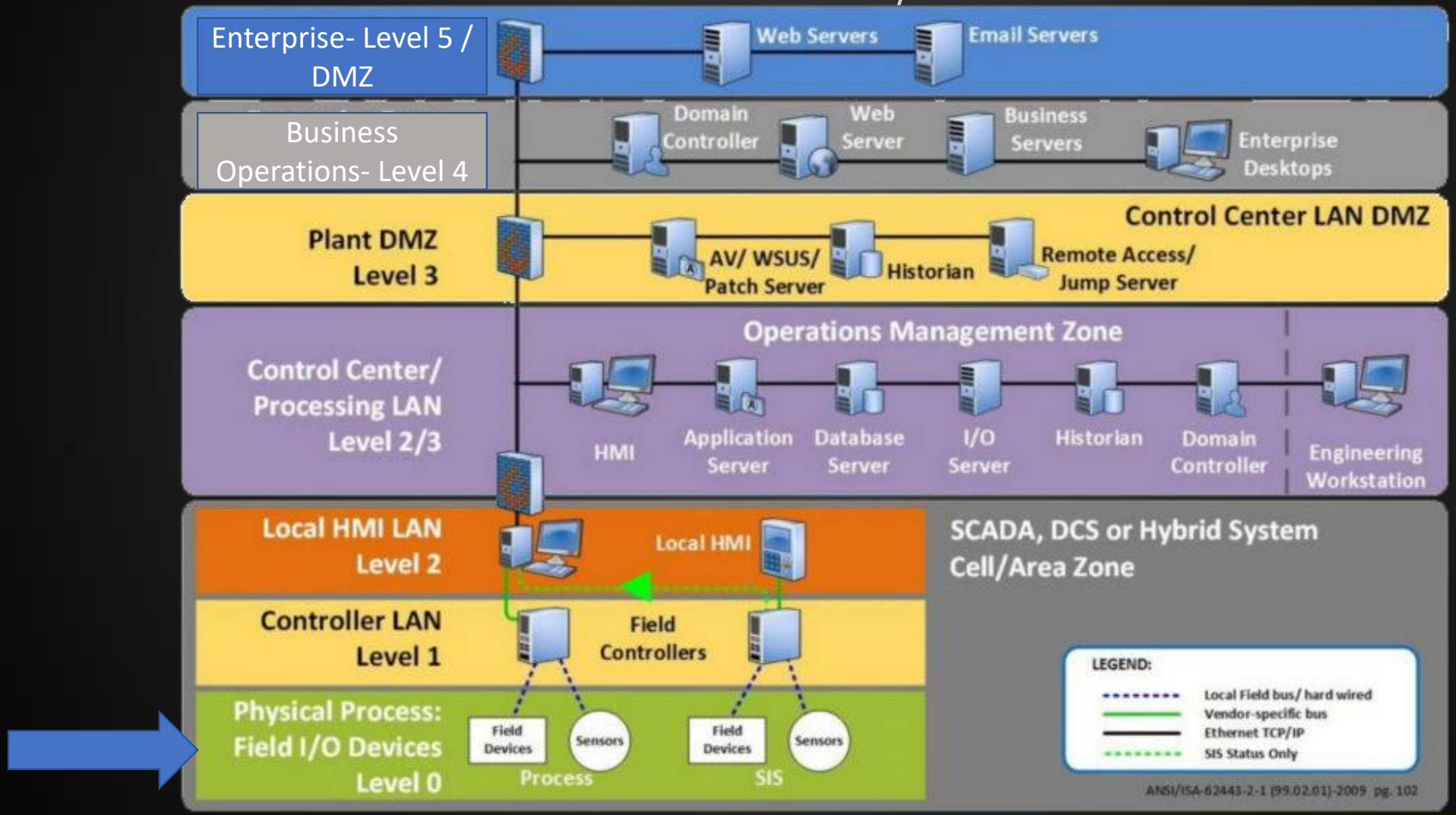


OT/IT Network Basics



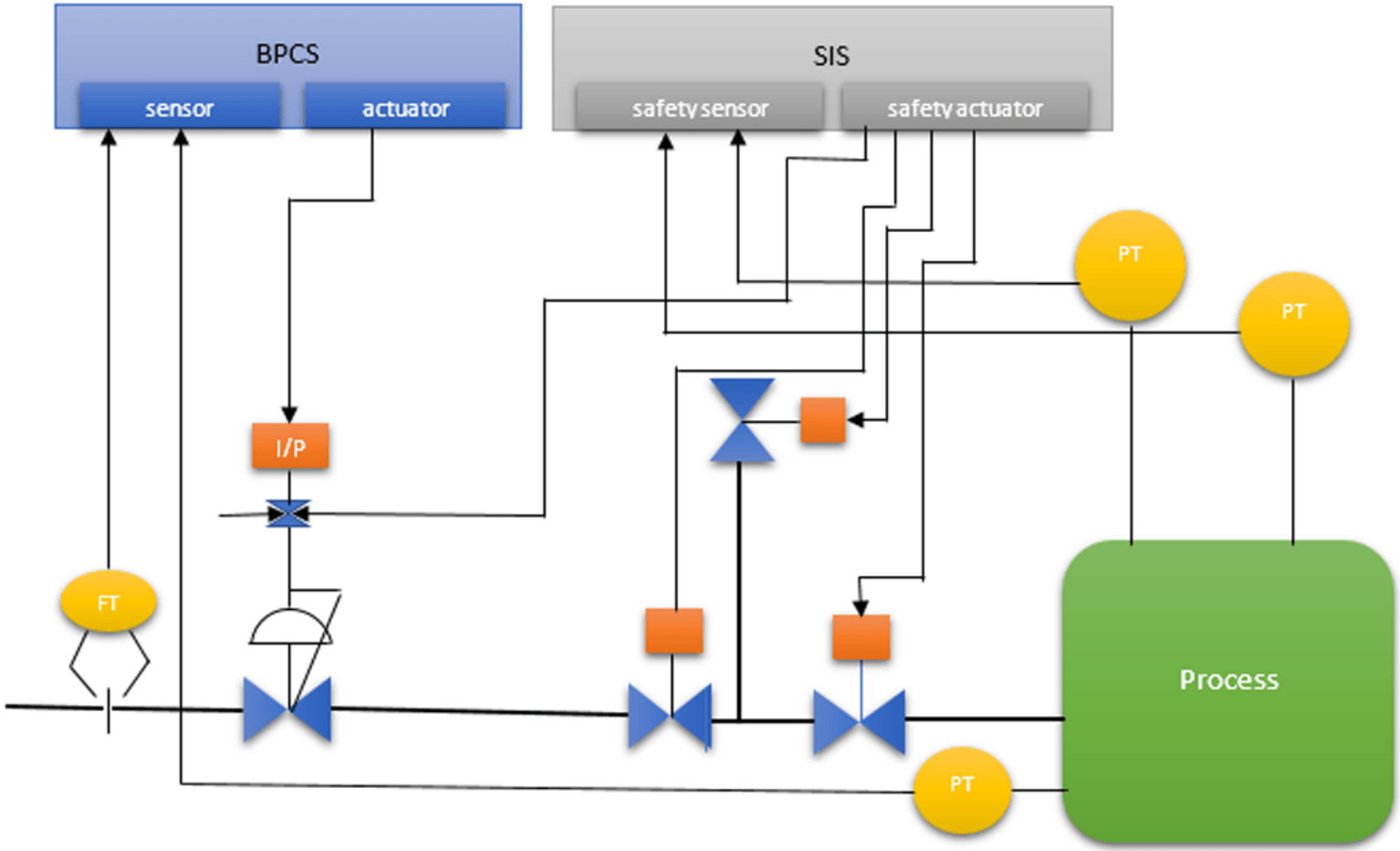
Cybersecurity

OT/IT Network Structure Basics



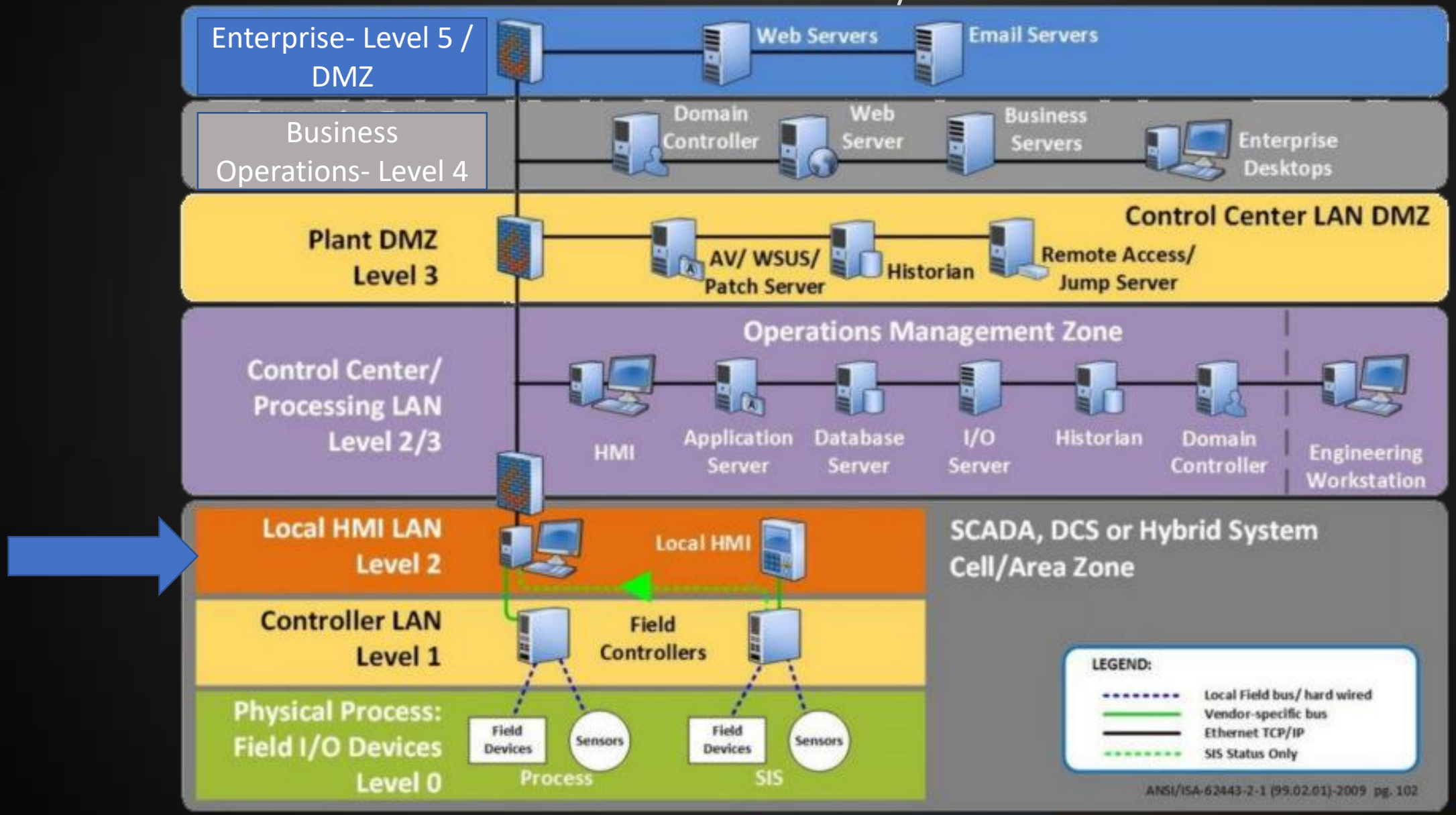
Cybersecurity

OT/IT Network Structure Basics



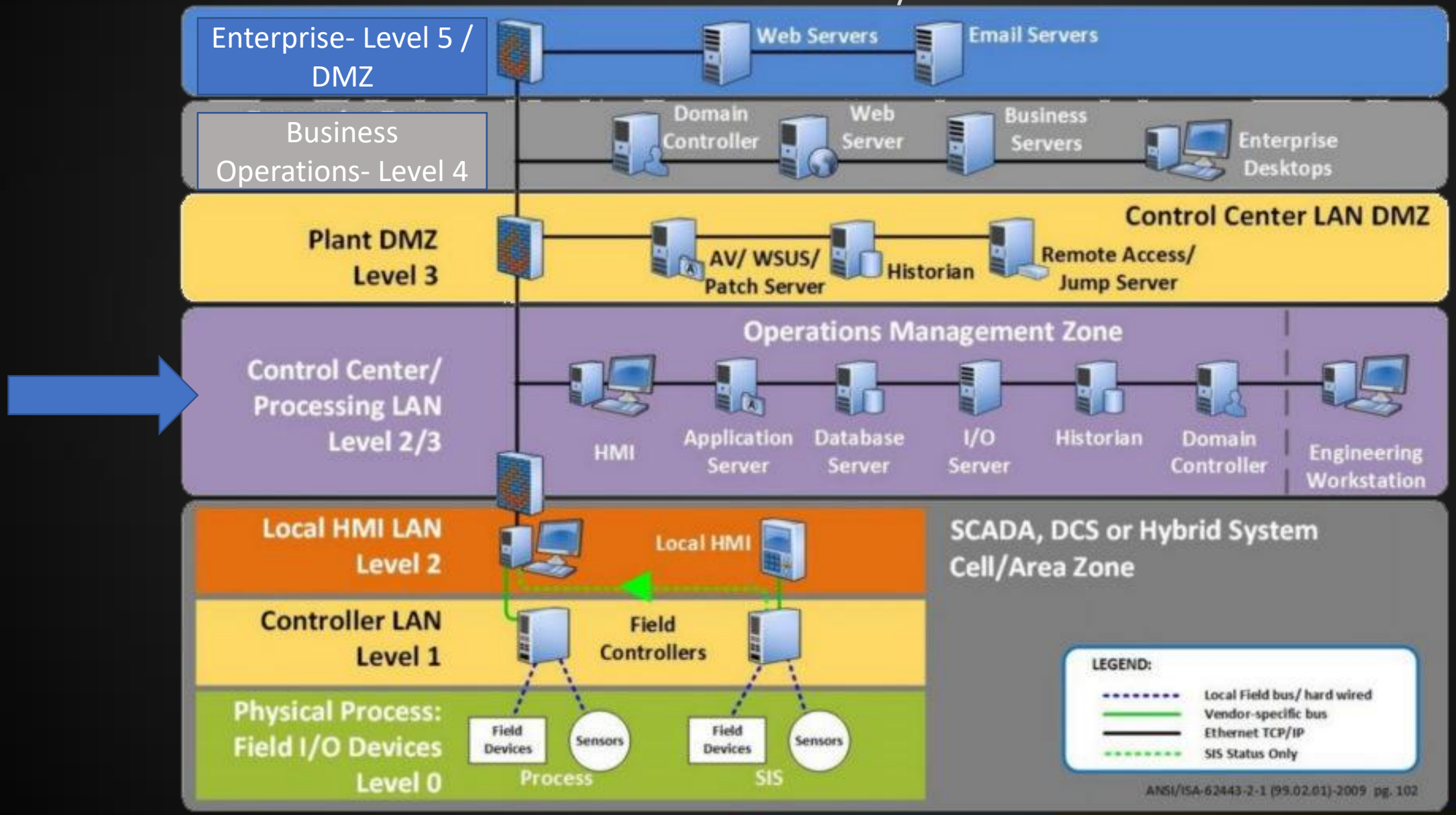
Cybersecurity

OT/IT Network Structure Basics



Cybersecurity

OT/IT Network Structure Basics



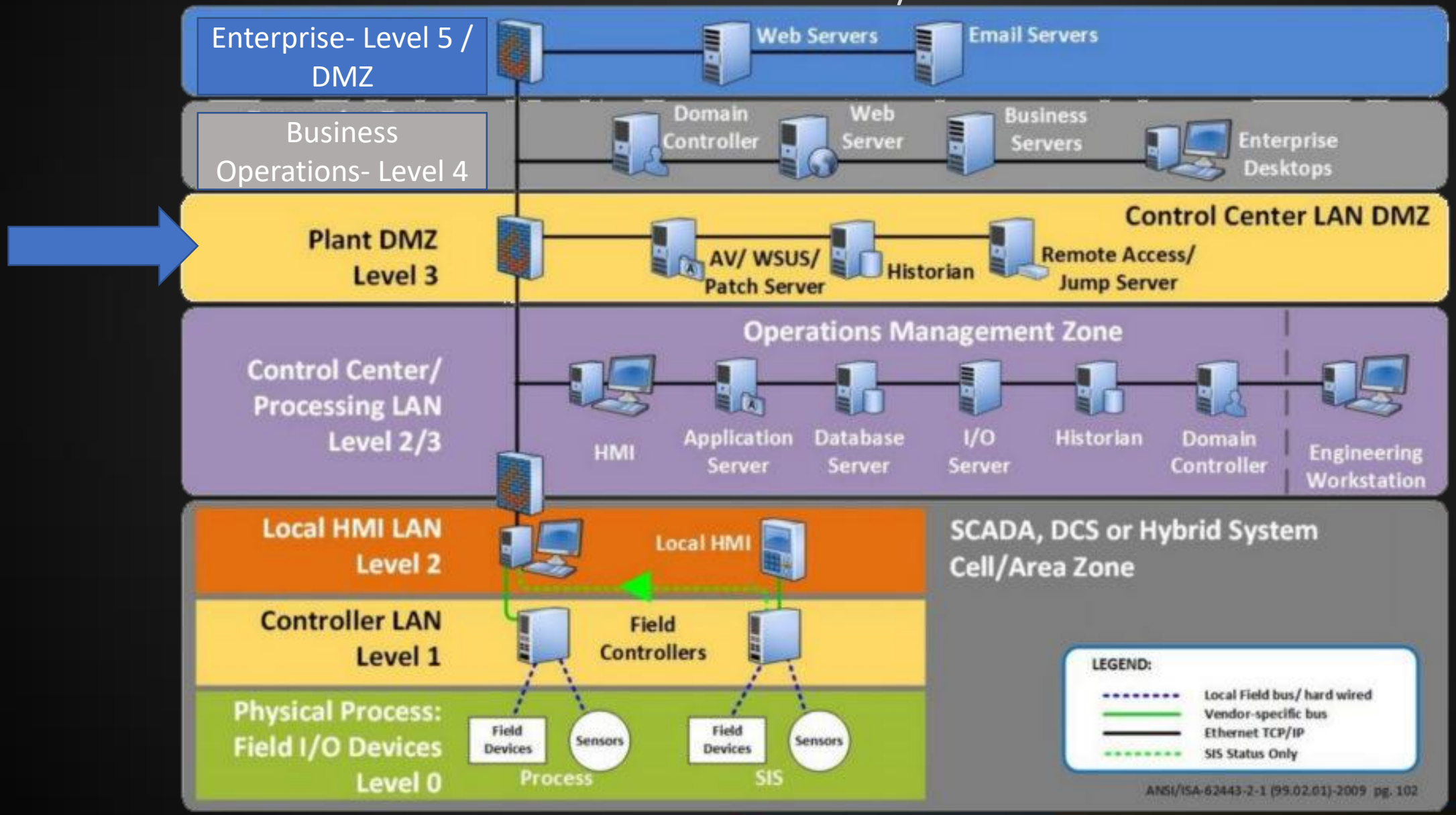
Cybersecurity

OT/IT Network Structure Basics

SCADA Security Features

Cybersecurity

OT/IT Network Structure Basics



Cybersecurity

Types of Attacks: Basic

Brute Force Attacks

- Using automated tools to guess usernames and passwords until you gain access

Unauthorized access

- Using a username or password not assigned to you by the system admin.
- Accessing areas of a system that you do not have permission to be in. Even when you have credentials for a system.

Types of Attacks: Advanced

APTs - Advanced Persistent Threats

- State or state sponsored
- Go undetected for extended periods

Types of Attacks: Advanced

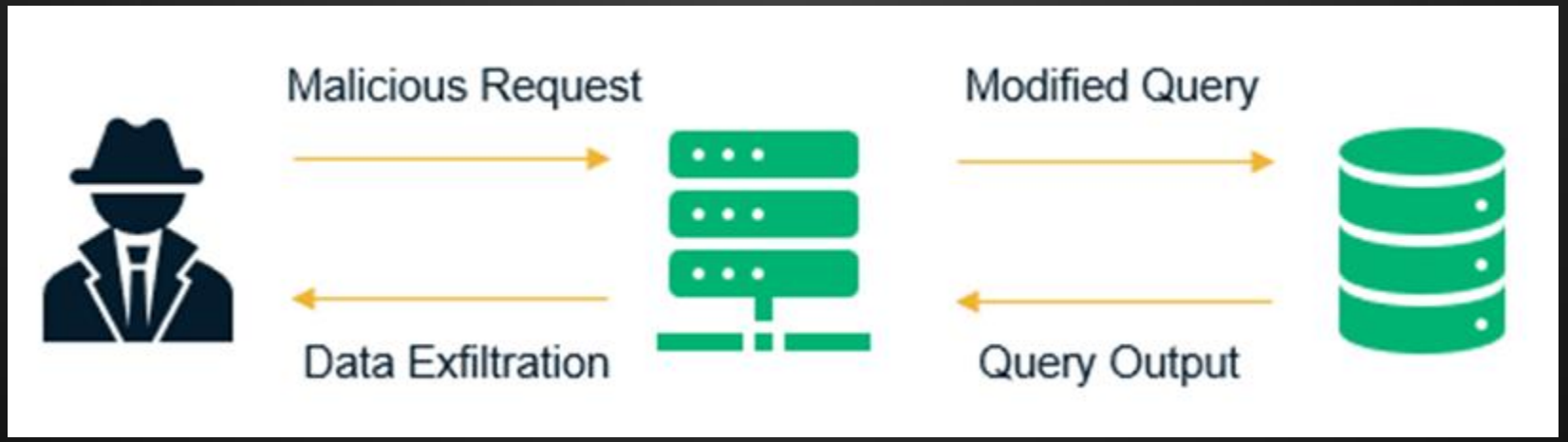
Spear Phishig

- E-mail or electronic communications attack
- Used to steal data or deliver malware
- Targeting a specific person or organization

Types of Attacks: Advanced

SQL Injection

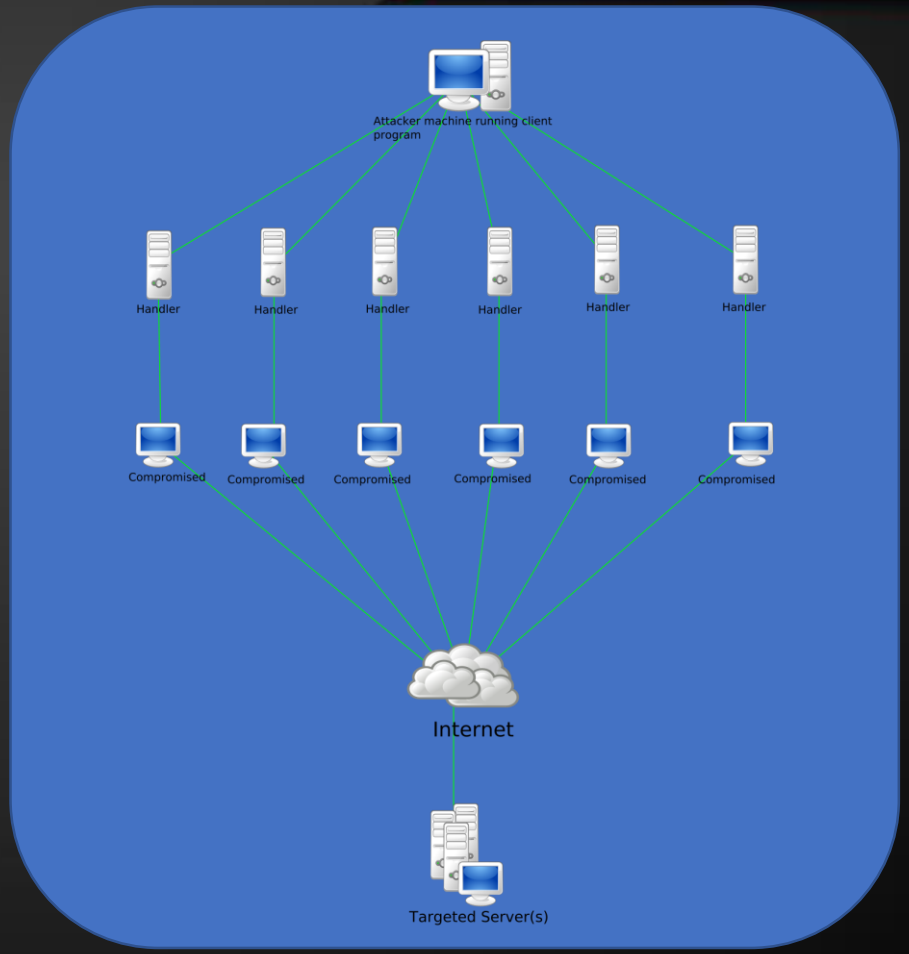
- Interferes with queries by an application
  - Delete or manipulate data



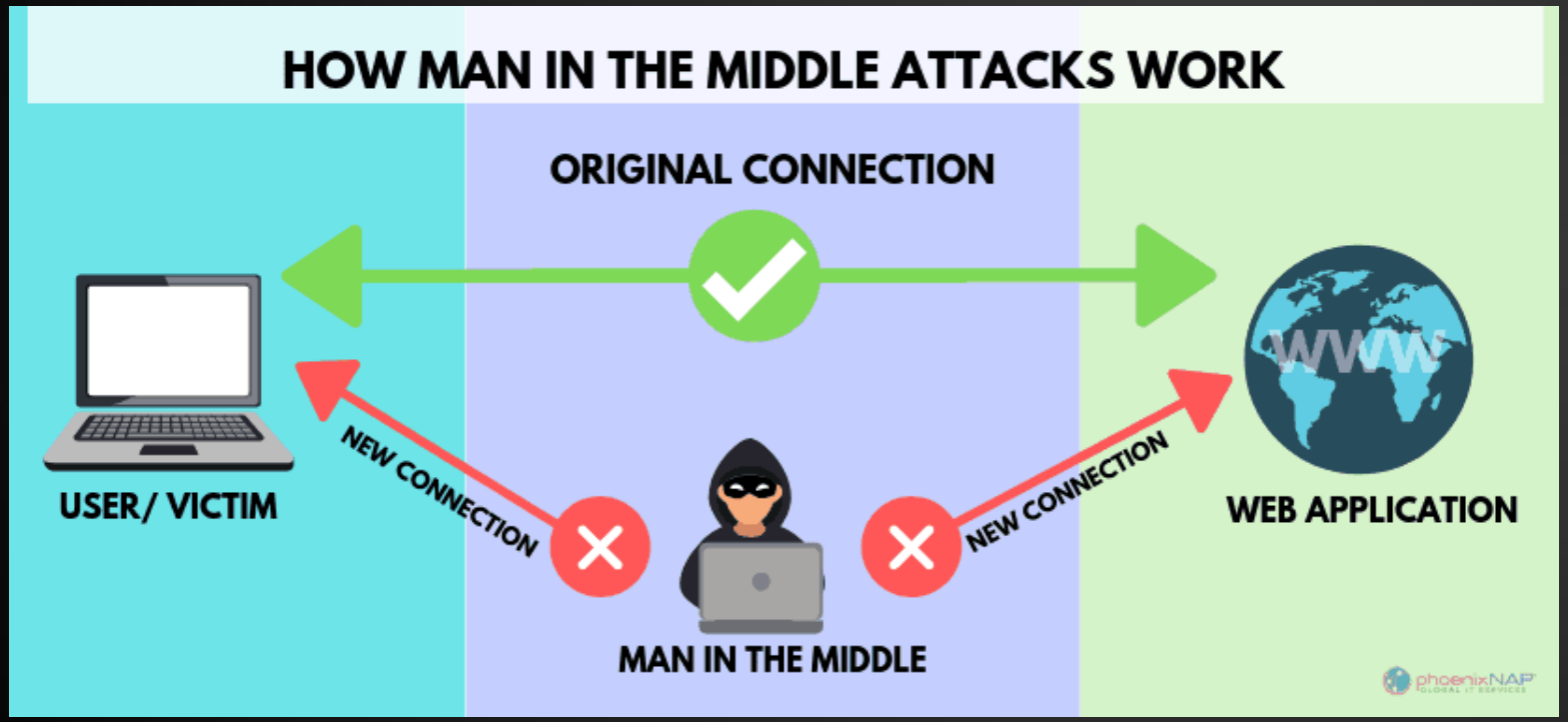
Types of Attacks: Advanced

DDoS -Distributed Denial o Service

- Perpetrator makes a machine or application unavailable.



Types of Attacks: Advanced



MITM – Man in the Middle

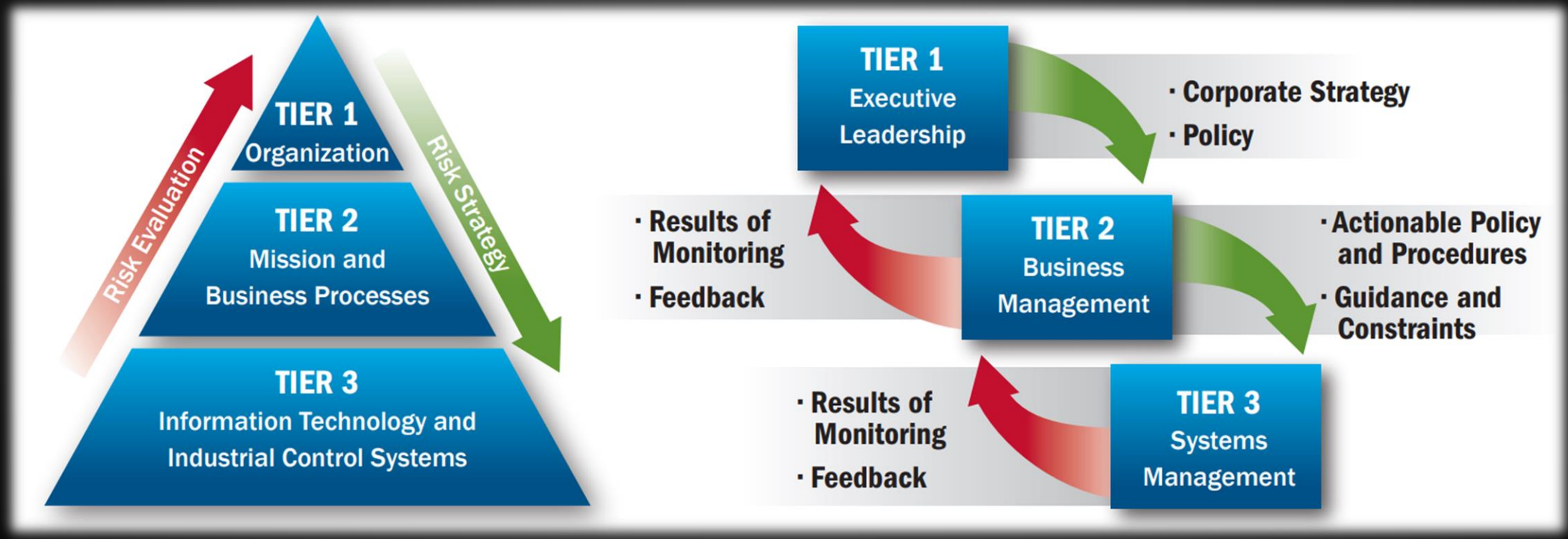
- Attacker makes two parties believe they are talking directly, but the attacker is controlling the conversation to gain intel

Multilayered Protection Plan

Defense in Depth (DiD)

- Risk Management
- Physical Security
- Security Monitoring
- Vendor Management
- Personnel Readiness and Compliance

Multilayered Protection Plan: Risk Management



Multilayered Protection Plan: Risk Management

Identify Threats: Asset Inventory/Survey

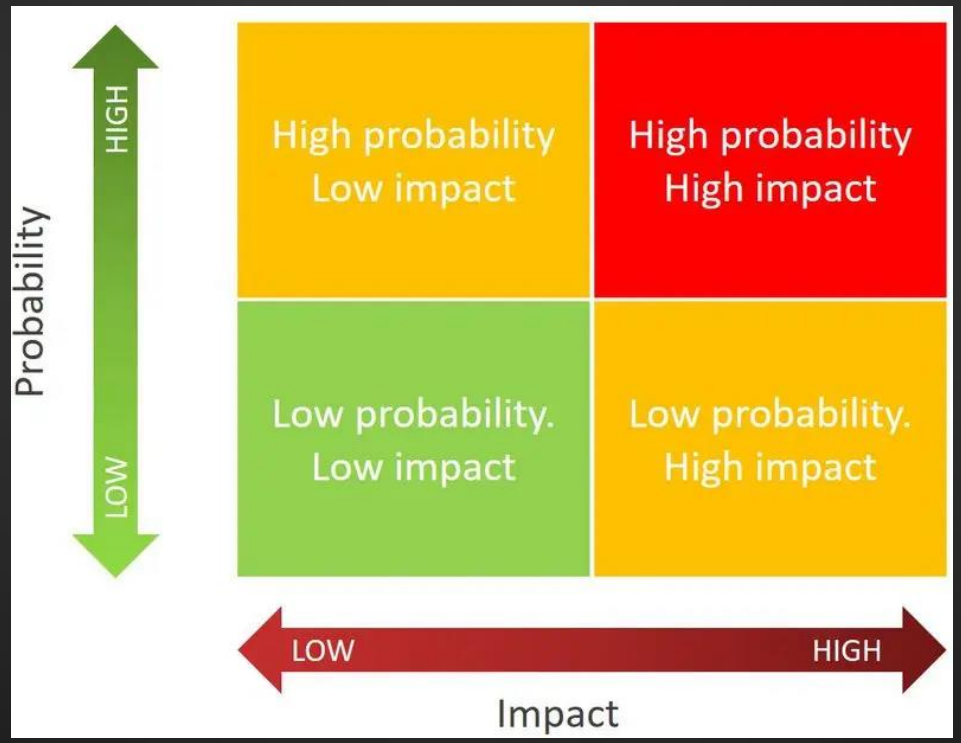
- What asset (information) needs to be protected?
- Why does the asset need to be protected?
- Who has the responsibility for managing and protecting the asset (what are the roles, responsibilities, accountabilities and authorities)?
- If the threat actor compromised the asset, what realistic worst-case scenarios would result?
- What is the value of the asset?
- What is the criticality of the process or information to the business mission?
- What are the protection levels for confidentiality, integrity, and availability?
- What interconnections are required for the systems to perform?
- What methods are currently available for user access?
- What dependencies are present for system functionality?
- How does the information flow through the system, and through what mechanisms?

Identify Threats: Known ICS Threats

- Insider intentional threats – disgruntled employees, vendors, systems integrators or anyone else with internal knowledge or access to the ICS
- Internal unintentional threats – inappropriate system design, policies, architectures, procedures, technologies or testing
- External nontargeted threats – maliciously designed software viruses and worms
- Malicious actors – “black hat” hackers, criminals, and nation states

Multilayered Protection Plan: Risk Management

Identify Threats: Determine Affects



Identify Threats: Identify Controls

- Critical process controls
- Controls that affect personnel or public safety

Identify Threats: Implement Security Controls

- Give priority to “High Impact/High Probability” affected assets
- Consider security controls as in integral part of the system life cycle
- Keep from implementing security controls that may create safety issues or collateral damage

Multilayered Protection Plan: Risk Management

Physical Security

- Reduces risk of accidental or deliberate loss or damage to assets including
  - Tools
  - Plant equipment
  - The environment
  - Surrounding community
  - Intellectual property
    - Proprietary data (e.g. process settings)

sider physical protection of cyber components and data as part of the

ntrols to the type of protection needed.

Cybersecurity

Multilayered Protection Plan: Risk Management

Physical Security: Physical Access

- Facility access controls
- ICS control and server room access
- Multifactor (for example, key card, card-and-personal identification number (PIN), or biometric) authentication for physical access
- Facility monitoring using cameras, motion detectors
- Alerting for device manipulation such as power removal, device resets, cabling changes, or the addition/use of removable media devices
- Visitor escort requirements and procedures.

Cybersecurity

Multilayered Protection Plan: Security Monitoring

What we are looking for:

- System changes
- Anomalous behaviors
- Attack signatures

Multilayered Protection Plan: Security Monitoring

Intrusion Detection System (IDS)

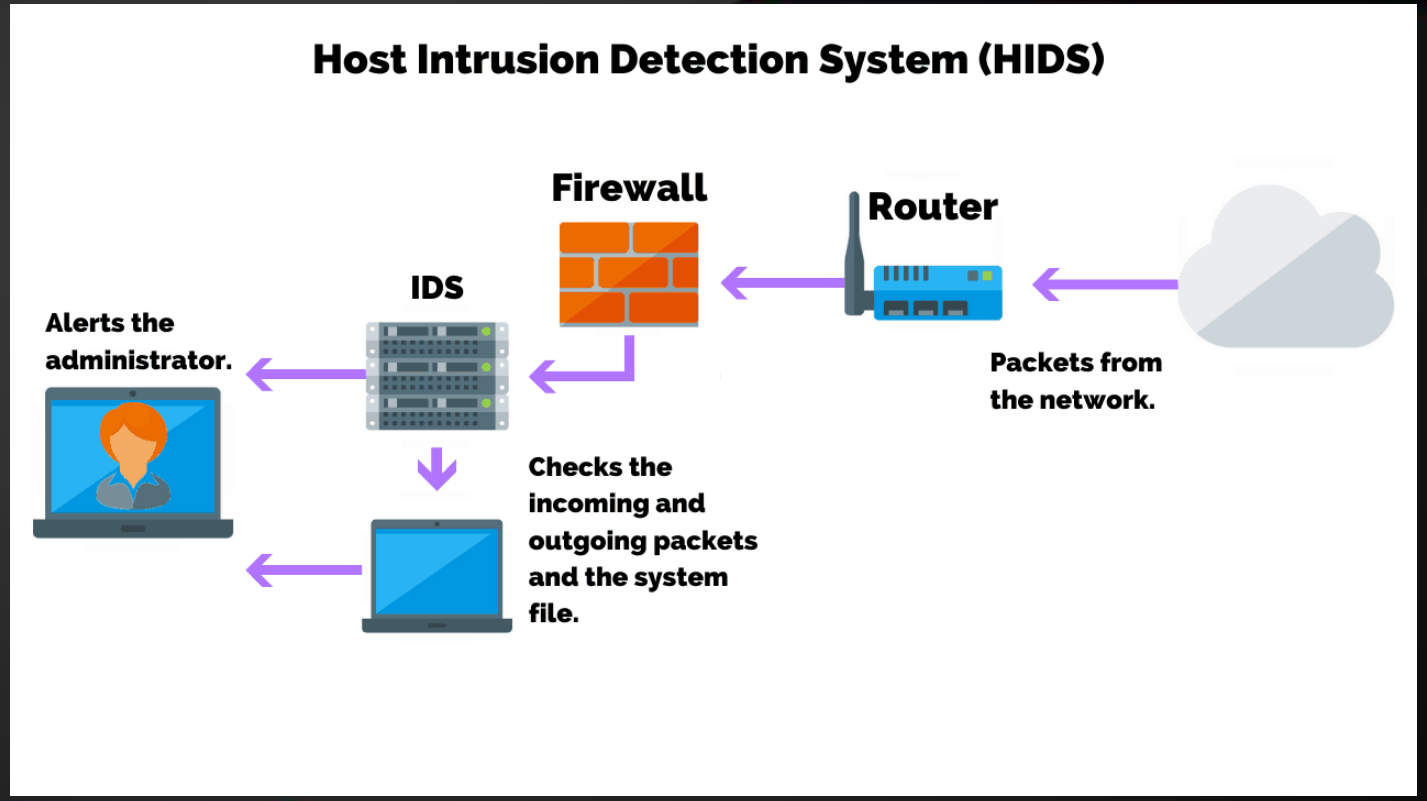
- Creates alarms for traffic outside normal operations
- Based on passive monitoring of network traffic

Intrusion Detection System (IDS)

How it works

Rules are written to monitor network traffic including

- IP source and destination
- Protocols
- Lengths of Packets



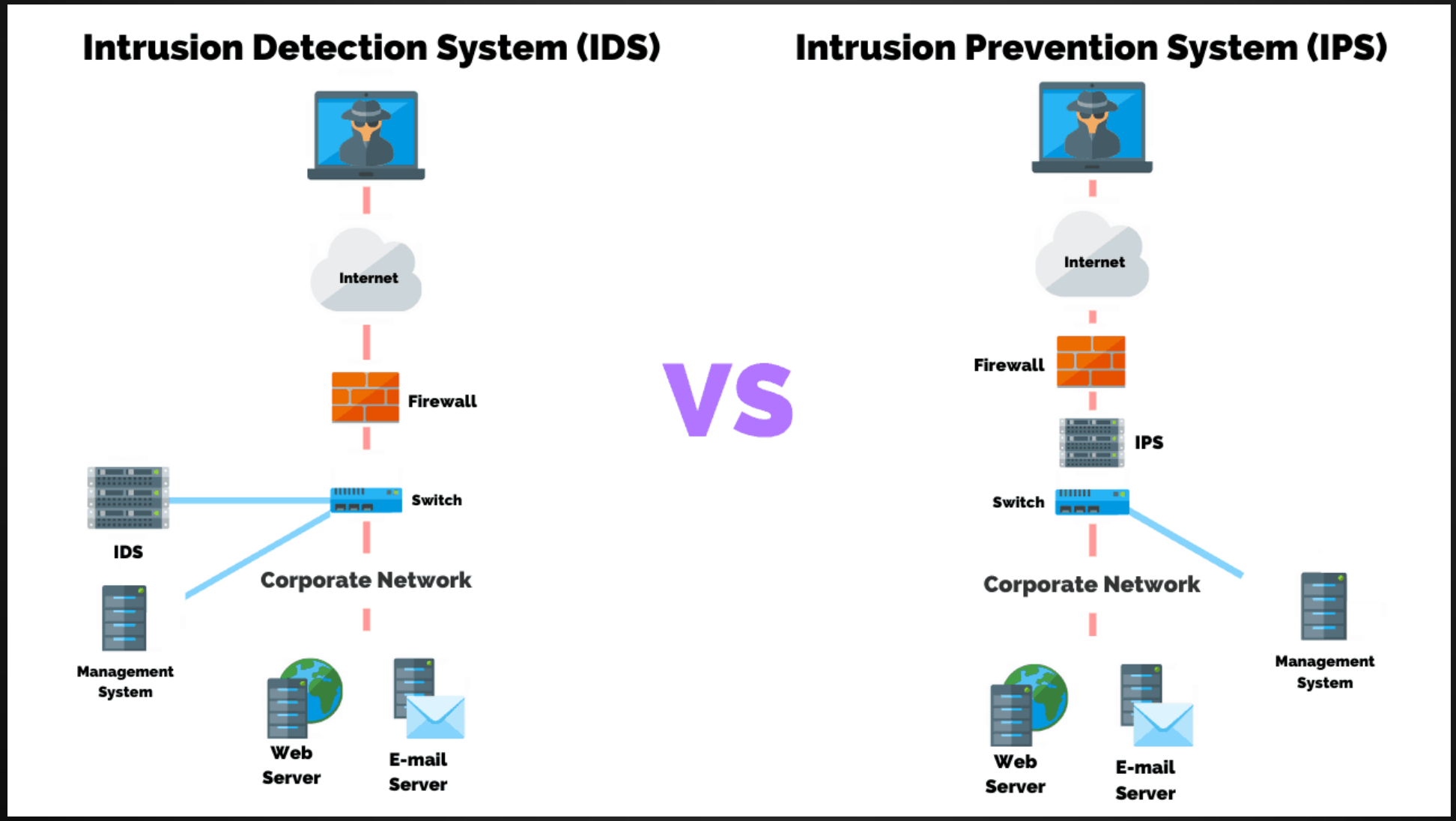
Multilayered Protection Plan: Security Monitoring

Intrusion Protection System (IPS)

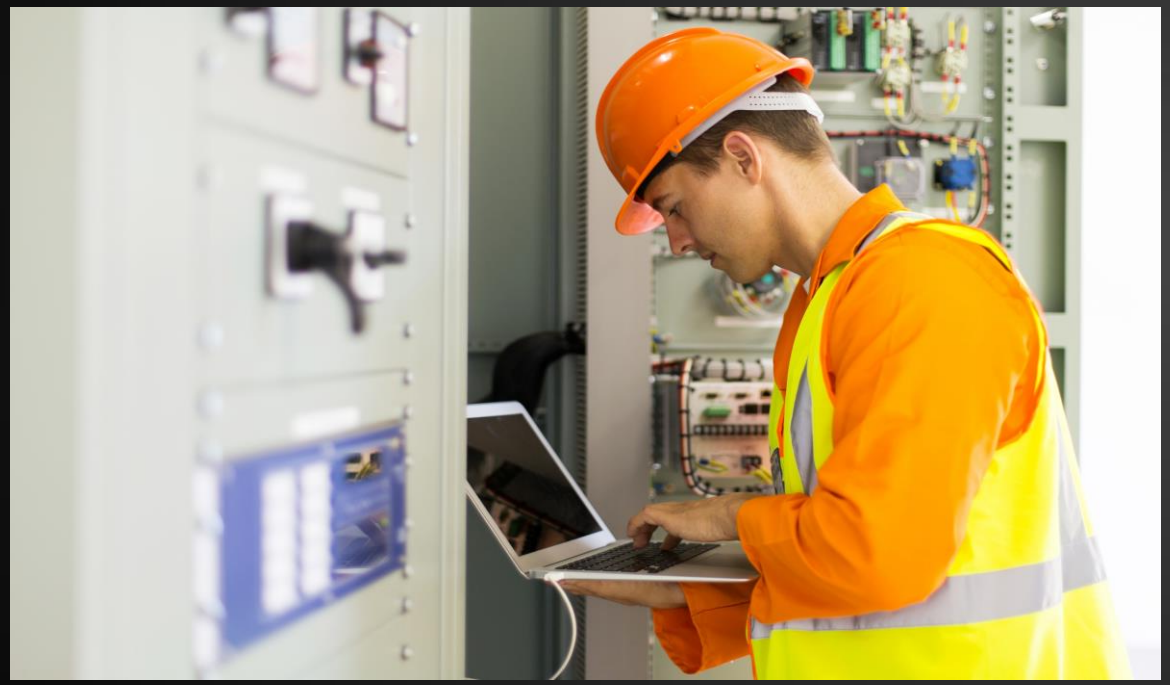
- Installed in line with firewalls and ICS equipment
- Blocks traffic that does not meet defined rules

Intrusion Protection System (IPS)

An IPS drawback is that it can stop critical processes if not configured properly.


Intrusion Detection System (IDS)
Internet
Firewall
Switch
IDS
Corporate Network
Management System
Web Server
E-mail Server
VS
Intrusion Prevention System (IPS)
Internet
Firewall
IPS
Switch
Corporate Network
Management System
Web Server
E-mail Server

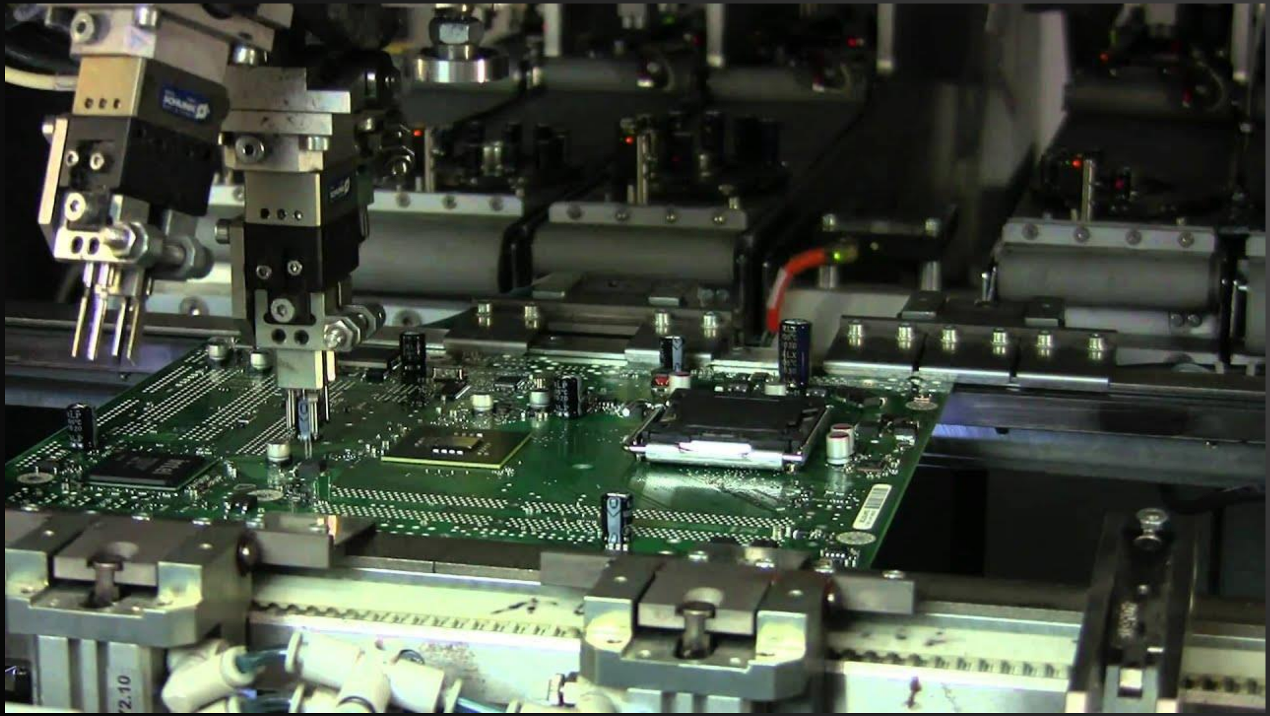
Multilayered Protection Plan: Vendor Security Management



- Many vendors are aware of the importance of cybersecurity
- Many vendors have incorporated security into products and procedures
- Should not assume that all are implementing security
- The organization should present and address requirements early in the relationship

Multilayered Protection Plan: Vendor Security Management

Supply Chain



Significant Risk

- Manufacturers and developers from different locations around the world
  - Many points of contact and exposure lead to compromising equipment
- Unauthorized back door software
- Poor procurement agreements and quality control by the vendor

Actions to Mitigate Risk

- Quality procurement agreements
- Qualify the vendor's quality control
  - Testing
  - Vulnerability Scanning

Cybersecurity

Multilayered Protection Plan: Personnel Readiness and Compliance

Policies

- Clear and actionable
- Create a framework for rigorous security control procedures
- Outline rules
- Sanctions / Consequences for noncompliance

Multilayered Protection Plan: Personnel Readiness and Compliance

Procedures

- State how personnel should conduct a particular process
- Ensure secure functioning and provide a standard, repeatable means to accomplish a task in a safe manner across the OT space

Multilayered Protection Plan: Personnel Readiness and Compliance

Training

- Personnel should be aware of potential loss and safety threats
- How it identify indications of cyber threats
- How to assist the vendor monitoring and controls
- Understanding that feedback as to how the policies and procedures implemented affect operations is critical for the organization’s safety strategy

Multilayered Protection Plan: Security Actions

First Steps

1. Identify, minimize, and secure all network connections to the ICS.
2. Harden the ICS and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.
3. Continually monitor and assess the security of the ICS, networks, and interconnections.

4. Implement a risk-based defense-in-depth approach to securing ICS systems and networks.
5. Manage the human – clearly identify requirements for ICS; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide ICS security training for all operators and administrators.

Cybersecurity

Closing Remarks

Control systems will grow more connected

Attacks will happen

All organizations should have an OT Cybersecurity Plan

Many measures are common practice and easy to implement

Cybersecurity

For more information contact:

Jason Rayle
jrayle@pteinc.com
330.692.3506

PRO-TECH SYSTEMS GROUP

Cybersecurity