# Introduction



## Introduction

Protecting industrial automation and control systems (IACS) from cyber threats is top of mind. But converting good intentions to action can be a daunting task. As IACS and underlying networks are often very complex, using legacy technologies and poor security procedures, one could wonder where to start.

For over 15 years, Cisco has been helping industrial organizations around the globe digitize their operations by developing a market-leading networking portfolio that is purpose-built for industrial use cases. Our deep understanding of operational technology requirements plus a comprehensive networking and cybersecurity portfolio is a rare combination.

Cisco's industrial security architecture simplifies complexity across the network by implementing a model that focuses on the use cases an organization must secure. This model treats each use case holistically, focusing on today's threats and the capabilities needed to secure the operational network against those threats. Cisco has deployed, tested, and validated the solution to provide guidance, complete with configuration steps that ensure effective and secure deployments for our customers.

## Target Audience

To successfully connect and secure the industrial environment, all stakeholders must work together. Operational technology (OT) teams understand the industrial environment—the devices, the protocols, and the operational processes. Information technology (IT) teams understand the network. The security team understands threats and vulnerabilities. By working together, these specialists can leverage existing networking and security technologies, tools, and expertise to constantly protect the industrial systems without disrupting production safety and uptime.

The Cisco Industrial Threat Defense solution is intended to be used by IT, OT, and security teams and their relevant partners and system integrators. Operations will appreciate the ease of use and simple deployment, as well as the broad support of various IACS vendors and protocols. IT network managers will appreciate the ability to apply skills, technology, and applications already deployed in the enterprise when looking to integrate

production environments. Security teams will have visibility into industrial assets and security events with context enriched by control engineers.

### Security Challenges

As highlighted in Figure 1, the first key challenge when securing the IACS is collaboration between IT and OT teams. The view that OT and IT are distinctly separate entities is antiquated. Failing to acknowledge the increasingly interconnected nature of OT and IT can have detrimental consequences for industrial organizations. A lack of trust, understanding, and collaboration between OT and IT departments can have a devastating impact on the security posture of an organization.

***Figure 1: Common security challenges in Industrial Networking***


IT and OT personnel have different operating procedures and roles to play, and their worldview can differ considerably. However, their goals with respect to securing the company should be identical, and the path forward involves finding common ground. OT personnel are focused on safety, reliability, and productivity. Their role is to protect people, lives, the environment, the operation, and production. Conversely, cybersecurity personnel are focused on maintaining the confidentiality of information and the integrity and availability of IT systems. However, the goals of these entities do overlap. Both are committed to securing the organization, minimizing risk, maximizing uptime, and ensuring that the organization can continue to safely generate revenue.

The second challenge when securing the IACS network is a lack of visibility. As industrial networks can be quite old, widely dispersed, and involve many contractors, operators often do not have an accurate inventory of what is on the network. Without this, they have limited ability to build a secure communications architecture. A lack of visibility also means operators are often unaware of which devices are communicating to each other or even of communications reaching industrial devices from the outside.

The lack of visibility ultimately leads to a lack of segmentation or control. OT networks have been deployed over the years with few or no security policies in place. Networks were not designed with security in mind, updates and patches are harder to deploy, and downtimes are less acceptable. It is critical that OT operations use the visibility to implement the segmentation in their network, as impacts can range from faulty production to lost revenues and even bodily injury, death, or damage to the environment.

Last, but certainly not least, security needs to be top of mind due to threat of malware impacting the environment. Malware must be prevented, when possible, detected when it attempts to breach a network, and

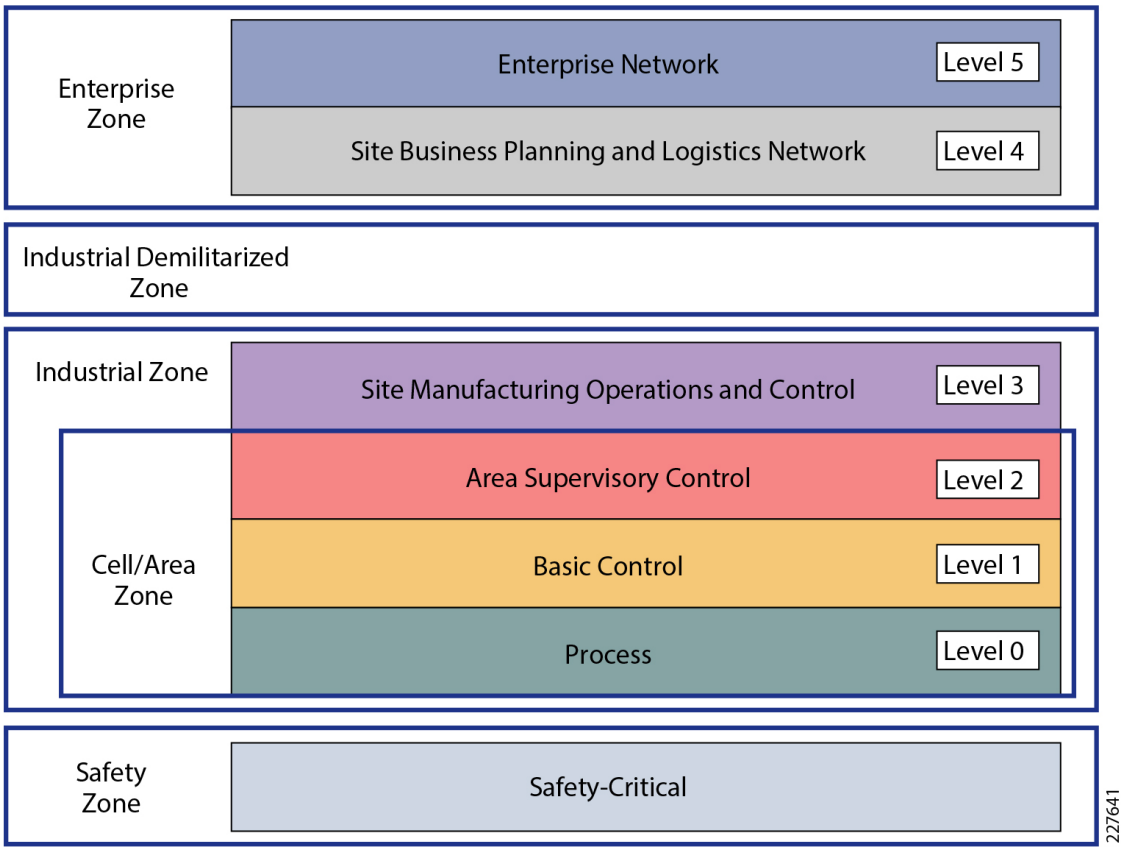
contained to limit potential damage when it infects systems and endpoints. Malware defense calls for a new best-of-breed architectural approach that spans all layers of the industrial network.

# Reference Architecture

### Plant Logical Framework

To understand the security and network systems requirements of an IACS, this guide uses a logical framework to describe the basic functions and composition of an industrial system. The Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) is a common and well-understood model in the industry that segments devices and equipment into hierarchical functions. In addition to the levels and zones, Figure 2 includes an additional demilitarized zone (DMZ) between the enterprise and industrial zones. The purpose of the DMZ is to provide a buffer zone where data and service can be shared between the enterprise and industrial network.

***Figure 2: Logical Industrial Cybersecurity Framework for Industrial Automation Networks***




### Industrial Zone

The Industrial zone is important because all the IACS applications, devices, and controllers critical to monitoring and controlling the plant floor IACS operations are in this zone. To preserve smooth plant operations and functioning of the IACS applications and IACS network in alignment with standards such as IEC 62443, this zone requires clear logical segmentation and protection from Levels 4 and 5.

The **Safety Zone** may be the most critical zone in an IACS environment. For example, in a manufacturing environment, a robot can cause a fatal impact to personnel if proper safety procedures are not followed. Not only are safety networks isolated from the rest of the IACS (as per Figure 2, positioned below the Industrial Zone), but they typically also have color-coded hardware and are subject to more stringent standards. Industrial automation allows safety devices to coexist and interoperate with standard IACS devices on the same physical infrastructure to reduce cost and improve operational efficiency, resulting in the need for effective security controls to protect from malicious actors looking to cause harm.

The **Cell/Area Zone**, a functional area within a plant or factory, is the foundation of an industrial automation architecture. Most plants will have 10s if not 100s/1000s of functional areas. This is the network that connects sensors, actuators, drives, controllers, robots, machines, and any other IACS devices that need to communicate in real-time (I/O communication). It represents Levels 0-2 of the Purdue model. Most importantly, Cell/Area Zone networks support the critical automation and control functions that keep the plant operating and producing quality products. Fundamentally, the Cell/Area Zone is a Layer 2 access network: a subnet, a broadcast domain, a virtual local area network (VLAN) and/or a service set identifier (SSID). PLCs communicate with their assigned sensors, actuators, and other IACS devices within a Cell/Area Zone. Some industrial traffic is Layer 2 only as there is no IP header attached.

Level 3, the **Site Operations and Control Zone**, represents the highest level of the IACS network and completes the segments of the Industrial Zone. Site operations is generally a “carpeted” space meaning it has heating, ventilation and air conditioning (HVAC) with typical 19-inch rack-mounted equipment in hot/cold aisles utilizing commercial grade equipment. As the name implies, this is where applications related to operating the site reside, where operating the site means the applications and services that are directly driving production. These applications are primarily based on standard computing equipment and operating systems (Unix-based or Microsoft Windows). For this reason, these systems are more likely to communicate with standard Ethernet and IP networking protocols. As these systems tend to be more aligned with standard IT technologies, they may also be implemented and supported by personnel with IT skill sets.

### Enterprise Zone

The enterprise zone is where the traditional IT systems exist. These functions and systems include wired and wireless access to enterprise network services such as:

- Internet Access
- Email services
- SAP
- Oracle

Although important, these services are not viewed as critical to the IACS and thus industrial zone operations. Direct access to the IACS is typically not required, but there are applications such as remote access and data collection where traffic must cross the IT/OT boundary. Access to the IACS network from an external zone must be managed and controlled though the industrial demilitarized zone (IDMZ) to maintain the security, availability and stability of the IACS.

### Industrial DMZ

Although not part of the Purdue mode, the industrial DMZ is deployed within plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. Network access is not permitted directly between the enterprise and the plant; however, data and services are required to be shared between the zones, thus the industrial DMZ provides architecture for the secure transport of data. Typical services deployed in the DMZ include remote access servers and mirrored

services. Further details on the design recommendations for the industrial DMZ can be found later in this guide.

### Understanding the threats

There are many great resources when learning about the techniques used to infiltrate industrial networks. For example, MITRE ATT&CK for ICS is a knowledge base useful for describing the actions an adversary may take when operating within an IACS network. ATT&CK is short for Adversarial Tactics, Techniques, and Common Knowledge.

There is also the yearly Verizon Data Breach Investigations Report (DBIR) which analyses thousands of incidents and confirmed breaches from around the world so security analysts can understand the most commonly exploited vulnerabilities across industries.

This design guide will use elements of both resources to look at some of the common attack vectors, exploring what they mean and the mitigations that can be put in place to defend against them. Figure 3 shows four common attack techniques described in the MITRE ATT&CK framework.

***Figure 3: Typical attack techniques used to exploit the Industrial Network***


Initial Access is described by MITRE ATT&CK as an adversary attempting to get into your IACS environment. This is traditionally accomplished by exploiting public facing applications, or the exploitation of remote services. The Colonial Pipeline attack for example, while not an entry into the OT network, was a result of a forgotten Virtual Private Network (VPN) termination point with stolen credentials and no Multi-Factor Authentication (MFA). The 2022 Verizon DBIR stated that over 80% of attacks come from external sources, and with many industrial sites using technologies such as VPN and Remote Desktop Protocol (RDP) for remote access services or implementing Industrial IoT (IIoT) gateways for data collection, it is critical that public facing applications are implementing with security top of mind.

In the case where initial access security was poorly implemented, or an exploit has been found, the first thing an adversary will do on the network is try to discover more information to identify and assess targets in the IACS environment. Triton malware is an example of this where a python script was executed in the network to discover Triconex safety controllers distributed by Schneider Electric. Triconex safety controllers used a proprietary protocol on UDP port 1502, and Triton used this knowledge to scan the network for the devices. If the device exists, the malware can then read the firmware version and use this information in the next phase of an attack. Network segmentation is a great way to combat this threat, as if an attacker does manage to exploit a machine in the network, their reach should not be able to extend beyond the network segment the exploited machine is in. Additionally, being able to detect the presence of network scans enables security analysts to react before an adversary has the chance to use the discovered information in an exploit attempt.

Lateral Movement refers to the adversary attempting to move through the IACS environment. This could involve jumping to engineering workstations using RDP with weak or default credentials, or in the case of e.g., the WannaCry vulnerability, using protocol exploits to hop across machines in the network. Other than

making sure default credentials are not used within the IACS, network segmentation helps solve this problem too, by containing an adversary to the zone in which the initial exploit occurred.

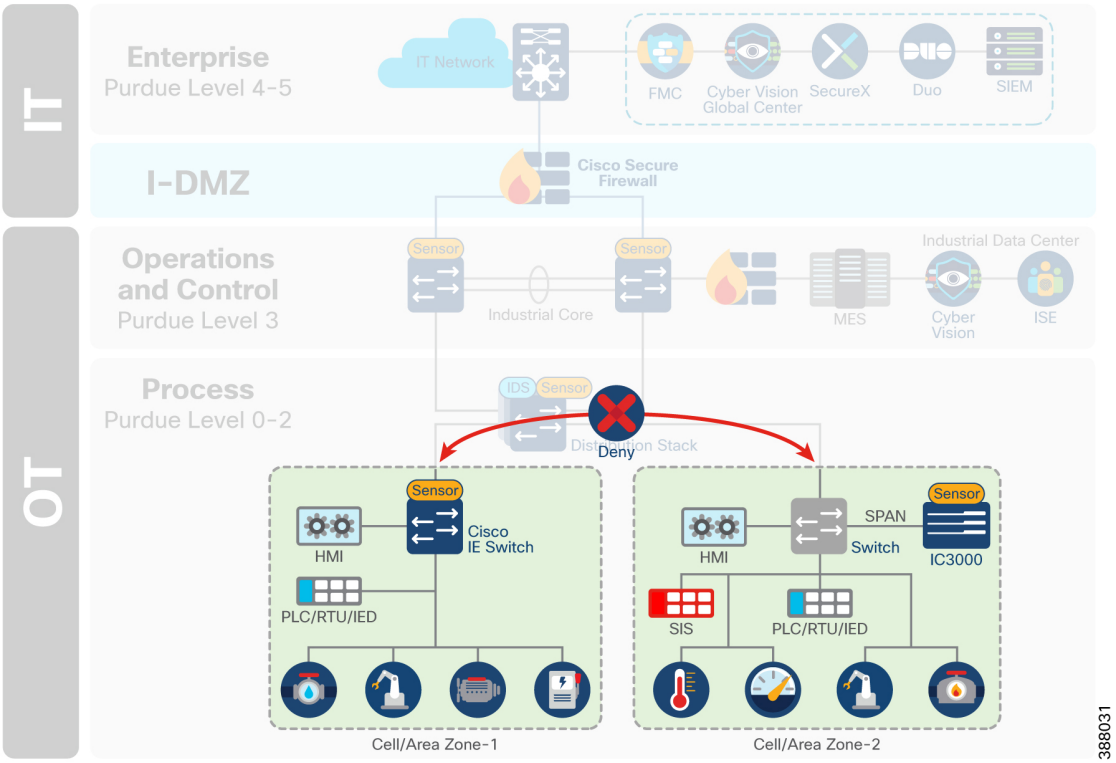
Finally, the adversary will try and communicate with, and control compromised systems, controllers, and applications within the IACS environment. This is known as Command and Control.

**Use cases**

Common use cases and personas that must be secure in an industrial network include:

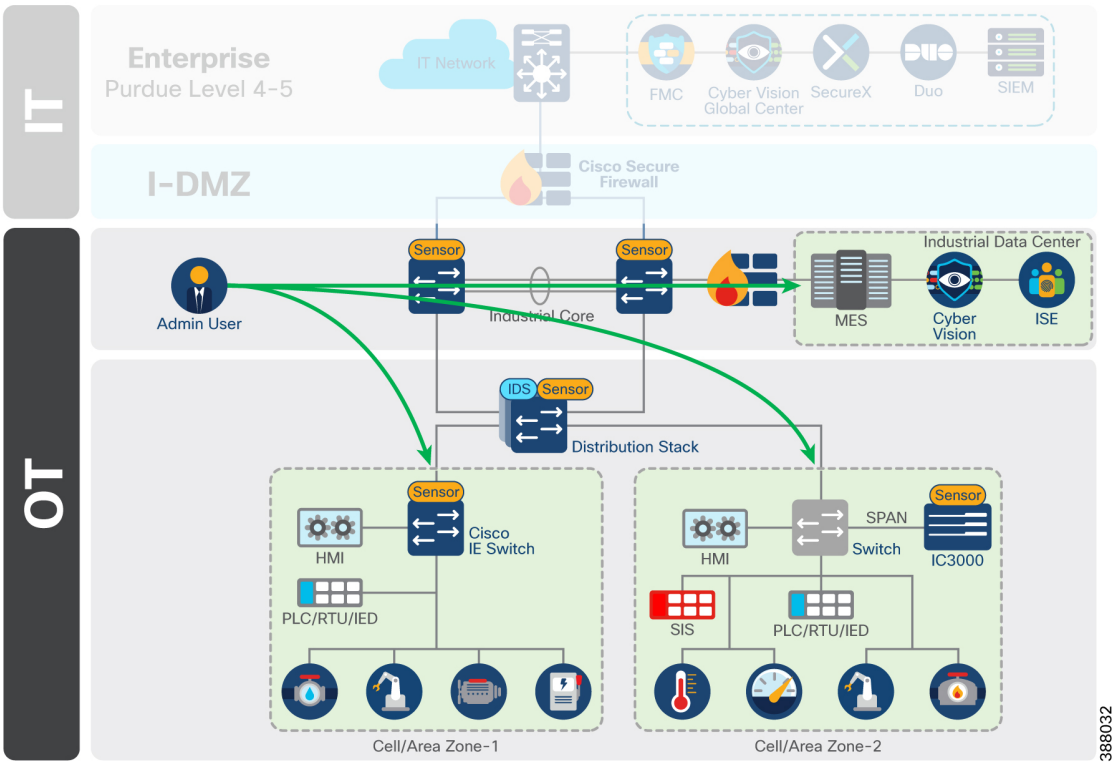
- **Cell/Area Zone**: The industrial zone is typically comprised of multiple cell/area zones. All devices located within a given Cell/Area zone should be able to freely communicate with all other assets in this zone. Communication that crosses zone boundaries should be denied unless explicitly allowed as depicted in Figure 4.

***Figure 4: Cell/Area Zone to Cell/Area Zone denied by default. No segmentation inside the zone.***



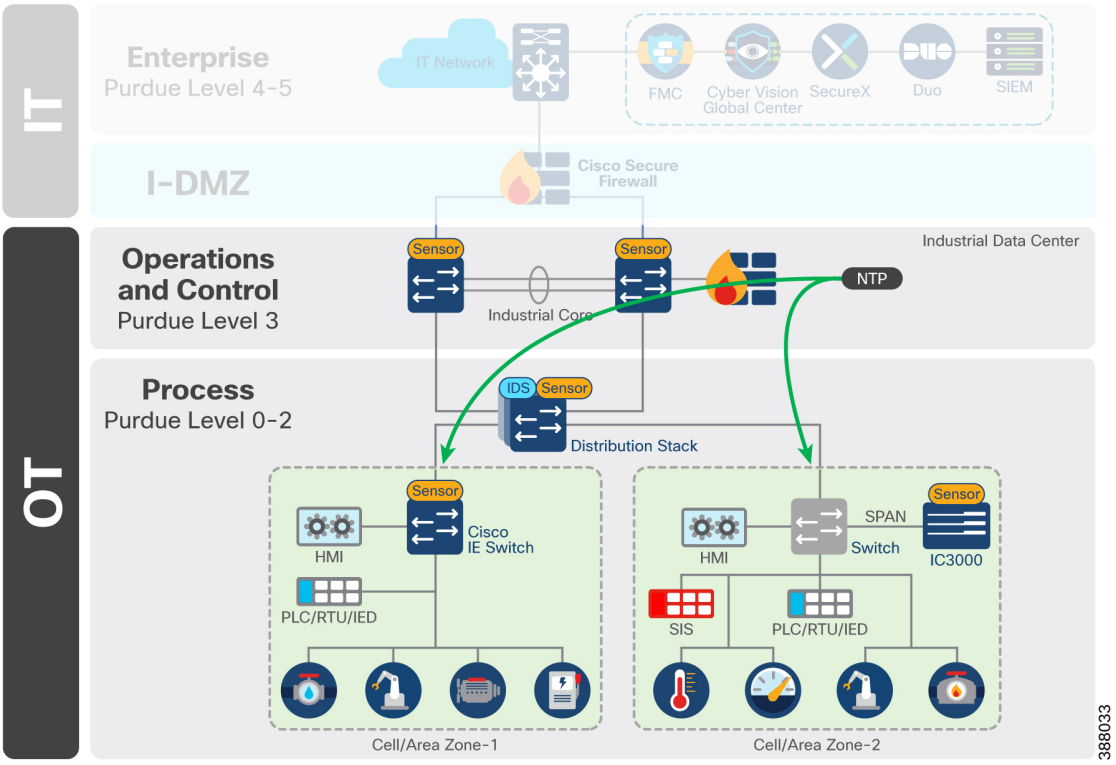

- **Administrative Users**: Figure 5 shows an administrative user who requires access to all zones in the network. They may be responsible for configuration of the network infrastructure, or the application of control logic. Their access should not be limited, but their data should be protected.

*Figure 5: Administrative Users need access to all zones*



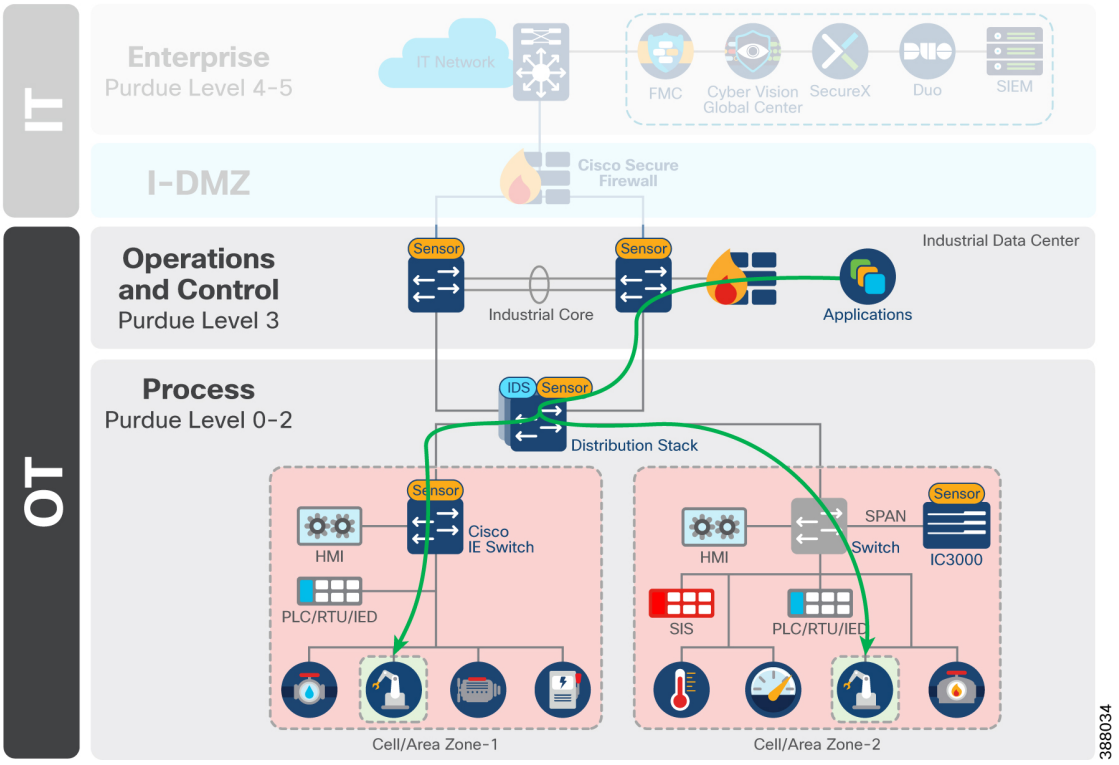

- **Infrastructure Services**: Endpoints that do not have user presence, but still require access to a large chunk of the plant. Services such as DHCP, NTP or LDAP may touch each device on the network.

*Figure 6: Infrastructure services that need access to all Cell/Area Zones*



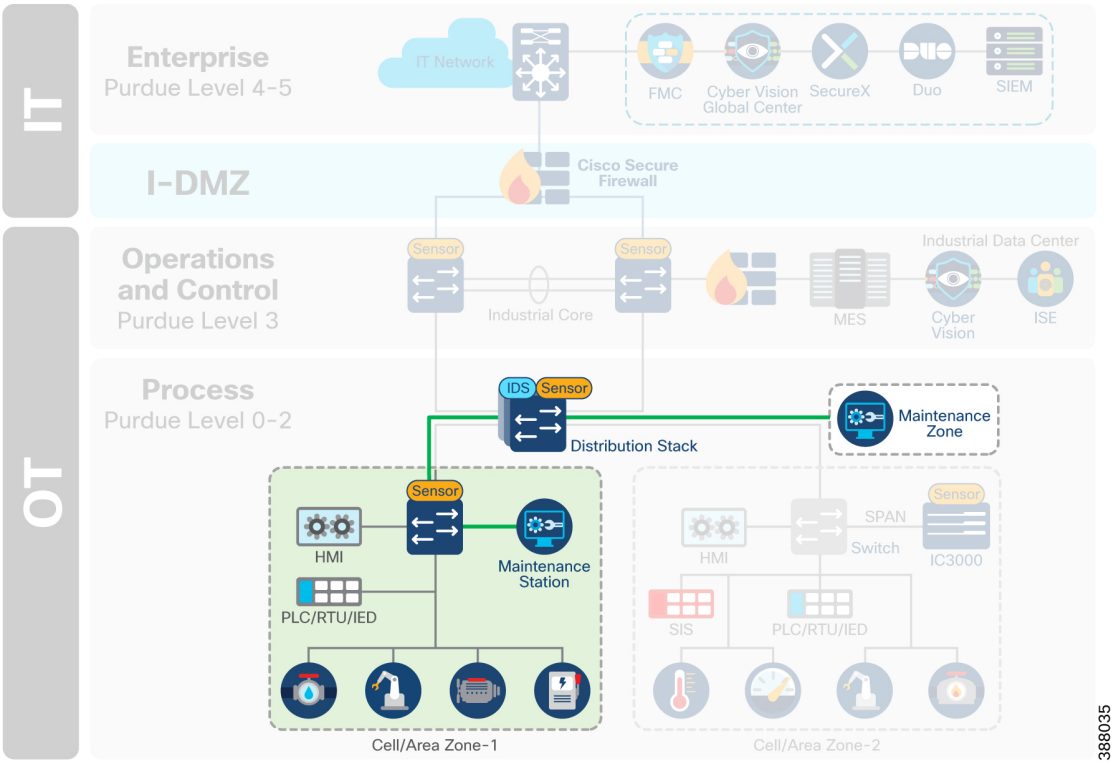

- **Plantwide Applications**: Applications within the industrial data center (IDC) that have specific access requirements. Examples include analytics platforms that require read only access to relevant machinery, or vendor tools used to monitor and maintain plant floor equipment.

*Figure 7: Applications that need access to specific services in the cell, but not the full cell*



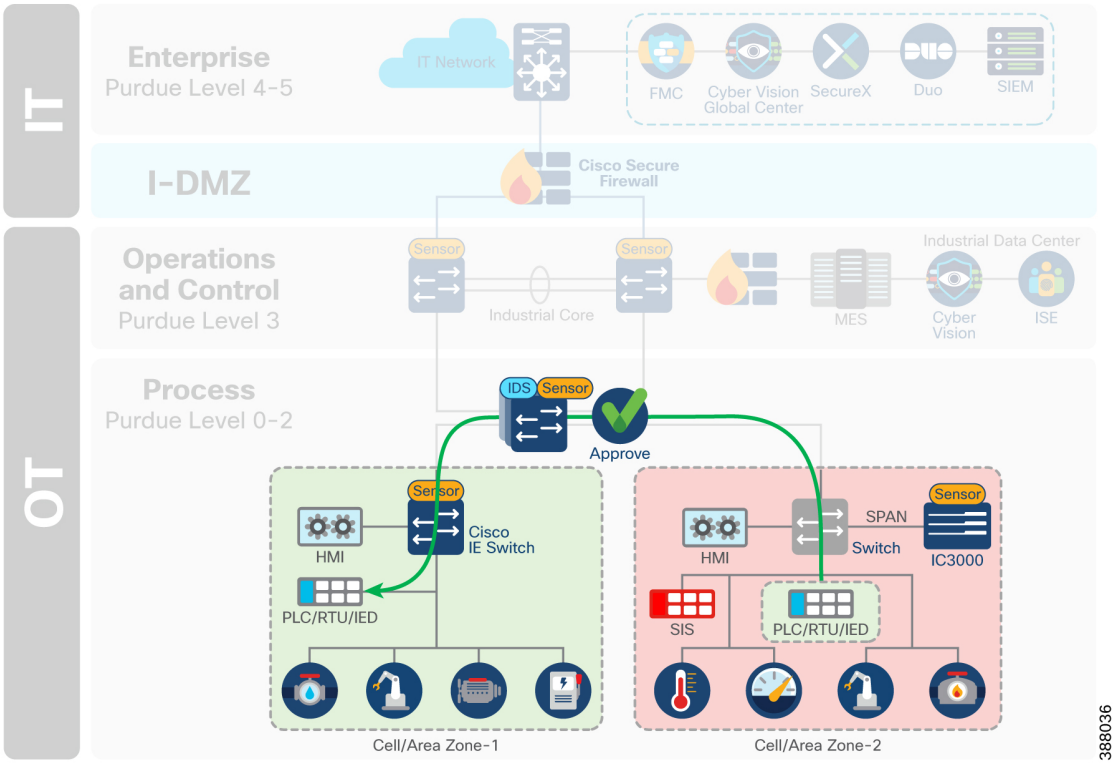

- **Maintenance Workstations**: Maintenance workstations can either reside in a zone outside of the cell/area, and act as the maintenance machine for select zones, or reside within the cell/area zone itself, but require additional privileges when leaving the zone.

*Figure 8: Maintenance workstations may reside within the cell or in a dedicated zone outside the cell*



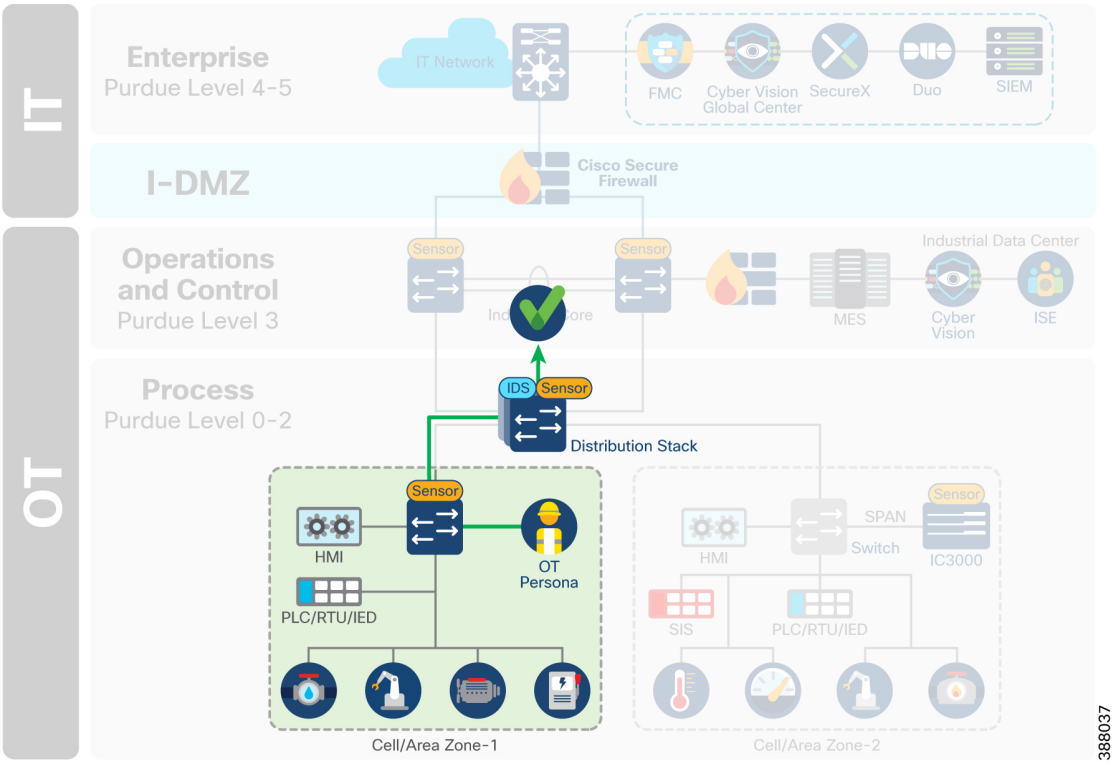

- **Interlocking Programmable logic controllers (PLC) / Interzone communication:** While most control traffic is contained within a cell/area zone, some industrial communications may need to traverse zones for distributed automation functions. A PLC in one zone should not have full access to the services in another zone and least privilege policy should be applied to ensure only valid communication are permitted. If malware was to be introduced into one zone on the network, it is important that it has no automated mechanism to spread to other zones.

*Figure 9: Select devices, such as interlocking PLCs, require communication across zones*



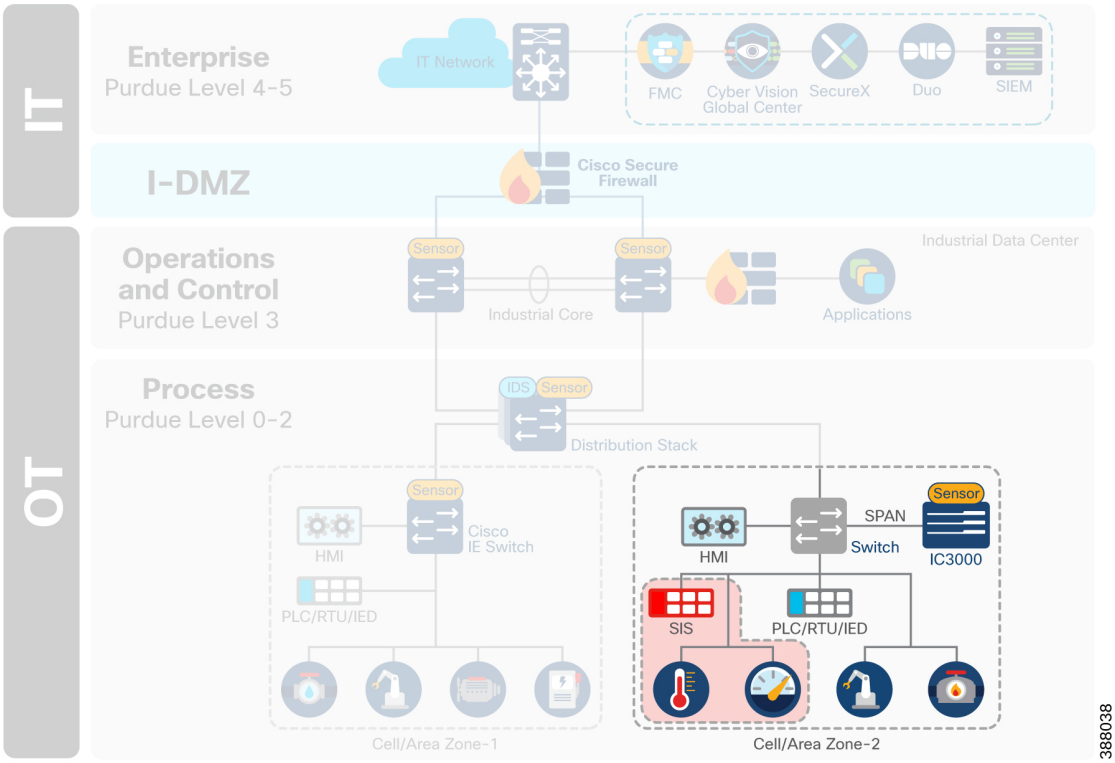

- **Convenience Port:** As operators plug directly into the infrastructure, they will typically bypass all the security checks that have been deployed in the architectural layers above it. Ensuring only authorized users with authorized device posture checks can connect to the network can aid in securing this use case.

*Figure 10: Operators plug into a cell using a convenience port and should be able to reach out to extra services*



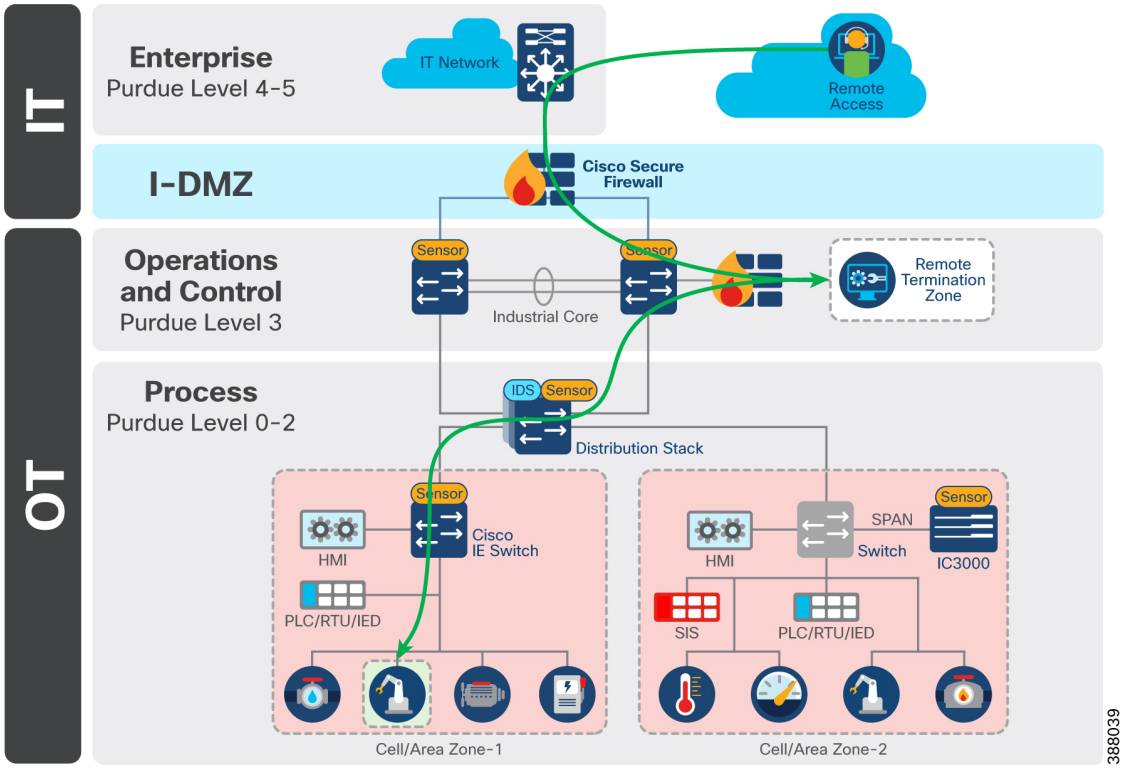

- **Safety Networks:** Safety Instrumented Systems (SIS) are critical to the control network and should either be air gapped from the rest of the network or logically segmented to ensure no data can leak into this zone.

*Figure 11: Safety Network could be air gapped, or logically separated from the rest of the network*




- **Remote Users:** Remote access is commonly granted to personas such as employees, partners and vendors for maintenance, process optimization and troubleshooting purposes. Remote access should be restricted to select devices on the plant floor for a limited amount of time.

*Figure 12: Remote users need access to select devices, not a full zone*

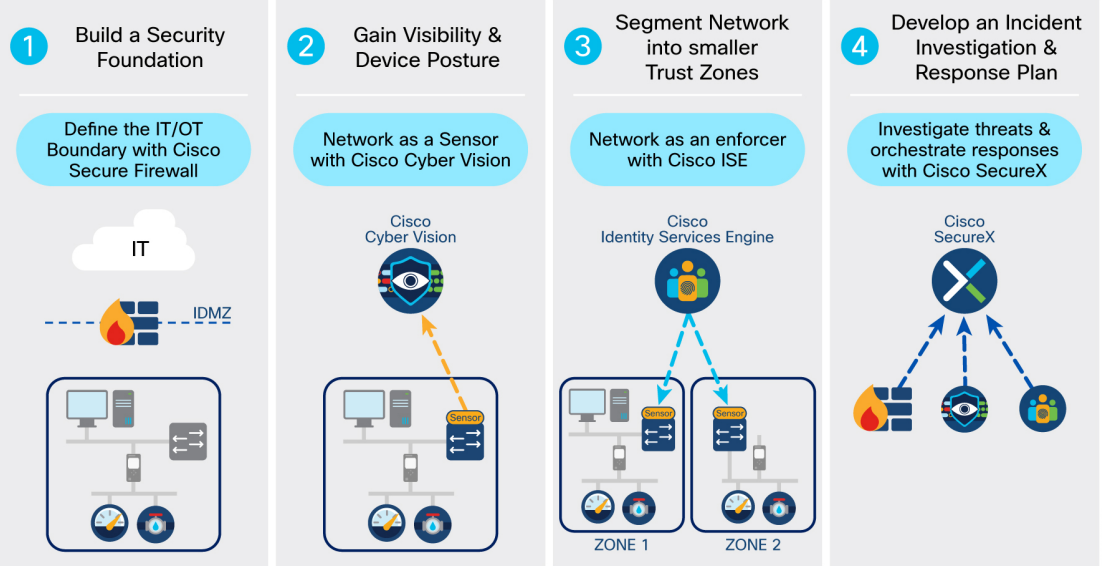



# Industrial Security Journey

### Industrial Security Journey

Addressing these issues and building a secure industrial network will not happen overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

*Figure 13: Industrial Security Journey*




# Building a Security Foundation

A solid and flexible network architecture is a key success criterion for robust and certified security. Poor network design creates a huge vulnerability and hinders the concepts of segmentation, extensibility, as well as the integration of cyber security controls and physical security measures.

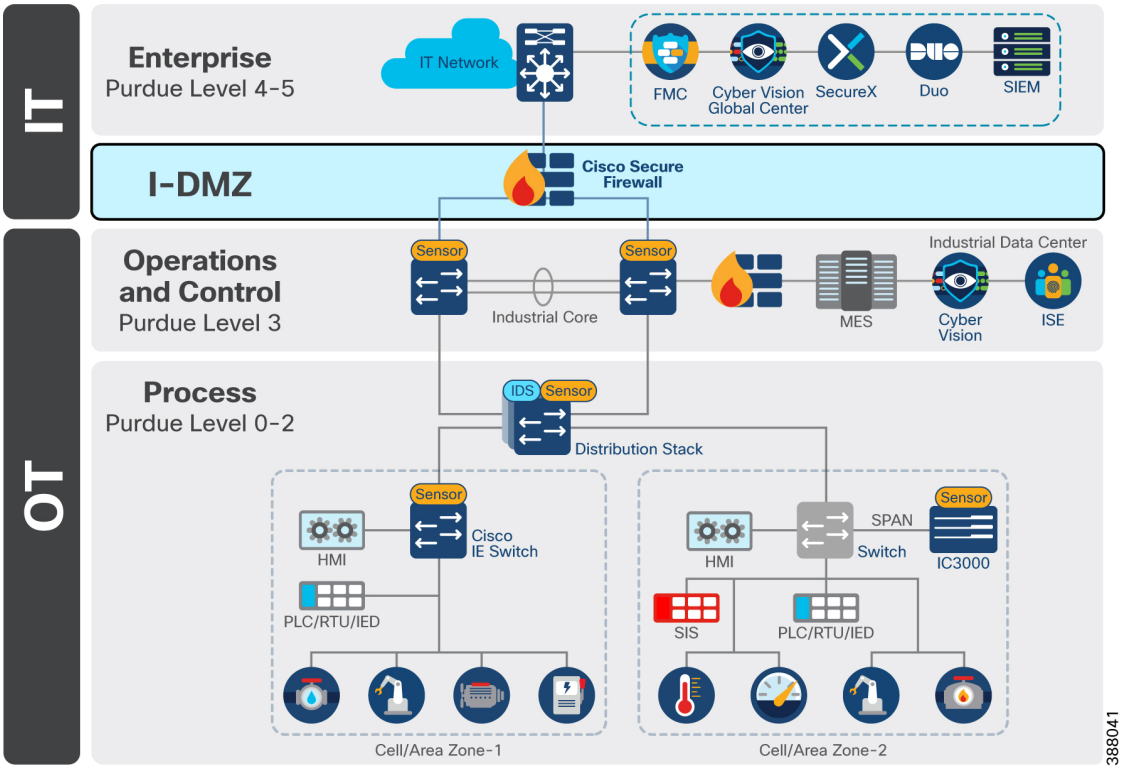
Security considerations used in this guide are focused around three key networking areas: The Cell/Area Zone supporting the core IACS embedded in the production environment functional zones, the Operations and Control Zone supporting plant-wide applications and services, and the IDMZ providing key segmentation between production and enterprise systems.

More information on the Cisco Industrial Automation reference architecture can be found in the Cisco Solution Brief for Industrial Automation Networks.

### Segmenting IT & OT Networks with the Industrial Demilitarized Zone

The first step in the journey to securing your industrial network is to restrict logical access to the OT network. A common deployment method is an Industrial Demilitarized Zone (IDMZ) network with firewalls to prevent network traffic from passing directly between the corporate and OT networks.

*Figure 14: Industrial DMZ Architecture*




The IDMZ offers a network on which to place data and services to be shared between the Enterprise and Industrial Zones. The IDMZ doesn't allow direct communication between the Industrial and Enterprise Zones but meets the data and service sharing requirement. With the deployment of an IDMZ and Industrial Zone firewall, attacks and issues that arise in one zone cannot easily affect the other zone. In fact, by temporarily disabling the IDMZ and the firewalls, an IACS or IT network administrator can help to protect a zone until the situation is resolved in the other zone.

Cisco Secure Firewall brings distinctive threat-focused next-generation security services. The firewall provides stateful packet inspection of all traffic between the enterprise and OT network and enables intrusion prevention and deep packet inspection capabilities for inspecting application data between the zones designed to identify and potentially stop a variety of attacks. Cisco Secure Firewall is the first line of defense adversaries meet when attempting to breach the network and is the enforcement point for least privilege access for legitimate services to cross the border in a secure way.

Providing design guidance for the IDMZ is out of scope for this design guide but has been extensively covered in another guide. For more information on the IDMZ, see Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense.

### Moving the IDMZ to the Cloud

Typically, IDMZ designs are architected and deployed at one facility, and replicated across each production site owned by the organization. One of the challenges with an exclusively on-site IDMZ is the limited ability to meet future demand in a world where the growth of Industrial IoT (IIoT) and IT/OT/cloud convergence requires new capabilities. It can also become challenging for operations staff to maintain IDMZ consistency across multiple sites and deliver consistent security policies.

A hybrid cloud IDMZ model can be an alternative. Like an IDMZ deployed on premises, it provides a holistic security strategy, with the benefit of shared resources and assets, allowing for a more repeatable and consistent architecture, as well as easing the operational overhead and complexity. A hybrid cloud IDMZ supports a regional operations center model, which is top of mind for some industrial organizations, especially those with a global footprint.

Design guidance for the hybrid cloud IDMZ will be added later as validation is still in the early stages of development. For an introductory insight into the architecture, see the Hybrid Cloud IDMZ white paper.

### Don't Forget about the Hardware

If the hardware is not reliable, any security measures you take on the network and resources that run on that hardware cannot be relied upon. Securing the hardware should be considered fundamental to securing operations.

IEC62443-4-1 describes requirements for the secure development of products used to assemble IACS as well as maturity levels to set benchmarks for compliance. These requisites include requirement, management, design, coding guidelines, implementation, verification and validation, defect management, patch management and product end-of-life. All of these are essential to the security capabilities of a component and the underlying secure-by-design approach of the IACS solution. The overall focus is on continuous improvement in product development and release.

Cisco software and hardware products are developed according to the Cisco Secure Development Lifecycle (CSDL), which enforces a secure-by-design philosophy from product planning through end-of-life.

IEC62443-4-2 contains requirements for components necessary to provide the required security base for 62443-3 and higher levels. In this regard, the standard specifies security capabilities that enable hardware equipment to be integrated into a secure IACS deployment. Part 4-2 contains requirements for four types of components: software application, embedded device, host device, and network device. In essence, a secure IACS solution needs to be built based on secure components.

Various Cisco products have already achieved IEC62443-4-2 certification. In combination with a 62443-certified development process (CSDL), Cisco offers trustworthy communication products which are essential for IACS deployment in critical infrastructures.