AI OFFENSIVE AND DEFENSIVE CYBERSECURITY SCENARIOS
USE CASE: ELECTRIC UTILITY SUBSTATION

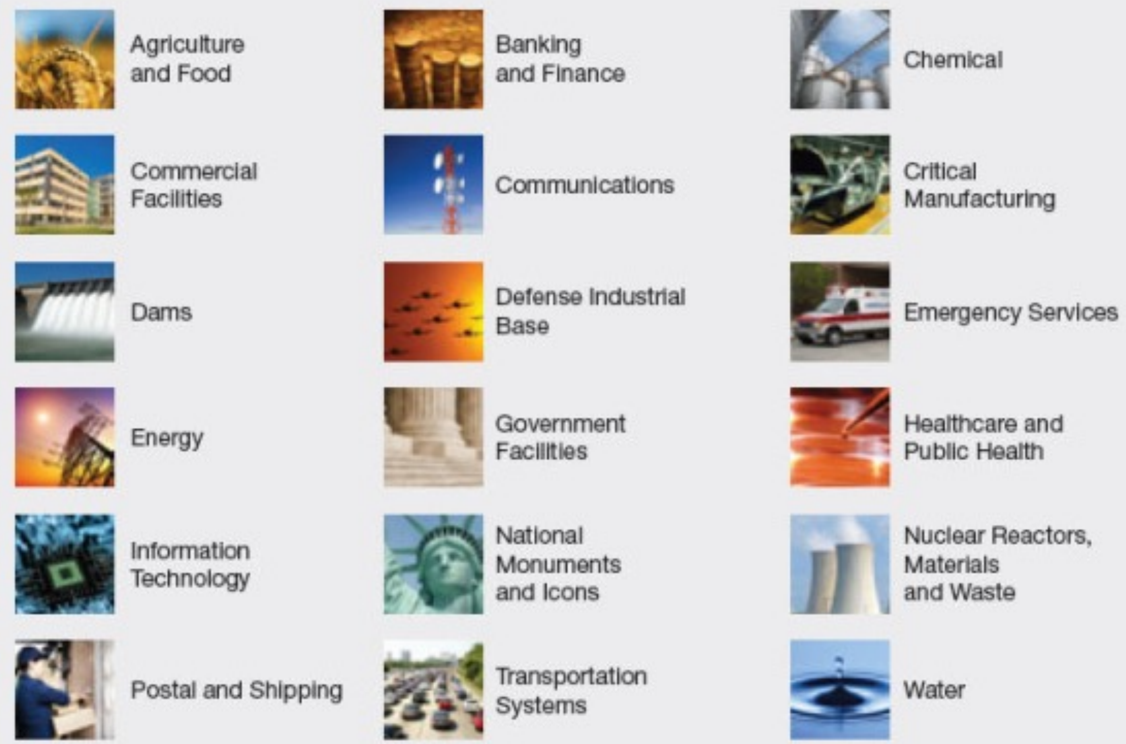
Alex Dely
CII CTO
DHS Industrial Controls Joint Working Group
Raytheon Advanced technology Mission Area (Retired)
Adjunct, College of Engineering SIE Department
ADely@CII-International.com
Adely@niketllc.com

10th Annual Cyber Workshop
Tucson, UA Tech Park

16 Flavors of Artificial Intelligence

- Sensor Hardware/Software/Firmware in Find/Fix/Track/Target/Engage/Assess
- Collaborative Autonomy
- Supervised vs Unsupervised Learning
- Reinforcement Learning
- Symbolic AI
- Advanced Modeling and Simulation
- Advanced Heuristics
- Convolutional Neural Networks
- All-Source Intelligence Fusion
- Cognitive Amplifiers
- Design of Experiments and Bayesian Networks
- Genetic Algorithms
- Intelligent Agents
- Decision Process Optimization
- Natural Language Processing (Generative LLM)
- Ontological Reasoning

Dept. of Homeland Security's 16 Critical Infrastructure Sectors



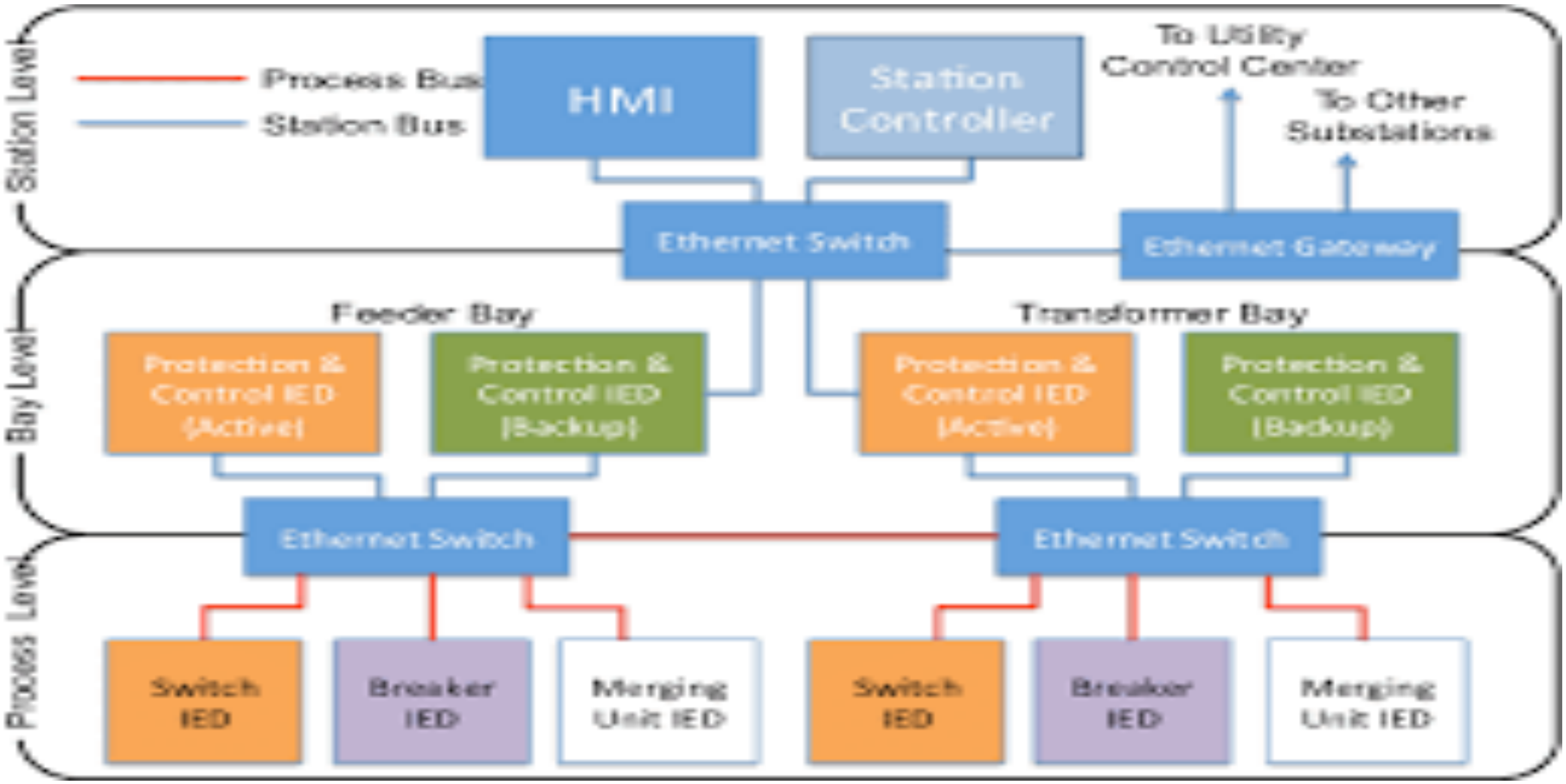
Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Complex Interactions With Corresponding
Government - Industry Expertise & Accountability

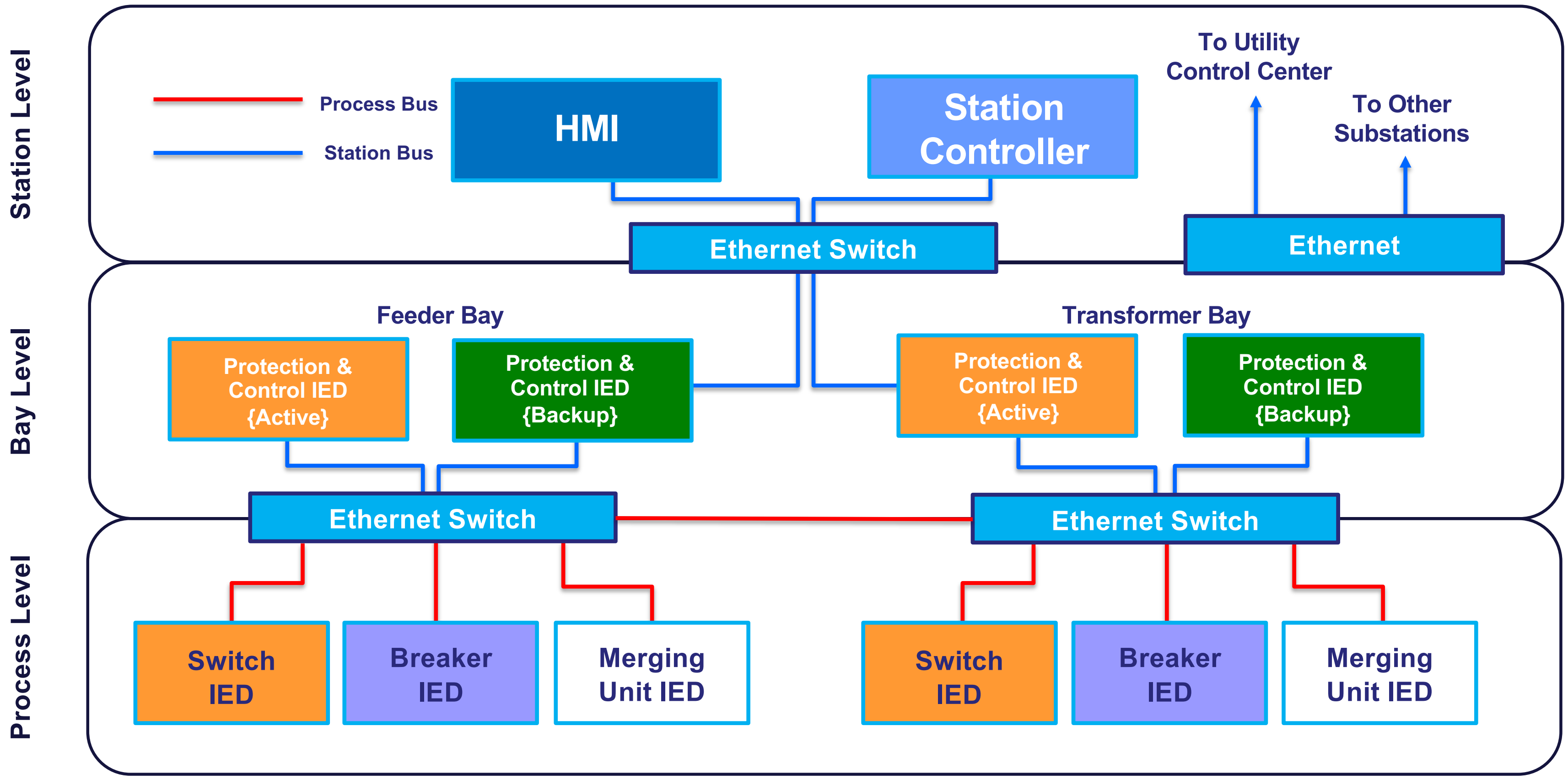
Typical Electric Utility Substation Layout

1. Primary Power Lines
2. Ground wire
3. Overhead lines
4. Potential transformer
5. Disconnect switch
6. Circuit breaker
7. Current transformer
8. Lightning arrester
9. Power transformer
10. Control building
11. Security fence
12. Secondary power line

Typical Industrial Control Systems (ICS) Managing Substation



Typical Industrial Control Systems (ICS) Managing Substation



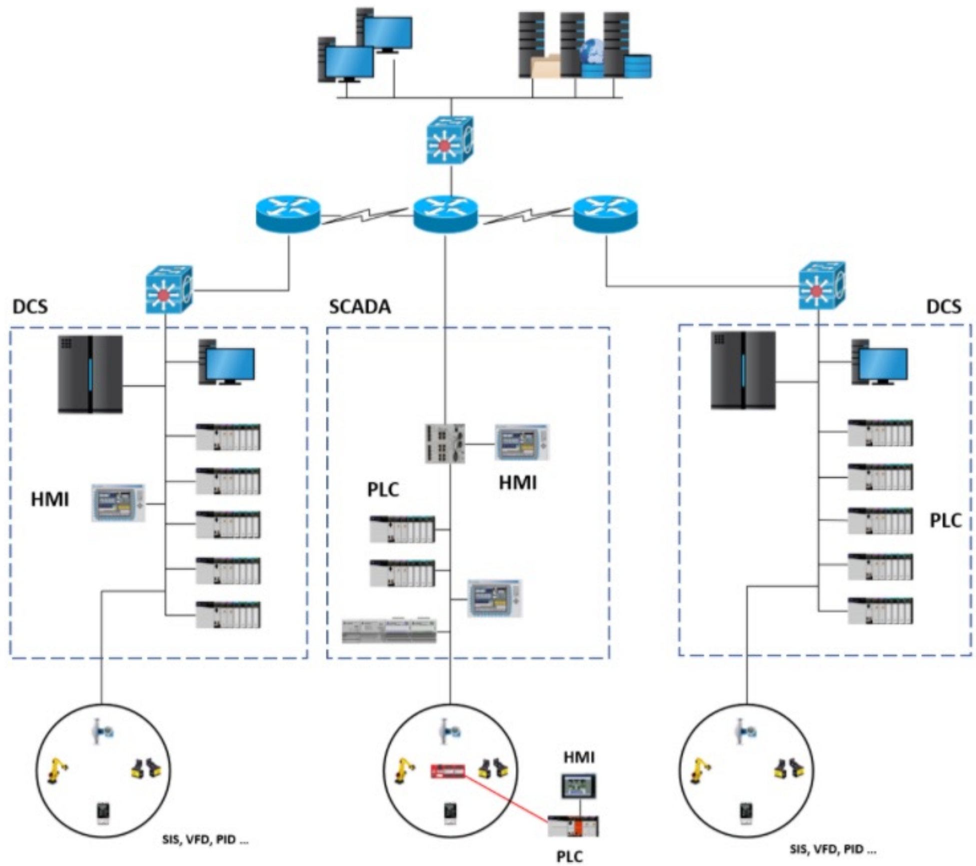
Typical Subsystems in an ICS

1) **Distributed Control Systems (DCS):**
   - Control Server
   - Input / Output Server
   - SCADA Server or Master Terminal Unit (MTU)
   - Data Historian

2) **Programmable Logic Controllers (PLC)**
   - Power Supply
   - Communications Module
   - Control Processor
   - Sensors and other Input Modules
   - Actuators / other Output Modules

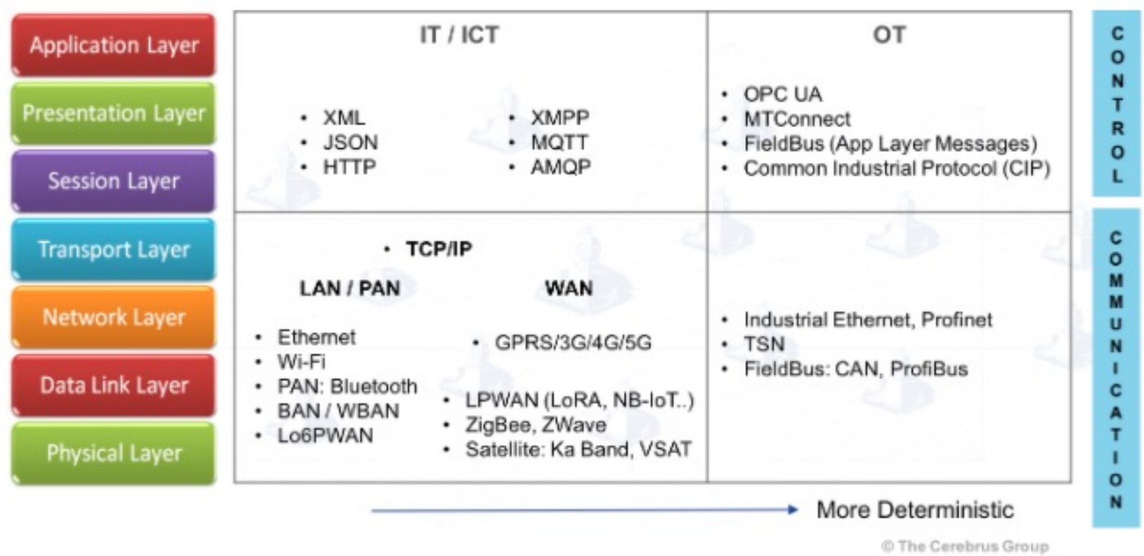
3) **Human Machine Interfaces (HMI)**

4) **Safety Instrumentation System**
   - In parallel to, and separate from, the normal process control system



Most Common Types of ICS Communication Protocols

- There are literally hundreds of protocols used in different ICSs
- Some of the most common include:
  - Modbus and Modbus TCP/IP
  - Process Field Net (PROFINET)
  - EtherNet/IP
  - HTTP
  - File Transfer Protocol (FTP)
  - Telnet
  - Address Resolution Protocol (ARP)
  - Internet Control Message Protocol (ICMP)

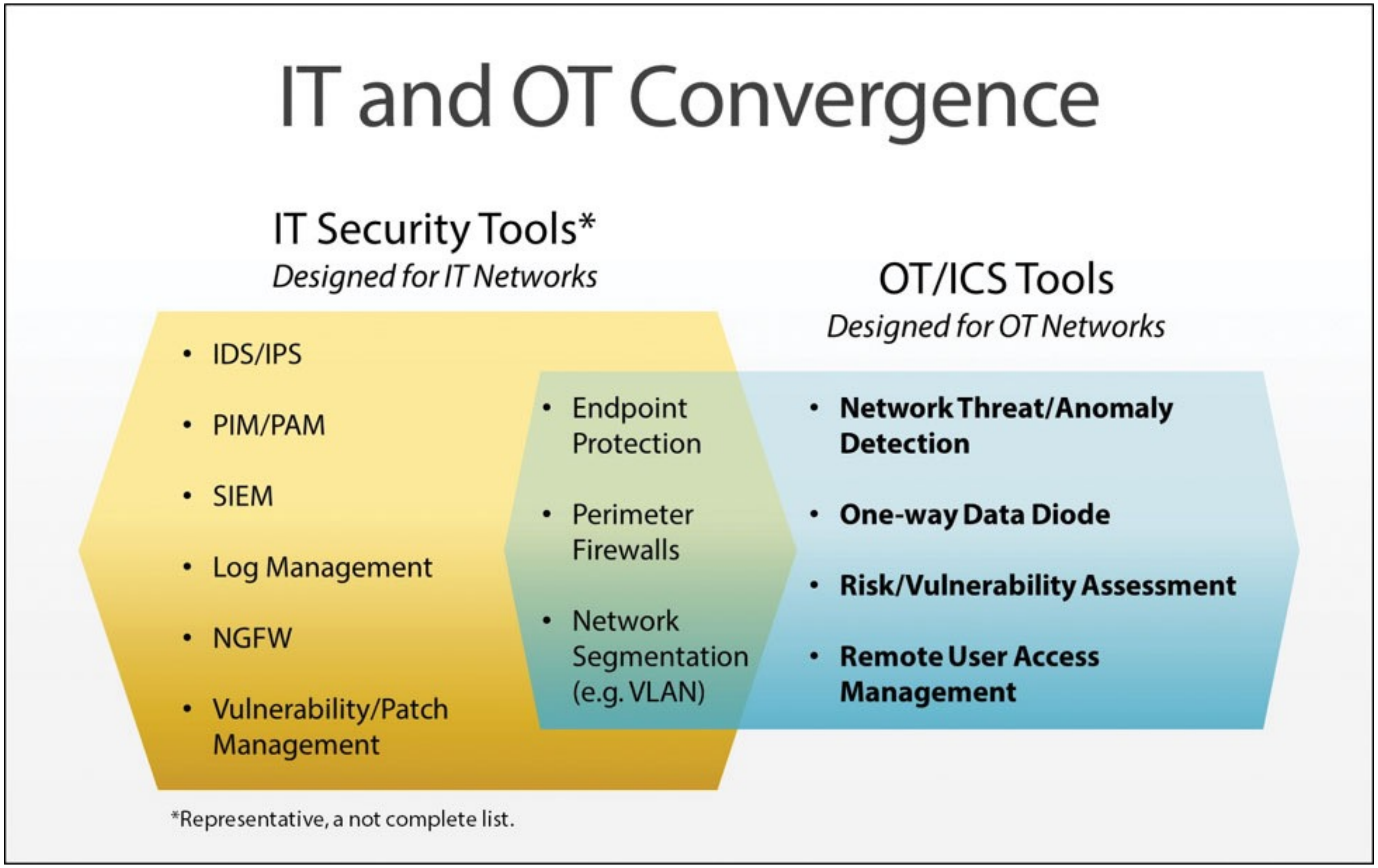


Standards of Control and Communication, Image Credit: The Cerebrus Group

Many Protocols are Insecure by Inheritance

[Industrial control system communication media and protocols - Industrial Cybersecurity (packtpub.com)]

IT and OT / ICS Security Tools Convergence



IT vs OT ….From a Security Perspective

IT vs. OT

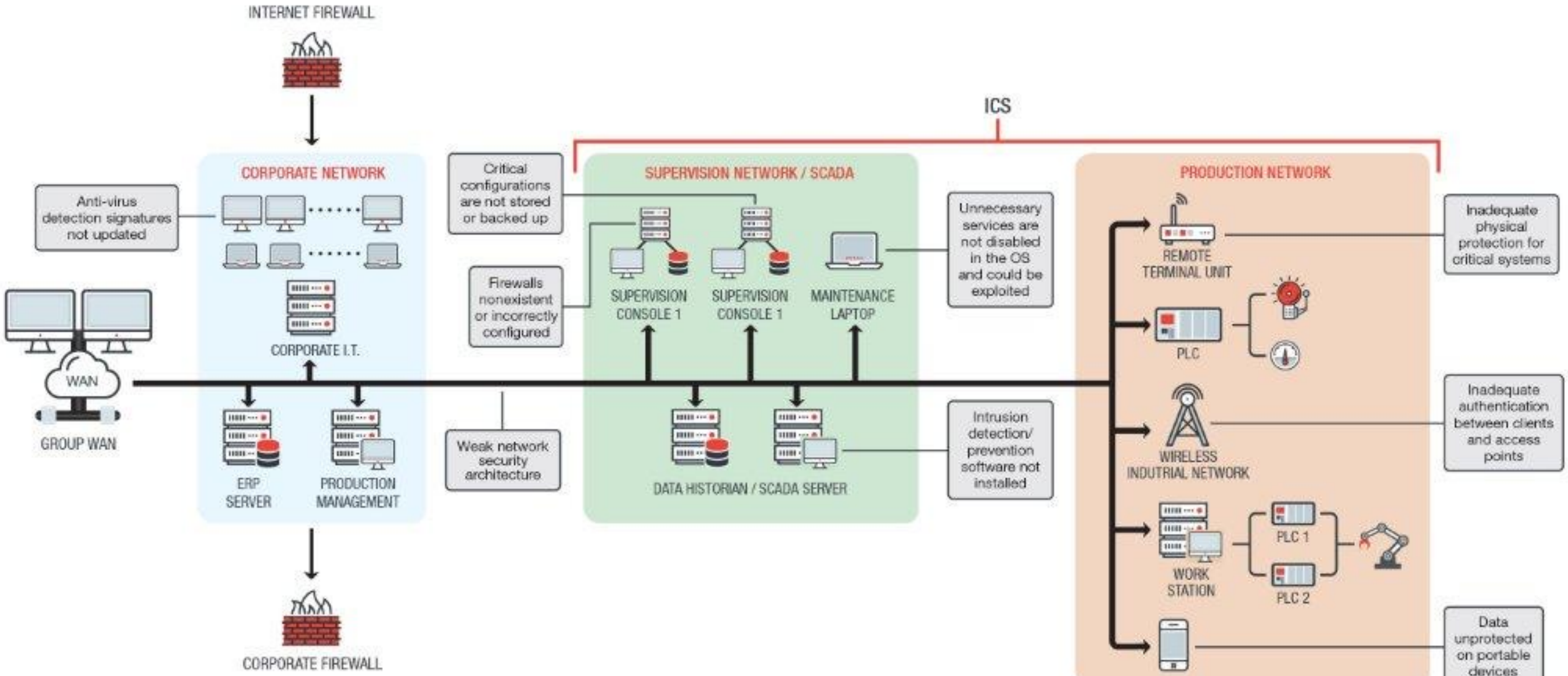
SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	Can be difficult to deploy
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	Up to 40+ years
OUTSOURCING	Common/widely used	Rarely used (vendor only)
APPLICATION OF PATCHES	Regular/ scheduled	Slow (vendor specific, compliance testing required)
CHANGE MANAGEMENT	Regular/ scheduled	Legacy based – unsuitable for modern security

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
TIME CRITICAL CONTENT	Delays are usually accepted	Critical due to safety
AVAILABILITY	Delays are usually accepted	24 x 7 x 365 x forever (Integrity also critical)
SECURITY AWARENESS	Good in both private and public sector	Generally poor inside the control zone
SECURITY TESTING/ AUDIT	Scheduled and mandated	Occasional testing for outages / audit for event recreation
PHYSICAL SECURITY	Secure	Traditionally good

Select Critical ICS / SCADA System Vulnerabilities

- Exposure over the Internet
  - Many ICS systems are connected to the internet
  - Insecure connections can allow backdoor access to the ICS environment
- Weak Segregation
  - Many ICS systems are architected with weak segregation between the IT and OT environments
  - Can allow an IT device /machine to reach a device on the ICS network
  - Malware can spread from one device to another
- Default Configuration
  - Some companies do not regularly update patches to their ICS networks
    - Lack of awareness
    - Don’t want to incur production downtime (resulting in lost revenues)
  - False security in thinking that the ICS network is isolated and not reachable

ICS Threat Landscape



Top Substation Attack Mechanisms

1. Wiper Malware to disrupt operations, including physical damage
2. Transformer Electronics Ransomware and Transformer Supply Chain
3. Denial of Service to OT/IT networks
4. Defensive AI at OT/Substations
    - Real-time threat detection among massive datasets (Unusual behavior/anomalies)
    - Automated RMF/Risk Prioritization-Based Response to Vulnerabilities
    - Enhanced Authentication/Reduced Human Error
5. Offensive AI at OT/Substations
    - Kill Chain Attack Automation/Scaling against System Weaknesses
    - Polymorphic Malicious Code automated to learn from failed attacks

Top Substation Vulnerabilities for Attack Mechanisms

Primary Attack Mechanism	Most Relevant Vulnerabilities
1. Wiper Malware	Weak Segregation • Exposure over Internet • Weak Protocols • Default Configuration • Insider Threat • Malware Vectors (USB/PDF) • Technical/Physical Malfunctions
2. Transformer Ransomware / Supply Chain	Third-Party Threats • Supply Chains • Weak Segregation • Weak Applications • Default Configurations • Exposure over Internet
3. DoS on OT/IT Networks	Weak Protocols • Exposure over Internet • Weak Segregation • Technical Malfunctions • DoS-specific Vulnerabilities
4. Defensive AI Use Cases	Lack of Awareness • Weak Segregation • Default Configurations • Weak Protocols/Apps • Human Error • Authentication Weaknesses
5. Offensive AI (Kill Chain Automation / Polymorphic Malware)	Weak Protocols • Weak Apps • Lack of Awareness (phishing) • Insider Threat • Weak Segregation • Default Configurations

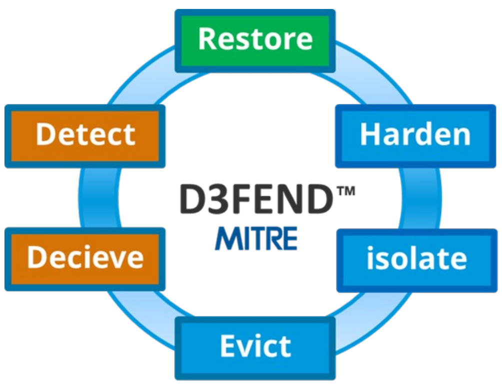
Likely ICS Attack Vectors

Typical Attack Vectors

* Force Listen Only Mode
* Clear Counters/Registers
* Unauthorized Read/Write Requests to PLC
* Denial of Service Attack
* Slave Device Busy Code Delay/Interruption
* Cold/Warm Restarts from Clients
* Timing Change Attempt
* Spoofing
* Replay
* COTP Disconnect
* *xxxx*-bit Asymmetrical Encryption Keys
* Reboot/Restart/Unlock PLC/Stop Detect/Remote Change Detect/Software Upload from (Un)Authorized Client
* Restart Communication Option
* Change Client/Servicer ID
* Incorrect Packet Size
* Function Code Scan
* Unsolicited Response Storm
* Broadcast Request from Client
* Failed Check Sum
* Eavesdropping
* Unauthorized Connection Query
* Invalid OSI-SSEL/PSEL
* Overlapping Link Certificates

EVOLVED DEFENSE – HARDENING NETWORKS

DETECT & RESPOND + PREEMPTIVE PROTECTION

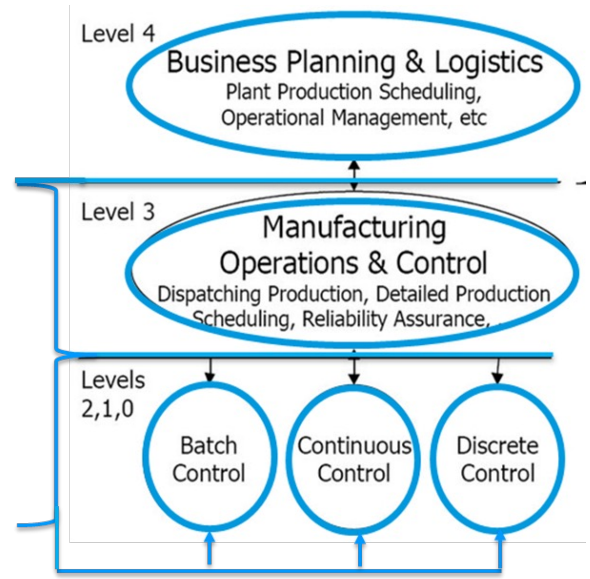


MITRE D3FEND™ Framework

Preemptive Zero Trust Protection for Critical Assets, Data, & Operations

CyberCloak™

Data Privacy Facility (DPF) protocols and methodologies autonomously isolate, contain, authenticate, and encrypt processes and data-in-transit



Purdue Enterprise Reference Architecture (PERA)

"By 2030 preemptive cybersecurity solutions will account for 50% of the IT security spending, up from less than 5% in 2024, and replace tractional "stand alone" detection and response solutions as the preferred approach to defend against cyberthreats." - Gartner July 2025

Black Fur

NIKET

HIGH ENTROPY SECURITY

Zero-Trust Approach for Power Infrastructure

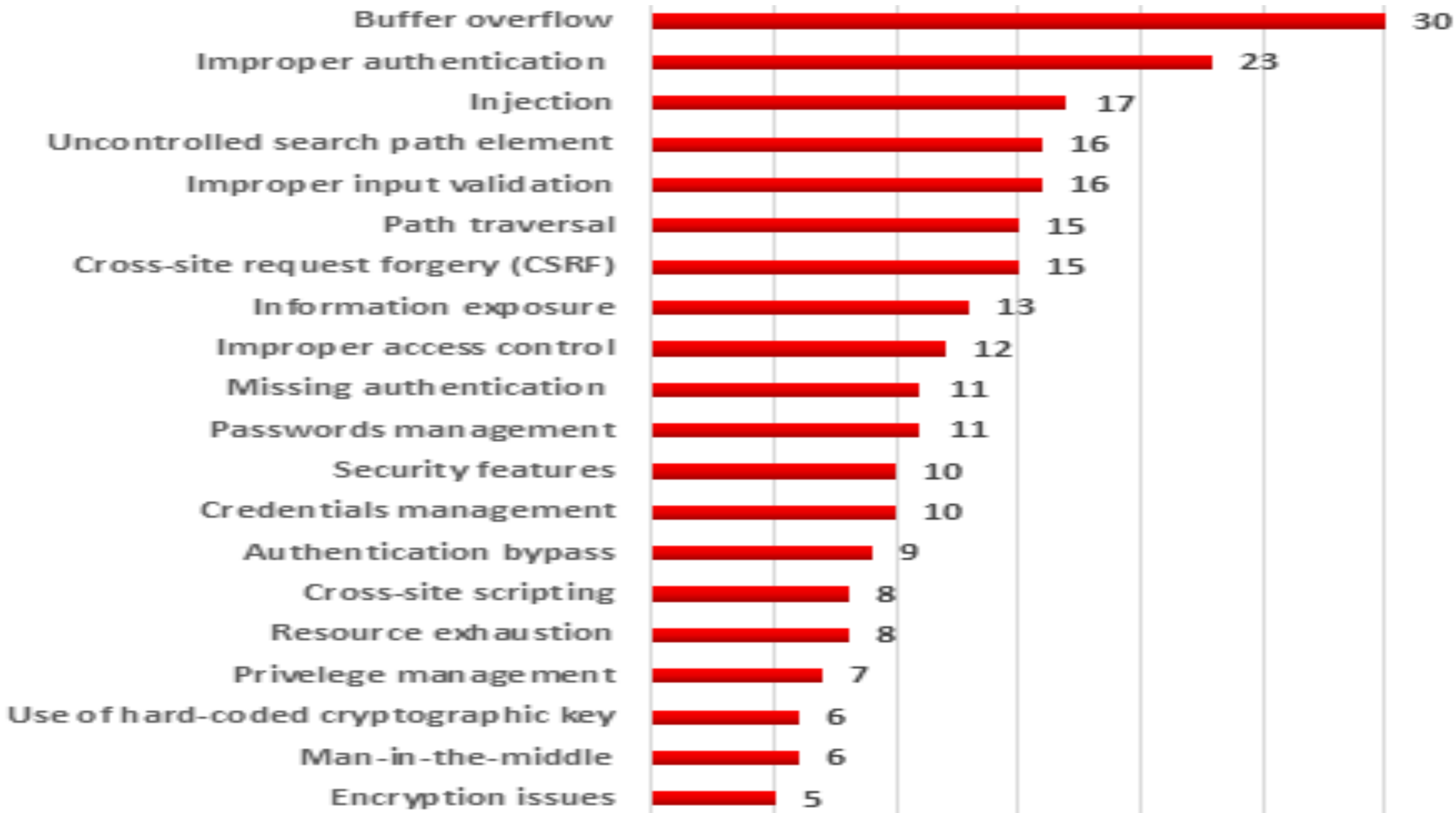
1. Securing cryptographic keys on OT equipment → Ephemeral Keys regenerated on demand using patented Challenge-Response Pair (CRP) mechanisms.

2. Securing packet-based communications against cyberattacks despite weak or intermittent connectivity. → Secure communications under jamming or poor connectivity, even with 45% noise / bad bits in the packet.

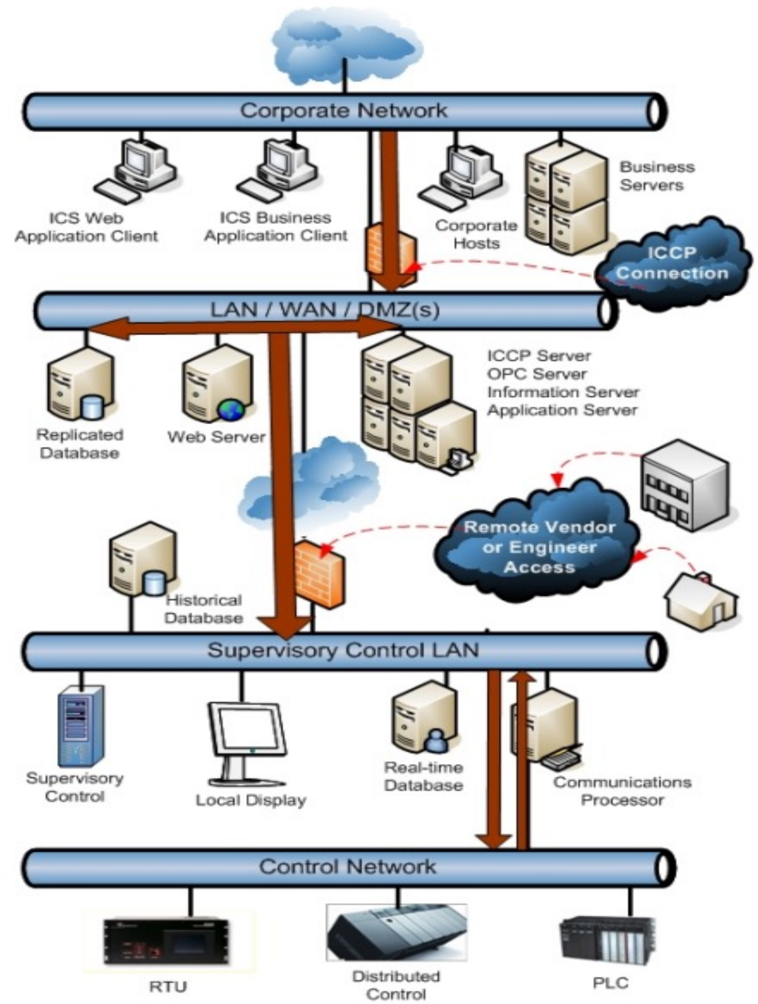
3. Protecting substation sensors from spoofing and malfunction → Resilient Sensor Fingerprinting for real-time monitoring

BACKUP

ICS Vulnerability by Attack Mechanism II

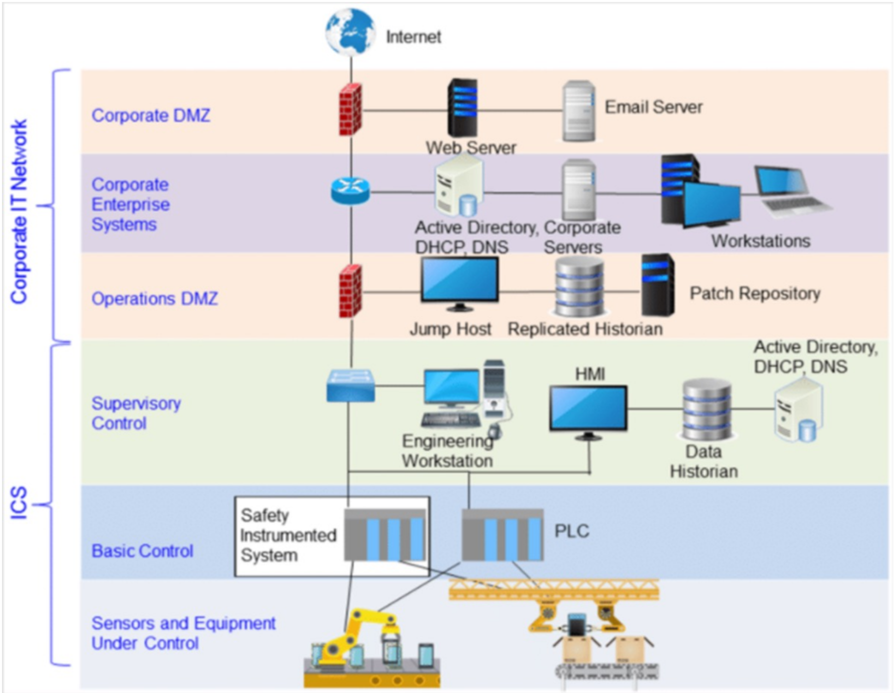


Potential Attack Vectors Between ICS Network Security Zones



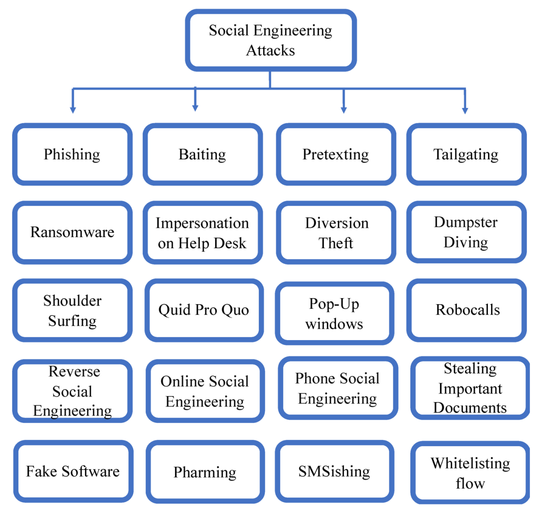
ICS / SCADA System Vulnerabilities

- Exposure over the Internet
  - Many ICS systems are connected to the internet
  - Insecure connections can allow backdoor access to the ICS environment
- Weak Segregation
  - Many ICS systems are architected with weak segregation between the IT and OT environments
  - Can allow an IT device /machine to reach a device on the ICS network
  - Malware can spread from one device to another
- Default Configuration
  - Some companies do not regularly update patches to their ICS networks
    - Lack of awareness
    - Don’t want to incur production downtime (resulting in lost revenues)
  - False security in thinking that the ICS network is isolated and not reachable



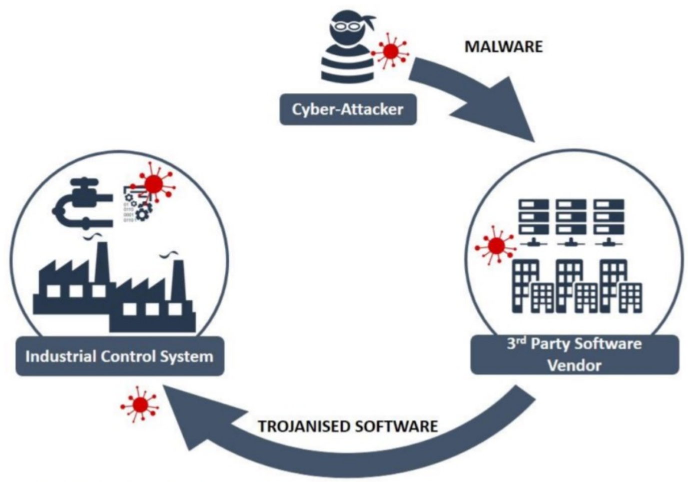
ICS / SCADA System Vulnerabilities

- Weakness in ICS Protocols
  - Older systems were not designed with security in mind and have not been updated or enhanced
  - For example:
    - No authentication
    - No encryption
- Weakness in ICS Applications
  - Some applications that reside on the ICS networks are vulnerable to various types of attacks
  - For example:
    - SQL injection, Command injection, or data manipulation
    - Credential sniffing
    - Cross-site scripting / session hijacking
- Lack of Security Awareness
  - Employees are not adequately trained on the cyber attack techniques
  - Some examples include:
    - Social engineering
    - Phishing
    - Spearphishing attacks



ICS / SCADA Systems Threats

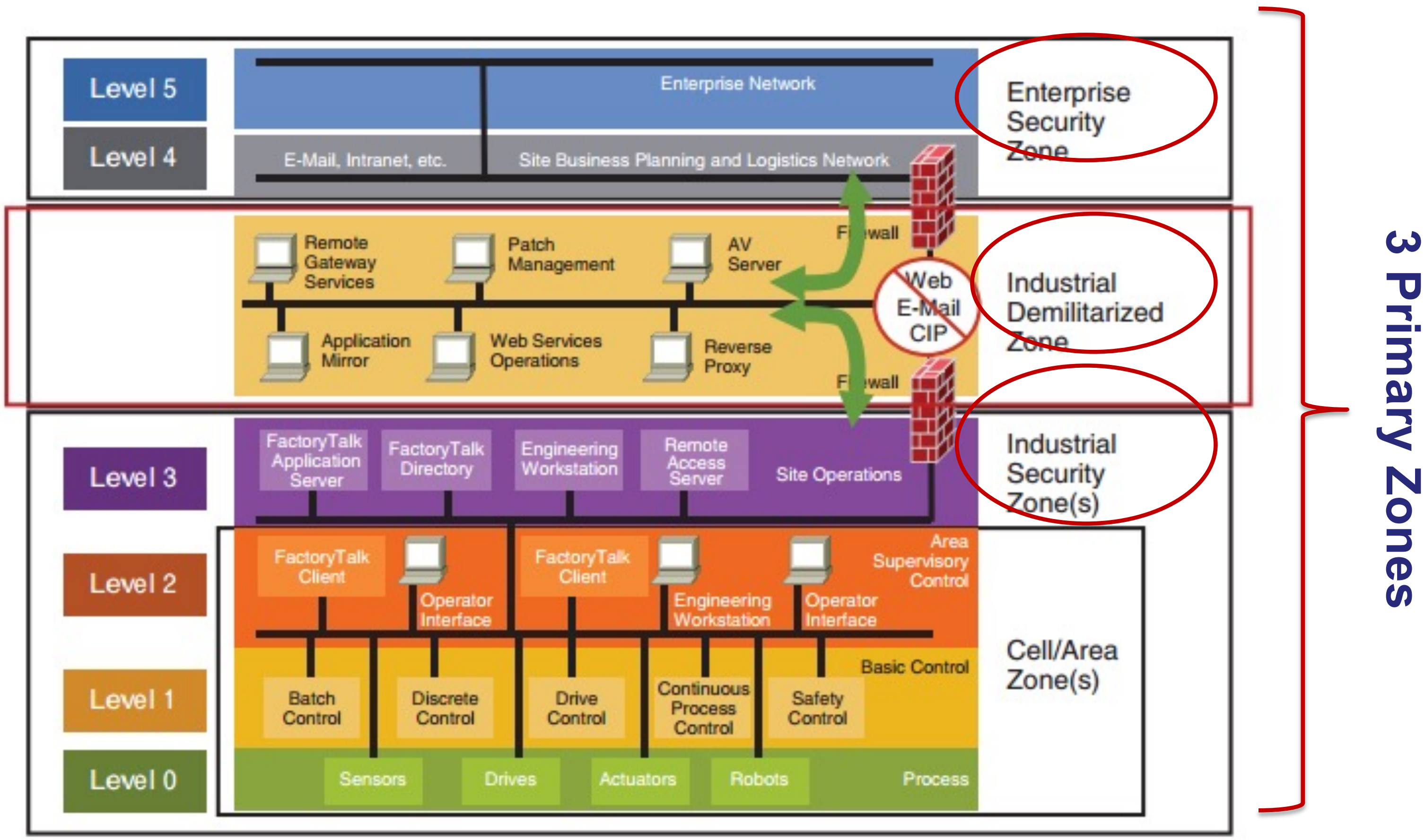
- Third party threats
  - Supply chain threats
  - For example:
    - Infected machines of outsourced services or support staff
    - Compromised parts / components introduced to the ICS network
- Technical or physical malfunctions
  - Component-level failure
    - Hard disk failures and system crashes
    - Run time errors
    - Power or other physical means of disruption with no backup capability
- Threats from terrorists and hackers
  - CI elements are key targets for terrorists and hackers
  - Can cause significant damage leading to financial loss, damaged company reputation and even loss of life

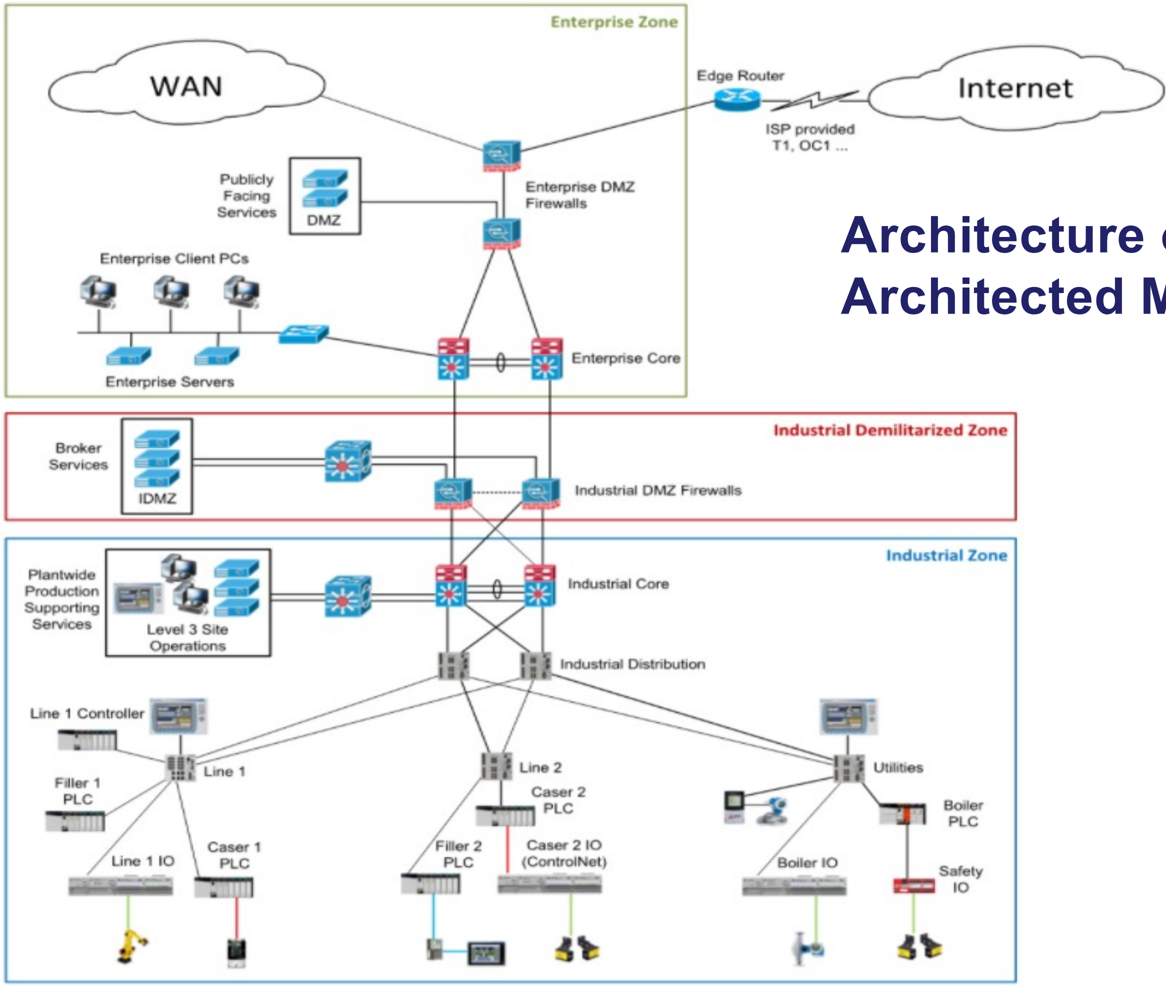


Examples of Typical ICS Attack Vectors

- Improper authentication:
  - Authentication bypass, e.g. client-side authentication
  - Use of standard IT protocols with clear-text authentication
  - Unprotected transport of ICS application credentials
- Improper access controls (authorization):
  - Wireless LAN access that can be used to get to the control network
  - Blank system administrator password on a Microsoft SQL Server database, which allows remote administrator access to the database and the server itself
  - VPN configuration problems that unintentionally allow clients unfettered access to the corporate, DMZ, or control LAN
  - System management software that allows central management of multiple servers may allow an attacker easy access to the same hosts
  - Common processes (any process that is installed and listening on multiple boxes), which if compromised, provide access to multiple hosts
  - Weak firewall rules
  - Circumvented firewalls
  - Shared printers that span security zones (A network transition that does not traverse the firewall)
  - Unsecure network device management.

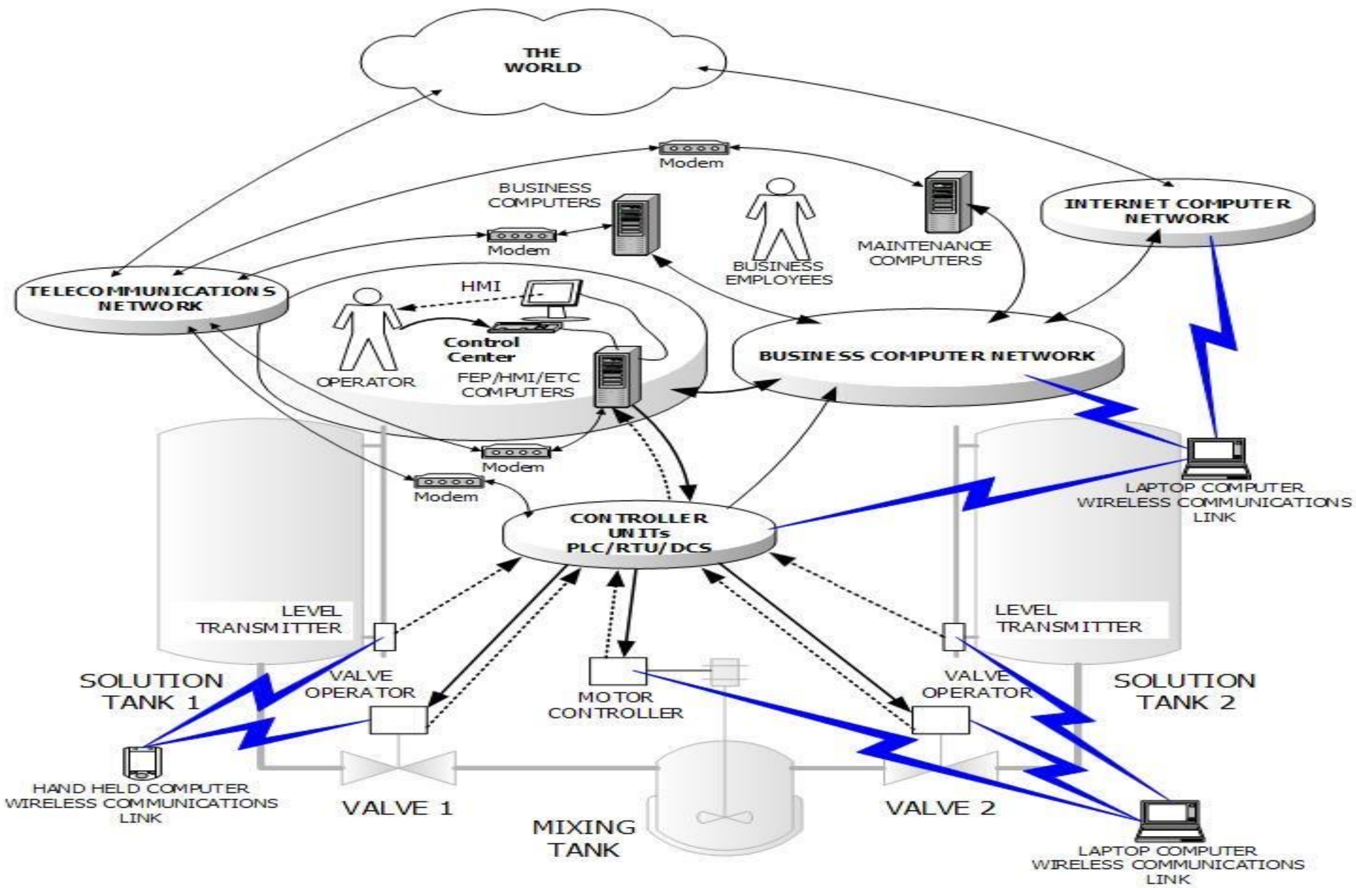
Example of a Reference Architecture for an ICS





Architecture of a Properly Architected Modern ICS

Typical ICS System Block Diagram Vulnerability Surfaces



Examples of Typical ICS Attack Vectors

- Published vulnerabilities:
  - Use of vulnerable remote display protocols
  - Secure Shell daemons that allow older versions of the protocol and are vulnerable to a downgrade attack
  - Anti-virus and spyware programs that do not have current signatures or are updated in such a manner that open an attack vector
  - Lack of a patching process/schedule leaves the ICS hosts open to attack from publicly disclosed vulnerabilities
  - Domain hosts using or storing antiquated LanMan hashes, which can be cracked using a dictionary attack
  - Backup software vulnerabilities that allow the attacker to manipulate data or server
- Web vulnerabilities:
  - Web HMI vulnerabilities
  - Secure Sockets Layer man-in-the-middle attacks where the attacker takes advantage of self signed HyperText Transfer Protocol over Secure Socket Layer (HTTPS) certificates
- Input validation vulnerabilities:
  - Buffer overflows in ICS services
  - SQL injection