Chapter 8

Securing IoT

MUGOYA DIHFAHSIH

2021/HD05/2353U

What we shall look at

- History of OT Security
- Common Challenges In OT Security
- How IT and OT Security Practices and Systems Vary
- Formal Risk Analysis Structures
  - OCTAVE and FAIR
- The Phased Application of Security in an Operational Environment

A Brief History of OT Security

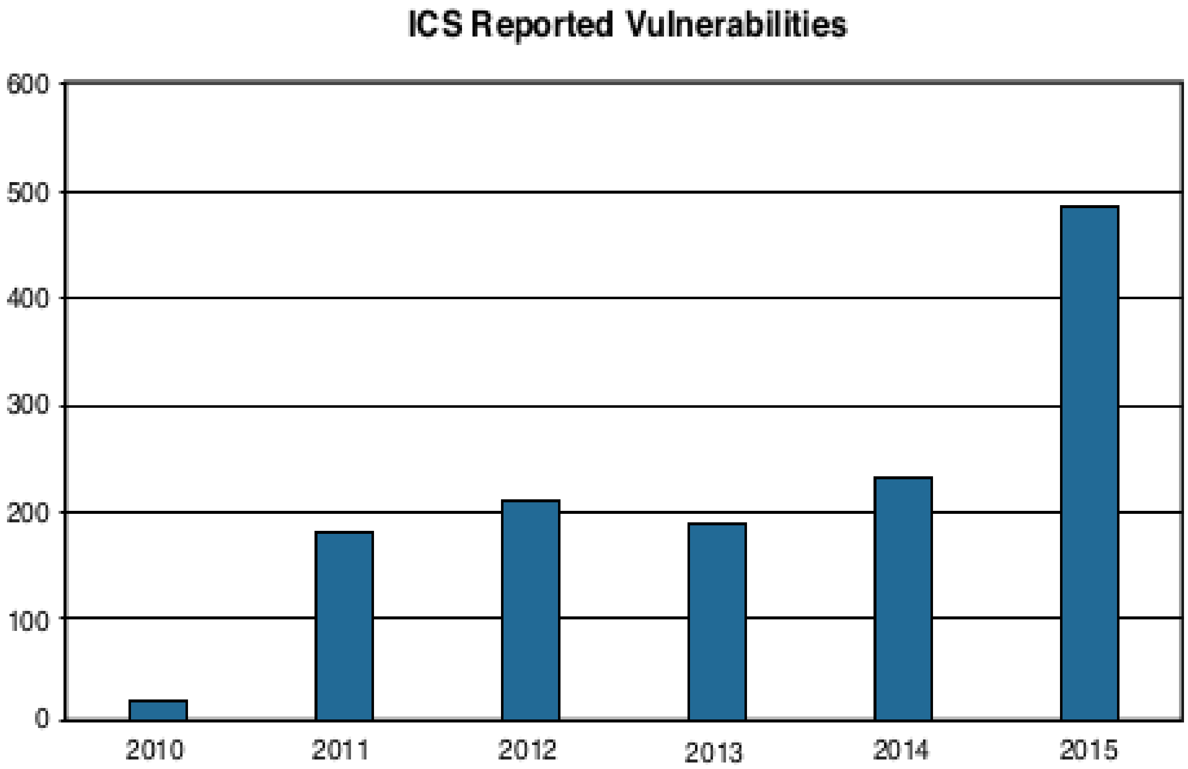


Figure 8-1 *History of Vulnerability Disclosures in Industrial Control Systems Since 2010 (US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) https://ics-cert.us-cert.gov).*

More than in most other sectors, cybersecurity incidents in industrial environments can result in physical consequences that can cause threats to human lives as well as damage to equipment, infrastructure, and the environment.

Most of the industrial control systems deployed today, their components, and the limited associated security elements were designed when adherence to published and open standards were rare.

Many of the security policies and mitigation procedures that were in place went unheeded; however, if properly implemented, they could have impeded or possibly stopped the attacks entirely.

- In addition to physical damage, operational interruptions have occurred in OT environments due to cybersecurity incidents.
- Historically, attackers were skilled individuals with deep knowledge of technology and the systems they were attacking. However, as technology has advanced, tools have been created to make attacks much easier to carry out.
- Communication networks, both local and geographically dispersed, have been used in industrial environments for decades.
- OT-specific communication systems have typically been standalone and physically isolated from the traditional IT enterprise networks in the same companies.

Common Challenges in OT Security

The security challenges faced in IoT are by no means new and are not limited to specific industrial environments. The following sections discuss some of the common challenges faced in IoT.

- Erosion of Network Architecture
- Pervasive Legacy Systems
- Insecure Operational Protocols
  - Modbus
  - DNP3
  - ICCP
  - OPC
  - IEC
- Device Insecurity
- Dependence on External Vendors
- Security Knowledge

Erosion of Network Architecture

- The challenge, and the biggest threat to network security, is standards and best practices either being misunderstood or the network being poorly maintained.
- With time what seemed to be a solid design is eroded through ad hoc updates and individual changes to the hardware and machinery without consideration
- These uncontrolled or poorly controlled OT network evolutions have, in many cases, over time led to weak or inadequate network and systems security.

Pervasive Legacy Systems

Legacy components are not restricted to isolated network segments but have now been consolidated into the IT operational environment.

From a security perspective, this is potentially dangerous as many devices may have historical vulnerabilities or weaknesses that have not been patched and updated, or it may be that patches are not even available due to the age of the equipment.

This includes switches, routers, firewalls, wireless access points, servers, remote access systems, patch management, and network management tools.

Insecure Operational Protocols

For the sake of interoperability, some protocols are typically published for others to implement them thus, it becomes a relatively simple matter to compromise the protocols themselves and introduce malicious actors that may use them to compromise control systems

- **Modbus**; Authentication of communicating endpoints was not a default operation because it would allow an inappropriate source to send improper commands to the recipient.
- **DNP3** (Distributed Network Protocol); In the case of DNP3, participants allow for unsolicited responses, which could trigger an undesired response thus making the system untrustworthy
- **ICCP** (Inter-Control Center Communications Protocol);
  - One key vulnerability is that the system did not require authentication for communication.
  - Second, encryption across the protocol was not enabled as a default condition, thus exposing connections to man-in-the-middle (MITM) and replay attacks.

- **OPC (OLE for Process Control);** OPC is the dependent on the Remote Procedure Call (RPC) protocol, which creates two classes of exposure.
  - The first requires you to clearly understand the many vulnerabilities associated with RPC
  - second requires you to identify the level of risk these vulnerabilities bring to a specific network.
- **International Electrotechnical Commission (IEC) Protocols;** Authentication is embedded in MMS, but it is based on clear-text passwords, and authentication is not available in GOOSE or SV.

Other Protocols

There is need of understanding of the most basic protocols, transport mechanisms, and foundational elements of any network, including ARP, UDP, TCP, IP, and SNMP.

IoT networks reach all the way to the individual sensors, so protocols such as Constrained Application Protocol (CoAP) (see Chapter 6) and Datagram Transport Layer Security (DTLS) are used, and have to be considered separately from a security perspective.

Device Insecurity

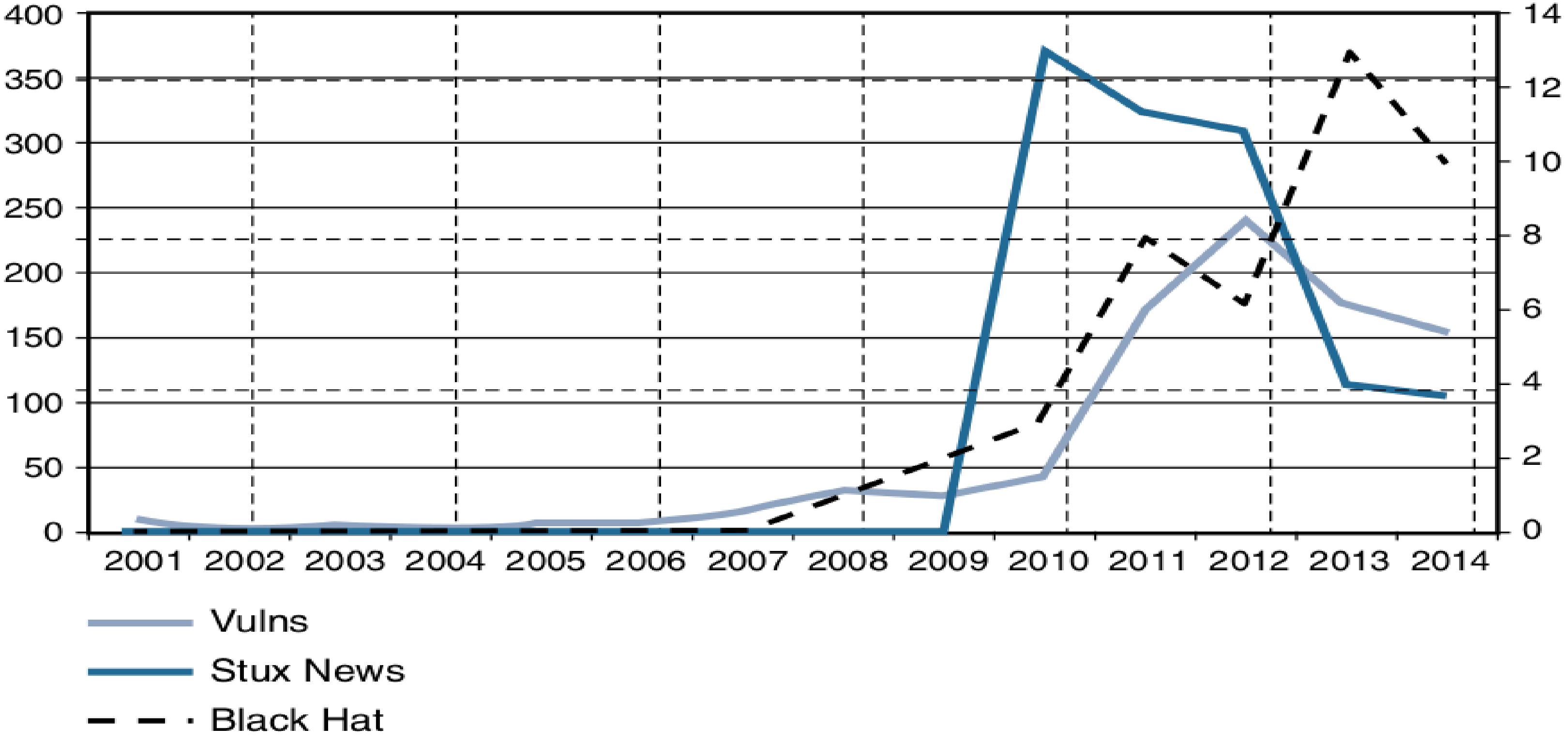


Figure 8-2 *Correlation of Industrial Black Hat Presentations with Discovered Industrial Vulnerabilities (US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) https://ics-cert.us-cert.gov).*

Dependence on External Vendors

- There are sometimes written contracts between the business and the products vendors for direct or on-demand access to critical systems.

  This allows vendors to remotely manage and monitor equipment and to proactively alert the customer if problems are beginning to creep in.

- These contracts generally fail to address questions of shared liability for security breaches or processes to ensure communication security.

Security Knowledge;

- OT security expertise is the comparatively higher age of the industrial workforce
- New connectivity technologies are being introduced in OT industrial environments that require up-to-date skills, such as TCP/IP, Ethernet, and wireless that are quickly replacing serial-based legacy technologies.
- To address this problem, Education for industrial security environments has grown steadily, particularly in the electrical utility space, where regulations such as NERC CIP (CIP 004) and IEC 62351 (01) require ongoing training.

How IT and OT Security Practices and Systems Vary

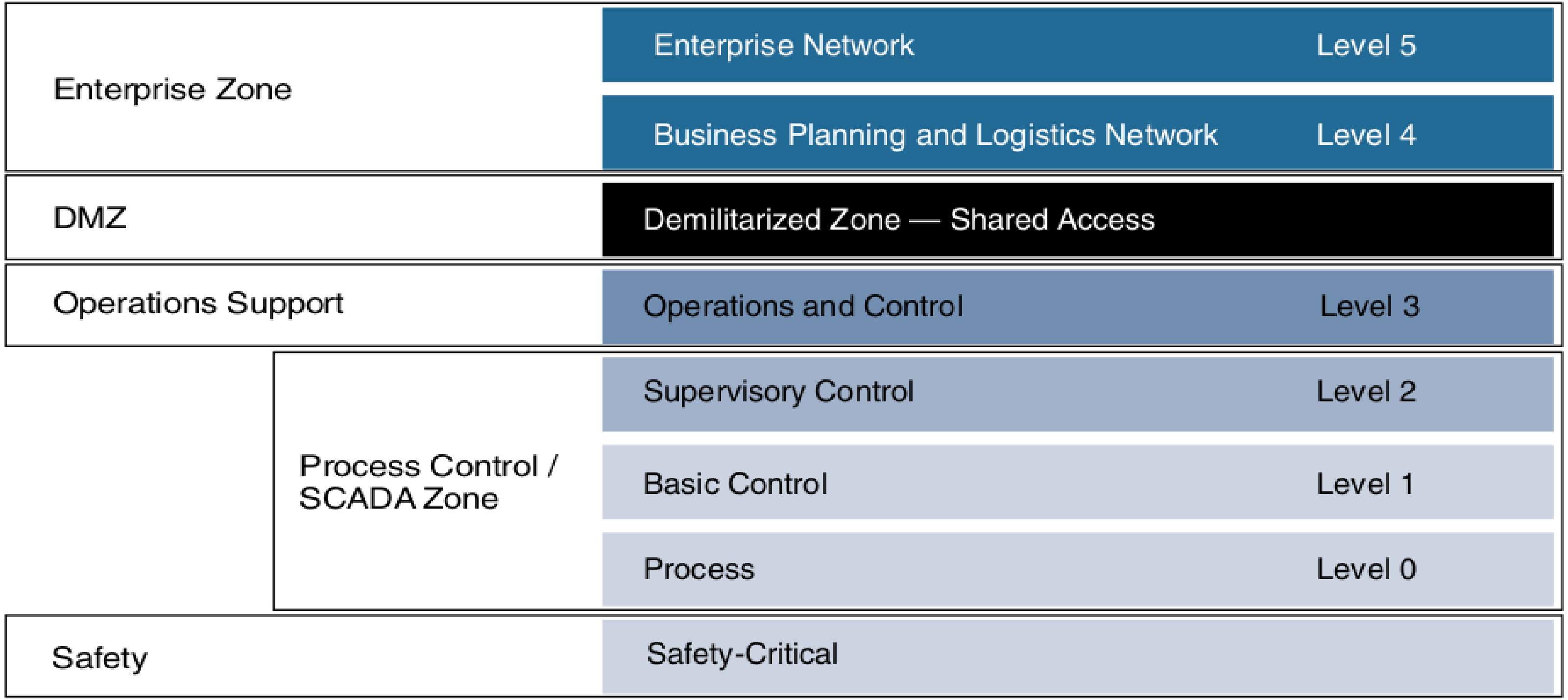
- The differences between an enterprise IT environment and an industrial-focused OT deployment are important to understand because they have a direct impact on the security practice applied to them.

  In this Section we look at;

  - The purdue Model for Control Hierarchy
  - OT Network Characteristics Impacting Security
  - Security Priorities: Integrity, Availability and confidentiality
  - Security Focus

The Purdue Model for Control Hierarchy

This model identifies levels of operations and defines each level. The enterprise and operational domains are separated into different zones and kept in strict isolation via an industrial demilitarized zone (DMZ):



Enterprise Zone	Enterprise Network	Level 5
	Business Planning and Logistics Network	Level 4
DMZ	Demilitarized Zone — Shared Access	
Operations Support	Operations and Control	Level 3
Process Control / SCADA Zone	Supervisory Control	Level 2
	Basic Control	Level 1
	Process	Level 0
Safety	Safety-Critical	

Figure 8-3 *The Logical Framework Based on the Purdue Model for Control Hierarchy*

Enterprise zone

Level 5: Enterprise network:Corporate-level applications such as Enterprise Resource Planning (ERP) and services such as Internet access and VPN entry from the outside world exist at this level.

Level 4: Business planning and logistics network: material flow applications, optimization and planning systems, and local IT services such as phone, email, printing,and security monitoring.

Industrial demilitarized zone

DMZ: It allows for easy segmentation of organizational control.

Operational zone

- Level 3: Operations and control:
- Level 2: Supervisory control:
- Level 1: Basic control:
- Level 0: Process:

Safety zone

- Safety-critical: This level includes devices, sensors, and other equipment used to manage the safety functions of the control system.

The Purdue model allows security to be correctly applied at each level and between levels.

IT networks typically reside at Levels 4 and 5 and use security. For example, principles common to IT networks. The lower levels are where the industrial systems and IoT networks reside.

OT Network Characteristics Impacting Security

While IT and OT networks are beginning to converge, they still maintain many divergent characteristics in terms of how they operate and the traffic they handle.

IT networks:

- The communication data flows that emanate from a typical IT endpoint travel relatively far.
- Data in the form of email, file transfers, or print services will likely all make its way to the central data center, where it is responded to, or triggers actions in more local services, such as a printer.

OT networks:

- The first is local traffic that may be contained within a specific package or area to provide local monitoring and closed-loop control.
- The second type of traffic is used for monitoring and control of areas or zones or the overall system.

When IT endpoints communicate, it is typically short and frequent conversations with many connections.

- In an OT environment, endpoint communication is typically point-to-point, such as a SCADA master to SCADA slave, or uses multicast or broadcast, leveraging a publisher/subscriber type of model.
- Network timing in the OT space,device clocking against a master time source, a number of use cases require an extremely accurate clock source and extremely accurate time/synchronization distribution
- IT networks are typically more mature and use up-to-date technologies.
- Industrial networks often still rely on serial communication technologies or have mixed serial and Ethernet.

Security Priorities: Integrity, Availability, and Confidentiality

- In an IT realm, the most critical element and the target of attacks has been information.
- In an OT realm, the critical assets are the process participants: workers and equipment.

  In the IT business world;

  - there are legal, regulatory, and commercial obligations to protect data, especially data of individuals who may or may not be employed by the organization
- In the OT world;
  - losing a device due to a security vulnerability means production stops, and the company cannot perform its basic operation.

Security Focus

- In an IT environment,
  - The most painful experiences have typically been intrusion campaigns in which critical data is extracted or corrupted.
  - The result has been a significant investment in capital goods and humanpower to reduce these external

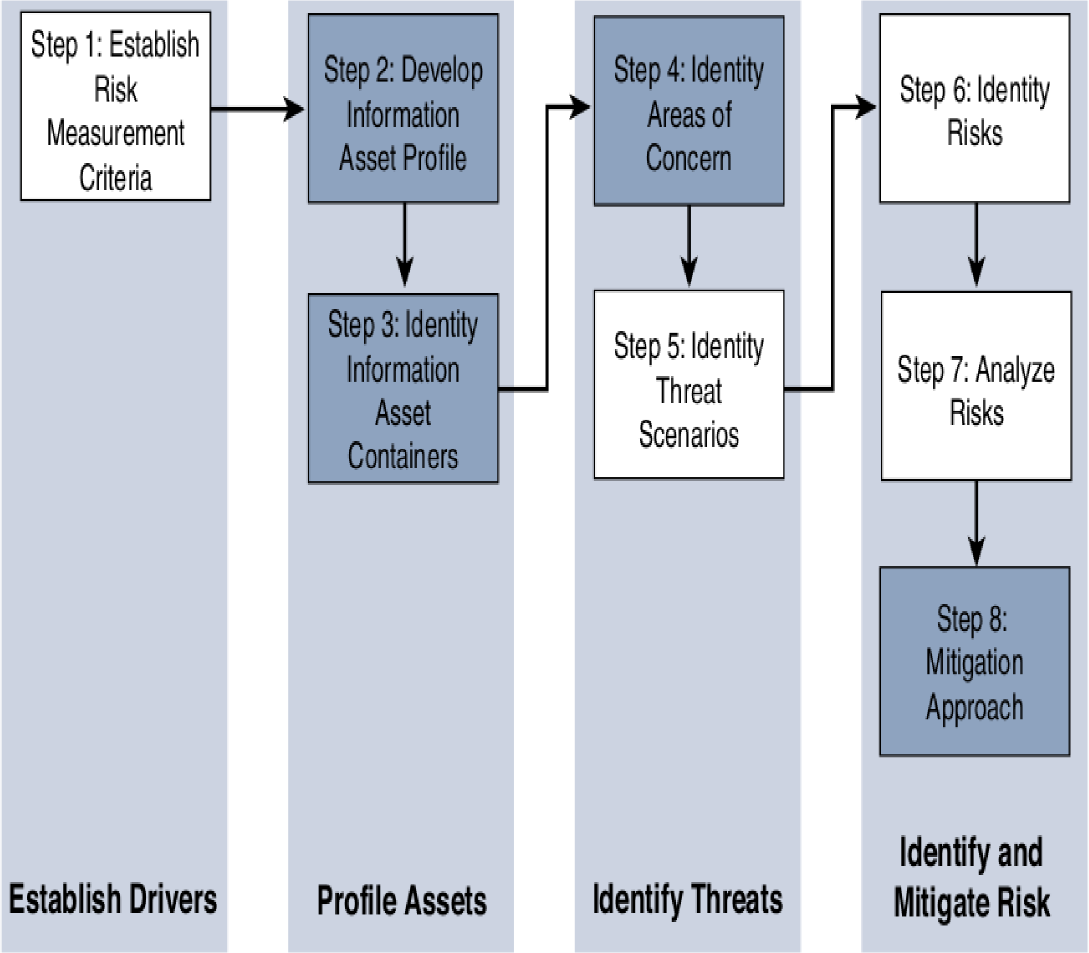
    threats and minimize potential internal malevolent actors.
- In the OT space,
  - The history of loss due to external actors has not been as long, even though the potential for harm on a human scale is clearly significantly higher.
  - Tnterest and investment in industrial security have primarily been in the standard access control layers.

Formal Risk Analysis Structures

- The key for any industrial environment is that it needs to address security holistically and not just focus on technology, it must include people and processes.
- This can be reviewed in two risk assessment frameworks;
  - OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) from the Software Engineering Institute at Carnegie Mellon University
  - FAIR (Factor Analysis of Information Risk) from The Open Group
- These two systems work toward establishing a more secure environment but with two different approaches and sets of priorities.

OCTAVE

- The Allegro version of OCTAVE;
  - Is lightweight and less burdensome process to implement
  - IT assumes that a robust security team is not on standby or immediately at the ready to initiate a comprehensive security review



Step 1: Establish Risk Measurement Criteria

Step 2: Develop Information Asset Profile

Step 3: Identity Information Asset Containers

Step 4: Identity Areas of Concern

Step 5: Identity Threat Scenarios

Step 6: Identity Risks

Step 7: Analyze Risks

Step 8: Mitigation Approach

Establish Drivers

Profile Assets

Identify Threats

Identify and Mitigate Risk

Figure 8-5 *OCTAVE Allegro Steps and Phases (see https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/).*

- Step 1;(Establish a risk measurement criterion).
  - OCTAVE provides a fairly simple means of doing this with an emphasis on impact, value, and measurement.
  - Helps to make risk prioritization
- Step 2(Develop an information asset profile)
  - Outline the importance of the process
  - The system calls for a justification of the prioritization
  - Align level of security investment with that individual asset.
- Step 3(identify information asset containers.)
  - Reference to the compute elements and the networks by which they communicate
  - Preferable target is information rather than assets
  - The container operates on the attribute of information which is endemic

- Step 4 (identify areas of concern)
  - Map security-related attributes to more business-focused use cases
  - Analysis of History both within and outside the organization
  - References to similar operational use cases and incidents of security failures are reasonable associations.
- Step 5 (Identify threat scenario)
  - Flag threats as potential undesirable events
  - Explicit identification of actors, motives, and outcomes
- Step 6; Identify risks and how they have impacted the organization
- Step 7; Risk analysis, with the effort placed on qualitative evaluation of the impacts of the risk.
- Step 8; Apply mitigation, take no action, take action, defer action

FAIR

- FAIR (Factor Analysis of Information Risk) is a technical standard for risk definition from The Open Group.
- Unlike with OCTAVE, there is a significant emphasis on

  naming, with risk taxonomy definition as a very specific target.
- FAIR places emphasis on both unambiguous definitions and the idea that risk and associated attributes are measurable
- FAIR Taxonomy of risk definition;
  - Frequency taxonomy; Loss even frequency is the result of a threat agent acting on an asset with a resulting loss to the organization.
  - Probable loss Magnitude; Quantifies the impacts with the emphasis being on measurable metrics.

The Phased Application of Security in an Operational Environment

- Phased approach to introduce modern network security into largely preexisting legacy industrial networks;
  - Secured Network Infrastructure and Assets
  - Deploying Dedicated Security Appliances
  - Higher-Order Policy Convergence and Network Monitoring

Secured Network Infrastructure and Assets

- As a first step, you need to analyze and secure the basic network design.
- Most automated process systems or even hierarchical energy distribution systems have a high degree of correlation between the network design and the operational design.

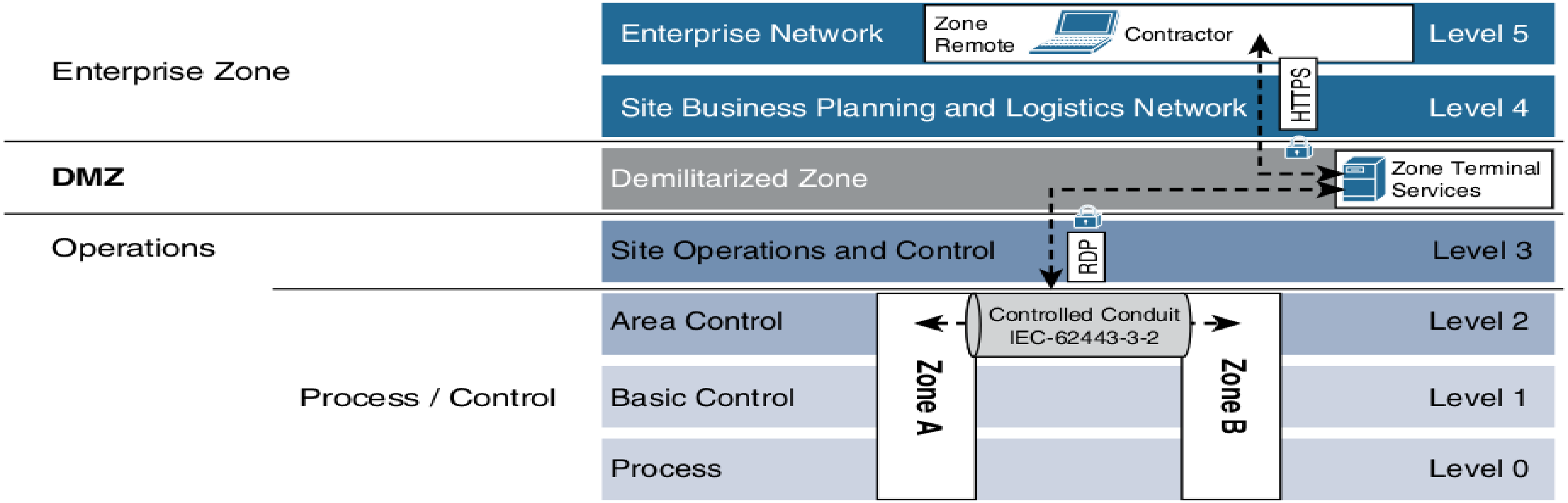


Figure 8-6 *Security Between Levels and Zones in the Process Control Hierarchy Model*

Deploying Dedicated Security Appliances

- The goal is to provide visibility, safety, and security for traffic within the network
- This level of visibility is typically achieved with deep packet inspection (DPI) technologies such as intrusion detection/prevention systems (IDS/IPS).
- These technologies can be used;
  - To detect many kinds of traffic of interest
  - To ascertain whether applications are communicating
  - To know whether exploits are targeting vulnerabilities
  - To passively identifying assets on the network

- With the goal of identifying assets, an IDS/IPS can detect what kind of assets are present on the network.
- Passive OS identification programs can capture patterns that expose the base operating systems and other applications communicating on the network.
- Application-specific protocols are also detectable by IDS/IPS systems. For more IT-like applications, user agents are of value, but traditionally, combinations of port numbers and other protocol differentiators can contribute to identification.
- All these actions can be done from a non-intrusive deployment scenario. Modern DPI implementations can work out-of-band from a span or tap.

Higher-Order Policy Convergence and Network Monitoring

- This is the adoption and integration of security across operational boundaries. This involves coordinating security on the both IT and OT sides of the organization.
- From a security perspective, the value follows the argument that most new networking and compute technologies coming to the operations space were previously found and established in the IT space.
- New technologies in the practices and tools in IT are mature than those in IT space

- **Areas that require Coordination across OT an IT environmrnts;**
  - Remote access
  - Threat detection
- For remote access,most large industrial organizations backhaul communication through the IT network.
- Often vendors or consultants who require some kind of remote access to OT assets also traverse the IT side of the network.
- The use of common access controls and operational conditions eases and protects network assets to a greater degree than having divergent groups creating ad hoc methods.