Grid Security Design Guide

What's New in Grid Security 3.0

The Grid Security 3.0 Cisco Validated Design (CVD) comprises this design guide and the corresponding implementation guide. This guide is focused on a holistic security strategy for the utility grid and is different from previous security validation efforts that were part of the Substation Automation CVDs. The Grid Security 3.0 CVD details the integration between various security platforms to achieve a holistic, secure operational technology (OT) network. This guide highlights the newly-launched Cisco Cyber Vision product and its capabilities. It details an end-to-end security approach and how Cisco Cyber Vision complements the existing security architecture with integration to and between Cisco Stealthwatch and the Cisco Identity Services Engine (Cisco ISE) when coupled with TrustSec and various enforcement points like the Cisco Industrial Security Appliance 3000 (Cisco ISA 3000) firewall.

Executive Summary

The physical and cyber security of the utility grid and associated operational monitoring and control networks has been an increasing source of concern and regulatory mandates. Legacy control systems are no longer cost effective to operate and are problematic to secure. Electric utility operators are changing their operational model and adopting new technologies. These changes are being driven by flat-to-declining revenues, grid stability issues as a result of renewables, the increasing dynamic load of electric vehicles, and a declining work force. The utility industry is rapidly migrating to a digital world. This transformation from proprietary siloed systems to a single standards-based digital system offers the opportunity to secure the operational grid network.

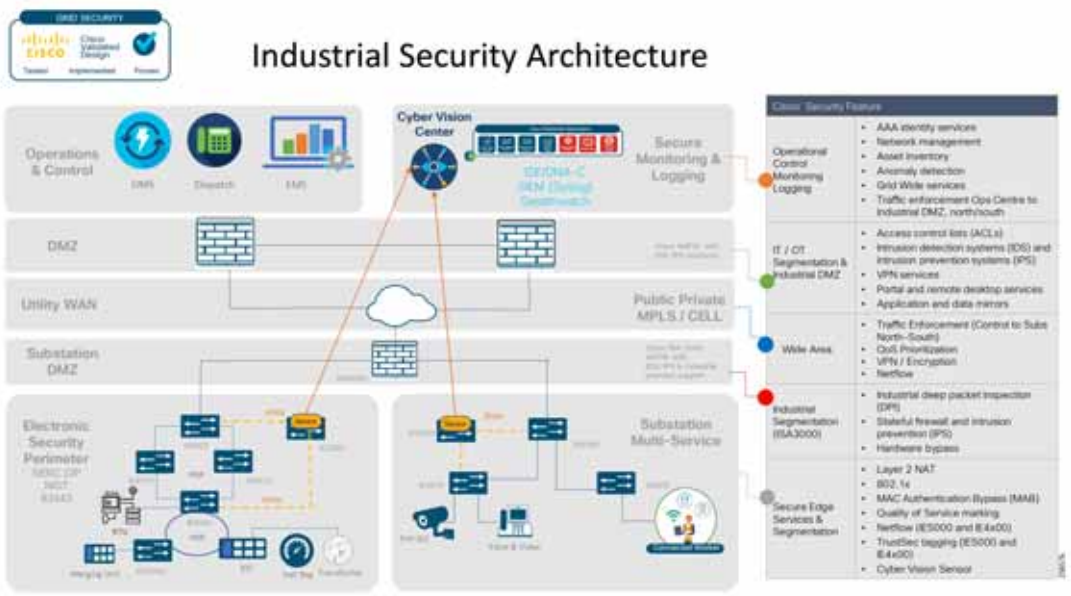
A well designed communications network can enable increased reliability and reduce operational expenses. Cisco Systems is addressing the security requirements of the utility industry with an integrated suite of validated security solutions.

The Cisco Grid Security solution, part of the Cisco portfolio of solutions for substation automation, utility WAN, and Field Area Network Advanced Meter Infrastructure (FAN AMI) provides the following with unique capabilities for electric grid operators:

- Cisco Cyber Vision is capable of non-intrusively monitoring OT protocols and identifying devices on the grid. Cisco Cyber Vision provides device-level visibility and status and operational personas of grid assets, such as device make, model, and firmware level.
- Cisco ISA 3000 industrial security firewall is a purpose built, fully ruggedized firewall leveraging the Cisco Firepower Next Generation Firewall (NGFW) with the added IoT-specific signature base to identify industrial protocols and perform deep packet inspection, segmentation, and enforcement.
- Cisco ISE has been widely deployed in information technology (IT) and OT environments for access control and authentication.
- Cisco Stealthwatch examines traffic at the application level, identifying anomalies on both the IT and OT networks.
- End-to-end testing and validation, completed and documented with various device vendors and use cases.

The Cisco Multi-tiered approach to Grid Security is illustrated in Figure 1.

Figure 1 Cisco Multi-Tiered Approach to Grid Security



The recent integration of the components described above provides an end-to-end OT security system with Cisco Cyber Vision identification of end points connected to a network, reporting of network devices, and the ability to authorize and authenticate these devices based on a device profile in Cisco ISE.

This integrated and validated architecture now includes Cisco Stealthwatch to inspect traffic on the network at the application level and detect anomalies with integration into Cisco ISE. Cisco ISE includes the ability to perform device and user authentication, authorization, and accounting (AAA), and provide policy enforcement using a policy engine. The Cisco ISA policy engine can enforce mitigation actions with the Cisco ISA 3000 firewall or at the switch level with security group tags from TrustSec or dynamic VLAN assignment on the edge switch.

This guide describes the Cisco Grid Security solution, which is based on industry-leading innovations in device discovery, anomaly detection, segmentation, isolation, profiling, and enforcement. Cisco networking technologies and the security features integrated into them allow the utility operator to turn every Cisco edge switch port and every routing hop on every Cisco switch and router into a security device, from deep in the substation network to the control and operations centers, forming an integrated and validated security system.

Navigator

Table 1 describes the sections in this document.

Table 1 Document Contents

Section	Description
System Overview, page 5	Overview of the existing security models and best practices to address the digital migration for the utility grid.
System Architecture, page 10	An examination of the architecture and its application to meet compliance and regulatory mandates.
Network Topology, page 15	Description of the Grid Security Architecture, and solution components.
System Components, page 16	An overview of the devices comprising the Grid Security solution with a description of their places and function in the utility network.

Table 1 Document Contents

Audience

The audience for this guide includes customers that are chief information security officers, system architects, security architects, OT network, compute, and systems engineers, field consultants, Cisco Advanced Services specialists, and others.

Readers may be familiar with networking protocols, SCADA protocols, compliance requirements, and basic security best practices associated with an OT network and associated grid topologies.

Document Objective and Scope

This document provides a comprehensive explanation of Cisco Grid Security system design. It includes information about the system architecture, possible deployment models, and guidelines for implementation. Recommended best practices and deployment issues are included.

Use Cases, Services, and Deployment Models

This guide addresses the following technology use cases:

- Operational visibility and insights—Know what to protect.

  Cisco Cyber Vision is embedded in your Cisco industrial network equipment so you can see everything that connects to it, segment your network, and deploy IoT security at scale.

- Maintain system integrity and production continuity.

  Cisco Cyber Vision understands proprietary industrial protocols and keeps track of process data, asset modifications, and variable changes.

- 360° threat detection—Detect threats before it is too late.

  Cisco Cyber Vision leverages Cisco threat intelligence and advanced behavioral analytics to identify known and emerging threats as well as process anomalies and unknown attacks. Fully integrated with Cisco security portfolio, it extends the IT Security Operations Center (SOC) to the OT domain.

- Authentication, authorization, and accounting—It is important to define what devices are connected to a network, at what location, and who is operating that device. AAA, especially when leveraged with Cisco ISE and 802.1x, builds a complete list of what and who is on the network by location for policy enforcement and audit logging and reporting.

Network segmentation

Industrial security best practices suggest migrating networks towards architectures compliant with IEC62443 zones and conduits. Placing assets that do not communicate with each other in isolated network segments helps prevent an attack from spreading to your entire industrial infrastructure. NERC CIP compliance dictates multiple segmentation "zones" based on criticality of assets in a substation and between substations.

Cisco Cyber Vision gives you an accurate view of your assets, network connections, and remote accesses so you can build a network that is designed to be secure and that can be effectively monitored. It lets you group assets and define their "industrial impact" so you can prioritize core events according to your own or mandated industrial safety targets. It summarizes all flows between zones so you can focus on monitoring relevant traffic. It also integrates with Cisco ISE to create asset groups and leverages Cisco industrial network equipment to dynamically enforce segmentation policies.

- Secure data transport—Data integrity is critical to the operations of the grid. Grid operators depend on secure data transport for real time and near time monitoring data as well as remote operational modifications and results of those changes to determine if further actions are necessary. Compliance mandates separation of critical data and encryption of data exiting a physical perimeter. Logging information must also be maintained with proof of secure delivery to the logging collector and storage facilities.

Threat detection and mitigation

When industrial networks are connected to IT networks, they must be protected from the usual IT threats such as malware or intrusion. Attacks on industrial networks generally appear to be legitimate instructions to assets and must be detected to prevent process modifications. To secure an industrial network, a variety of threat detection mechanisms are required.

Cisco Cyber Vision combines protocol analysis, intrusion detection, and behavioral analysis to detect any attack tactic. Future versions of this guide will elaborate on this subject. Steathwatch monitors application flow at every point in the network and identifies anomalies of data traversing the network (data in flight). ISE is the policy engine monitoring devices entering the network and departing and triggering an enforcement if something is in violation and works with the ISA-3000 firewall as well as Cisco routers and switches all the way to the edge. Integrations in this manner provide a comprehensive end to end industrial security solution.

System Overview

Security Concerns in the Changing Utility Landscape

The utility industry is undergoing a number of significant changes. Grid design at the distribution layer is moving to a more dynamic model incorporating intelligent devices at or near the edge. The inclusion of residential and commercial solar, the islanding and re-connection of micro-grids, and even the dynamics of electric vehicle charging are increasing challenges on grid operators to maintain a stable and reliable electrical distribution network. Grid operators cannot maintain the necessary stability without load demand information and in some cases predictive analysis based on historical data.

Grid Digitalization

A secure and highly reliable data network to the edge of the grid is required to deliver the data on which the operators rely so heavily. The ability to adjust the grid remotely in real time or use remote compute and analytics to automatically make changes in the grid is being referred to as the digitalization of the utility grid. This digitalization of the grid and the migration to a more dynamic grid is a necessary progression, and it exponentially increases the attack surface.

Design of the utility grid has not changed significantly in the last 100 years. The current shift to a more connected and data-driven operation of the grid is necessary to maintain stability due to the dynamics at the consumer edge. The increasing number of devices connecting to the grid demand a properly architected grid that can be safer, more reliable, and more secure. When establishing device logging, encryption, and threat analytics throughout the data network to the edge, the data network actually becomes a security tool. This secure network delivers trusted real time visibility to the device behavior operating the grid from the control center to the operational status of each device in the substation and eventually to the edge.

Substation Digitalization

Transformers, RTUs, relays, and PLC designs are all moving away from legacy and proprietary interfaces—and typically slower serial interfaces—to a more common and standards-based Ethernet communications interface. It may be difficult or financially challenging for a utility operator to migrate an entire substation at one time from a serial-based control network to an Ethernet network, so this migration is often done piecemeal or as assets age out. This makes developing a migration strategy critical.

Migration Strategies

Migration security strategy starts with device visibility and a clear understanding of the existing asset posture in the substation. Once the devices are known, a vulnerability assessment is critical and a remediation plan for devices with known vulnerabilities is necessary. If some devices cannot be patched at this time, an external scheme must be designed to protect them from remote or unauthorized access. Numerous tools are available including port security features, MAC ACLs and application layer profiling, and micro-segmentation, to name a few. The concept is to lock the device down at the point it accesses the network and only allow it to communicate with the specific devices necessary to complete its operation.

Terminal servers are often deployed for devices requiring serial connections; these should be eliminated or at least secured in a similar way. Most serial-based SCADA protocols can be transported over a packet (Layer 3) network using tunneling technologies (TCP-RAW-SOCKET) to a secure control center. This provides a single security point for assessment and helps to further reduce the vulnerabilities at the edge.

Ongoing Substation Monitoring

Once an assessment is completed, the migration or upgrade/replacement of end devices is in progress or even complete in the substation, ongoing monitoring of low level traffic flows is necessary. Details about communication peers on the process bus or between the process bus and station bus, for instance, are necessary to ensure stable operations. Continued monitoring of peer-to-peer and client-to-server (SCADA) protocols and communication flows is also

necessary to maintain a secure posture. Security can not be maintained with a "set-and-forget" approach. Continuous monitoring, especially for anomalous behavior and the secure alerting of any status changes, unplanned device additions, or deletions is necessary and often required by compliance mandates.

Physical Security

Cyber security is not the only security concern. Physical security and the monitoring capabilities that come with it have also seen significant improvements in the last few years. Monitoring the physical security of remote assets, such as a substation or a recloser cabinet on a pole, is part of the effort to improve reliability and prevent unwanted access, malicious attacks, and theft to address worker safety and security concerns. Video cameras, badge readers, and other sensors are being integrated to identify users authorized at a physical location.

Acoustical sensing and laser technologies are able to help eliminate false positives by identifying approaching vehicles that are continuing or stopping, and identifying and discriminating between animals and humans. A solid physical security system may be an early warning system for cyber security. These layered sensing technologies tied in with video provides a security team with much more detailed information about a possible threat, intruder, employee in a facility, or simply the status of a remote asset under both normal and adverse conditions. Consider the savings if storm damage can be assessed before dispatching a crew.

Data from these physical security devices and monitoring systems have the potential to oversubscribe a network, particularly a bandwidth-constrained wide area network. These monitoring systems are often lightly monitored and have little output unless triggered; they then tend to generate high traffic or bursts that must be accommodated. These bursts and any event alerts, either physical security or cyber security alerts, can be dealt with in a number of ways including a structured QoS scheme, alternate paths via a secondary WAN connection such as a low cost cellular or DSL connection utilizing either SD-WAN, or other least-cost routing mechanisms.

Comparing Attack Examples

The utility industry has a number of examples to learn from and help improve best practices. The physical security attack on the Metcalf substation in northern California and the nation state cyber-attack on the Ukrainian grid are two of the most publicized and noteworthy.

The physical security attack and damage to the Metcalf substation was a well organized and coordinated effort, but it had very little impact on the overall grid. This attack was effective in that it did take the substation down and was a significant expense to the operating utility. The lessons learned include improved perimeter security, additional high quality cameras, and additional analytics for the video feeds to identify persons of interest and anyone loitering at or near the fence line of a substation or any asset deemed of value.

The communications and controls network to the Metcalf substation were compromised, so real time physical monitoring was eliminated. Best practices would be to include a low cost alternate connection, such as cellular router or some form of radio or wireless connection into the substation data communications architecture. The cellular connections or other alternate data path would be capable of handling basic SCADA monitoring and high quality video providing multiple levels of situational awareness.

Conversely, the Ukrainian incident was disruptive to the utility, local and regional businesses, government, and the general public. This was also a well-coordinated remote cyber attack. As a result of the attack, it became apparent that the "security-by-obscurity" strategy is no longer viable. The lack of visibility into the grid and the events as they were unfolding was crippling to the utility operator. The legacy protocols and control system could not monitor for intrusion, remote access, or compromise. It can be prohibitive to upgrade or patch against known vulnerabilities, especially in remote patching situations.

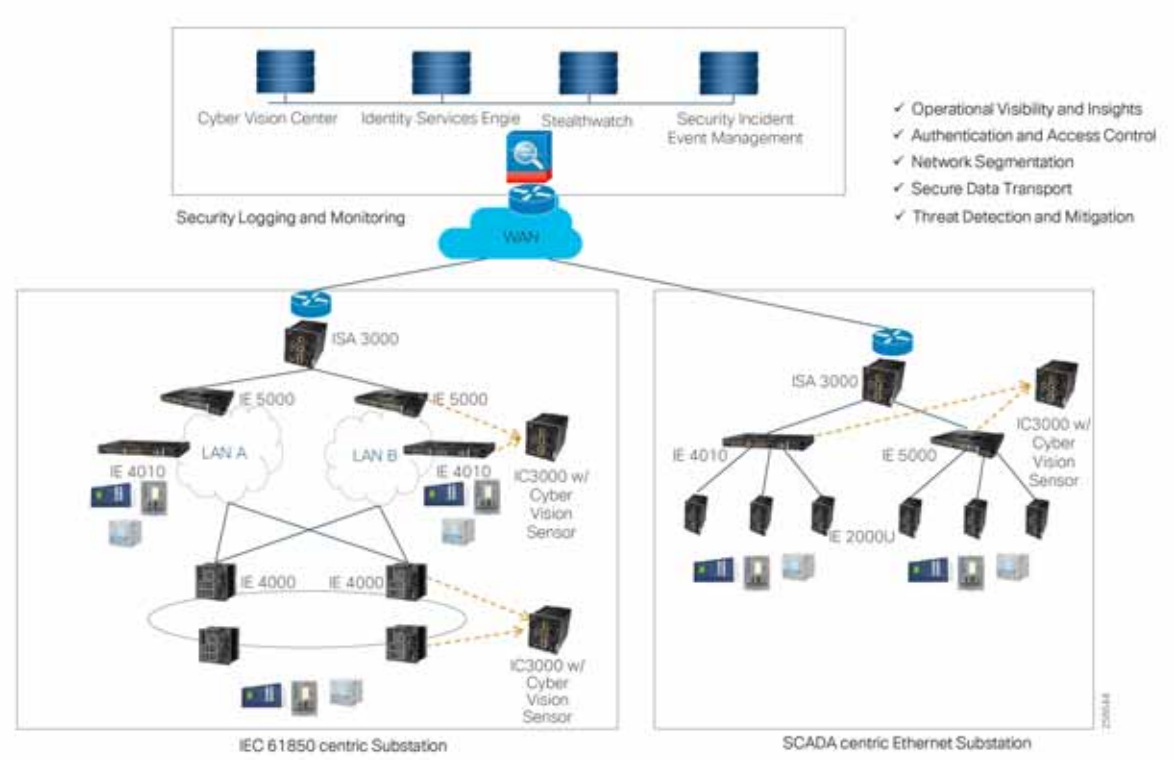
Best Practices

Best practices include significant efforts to segment lines of business, providing a boundary to apply controls and monitoring. Best practices are discussed below.

- Protection of the control center is paramount. Segmentation between IT and OT is ideal, although a true air gap is logistically impossible to implement and maintain. However, very tight segmentation and controls are possible and operationally effective.

- Network Administrators can apply a “jump box” facility, such as various remote desktop products, in conjunction with firewalls and AAA services to authenticate users and traffic traversing domains. IT and corporate (non-operational) networks are highly connected and security around user web access, email, and common practices around patching of servers and client devices become necessary to protect the utility and thwart a compromise from a beach head established inside the utility domain.
- Separation between business units and the establishment of perimeters and clearly defined boundaries both between and within IT and OT is necessary. This includes separation and monitoring between substations and also between the control and operations networks.
- A continuation of this segmentation is to implement firewall services in the substation, providing segmentation within and to the substation. For example, the WAN would be generally untrusted with only very specific connections permitted.
- The establishment of DMZs and levels of trust between networks for specific use cases within the substation. This might include the concept of a grid ops segment (security perimeter) for grid control devices only, a physical security DMZ for instance, or a segment/DMZ for IP telephony with phones and video end points. This is depicted in the Cisco reference architecture in Figure 2.

Figure 2 Defense-in-Depth Approach to Securing the Utility Substation



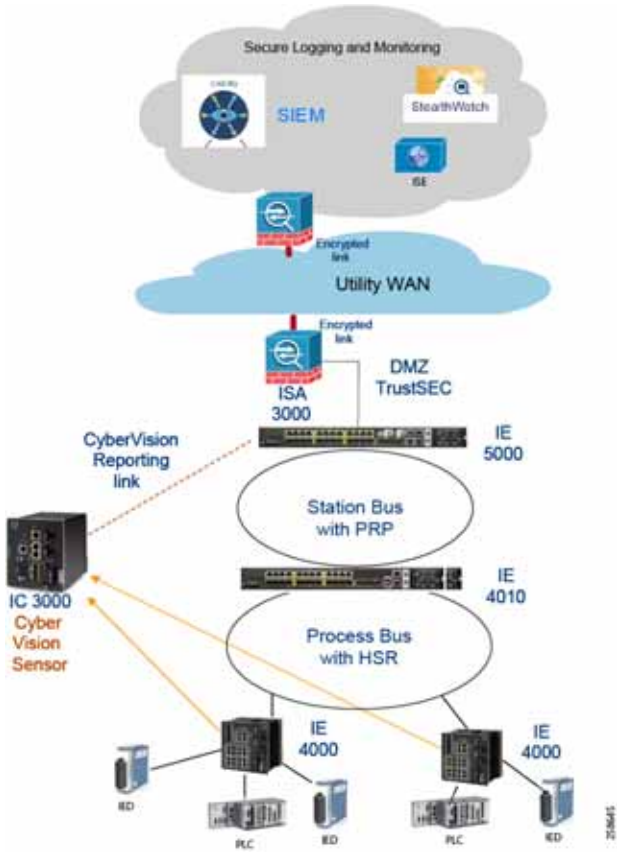
- Device identity and vulnerability assessments are necessary. The lack of visibility and situational awareness capability is commonly overlooked or inadequately architected. The truth of the adage “you cannot protect what you cannot see” was evident in both attack examples. Lack of segmentation and visibility played a significant roll in the Ukrainian compromise from the onset. A well architected and layered security posture would have identified and prevented the intrusion at various points throughout the infrastructure.

Summary

Address legacy and unpatched systems. Operation technologies, especially legacy and proprietary operation and control systems, present specific challenges to the cyber security specialist. Tools like port security features, MAC filtering, and ACLs can be implemented on the local switches connecting devices. Monitoring tools like SNMP and NetFlow are helpful to monitor connectivity and application level flows, even detecting anomalies at the network, session, and application layers of the OSI model. A significant amount of communication has previously gone unmonitored. Lower level substation equipment often communicates only within the substation. Examples of this are IEDs to RTUs, and most notably the multicast traffic in a 61850-implemented substation. Many devices communicating only at Layer 2 via multicast have been all but invisible to a remote operator (see Figure 3).

Secure stable connectivity to the edge of the grid. A compromised or even malfunctioning device has the ability to disrupt communications at both the process bus as well as the station bus. A faulty device could continuously transmit bad data onto a multicast network, congesting it in what looks like a distributed-denial-of-service (DDoS) event. The substation could become inoperable and in an unknown state until the substation engineer arrives, troubleshoots, and remedies the situation. Now consider this same faulty device, but with Layer 2 tools enabled, and visibility into detailed flow information. The remote operator is notified of a possible problem through normal alerting. The operator might troubleshoot or down the port connected to the offending device or quarantine that device. Resolution moves from hours to minutes and potentially seconds without a costly truck roll.

Figure 3 Cisco Cyber Vision Passive Mode Deployment in the Utility Substation



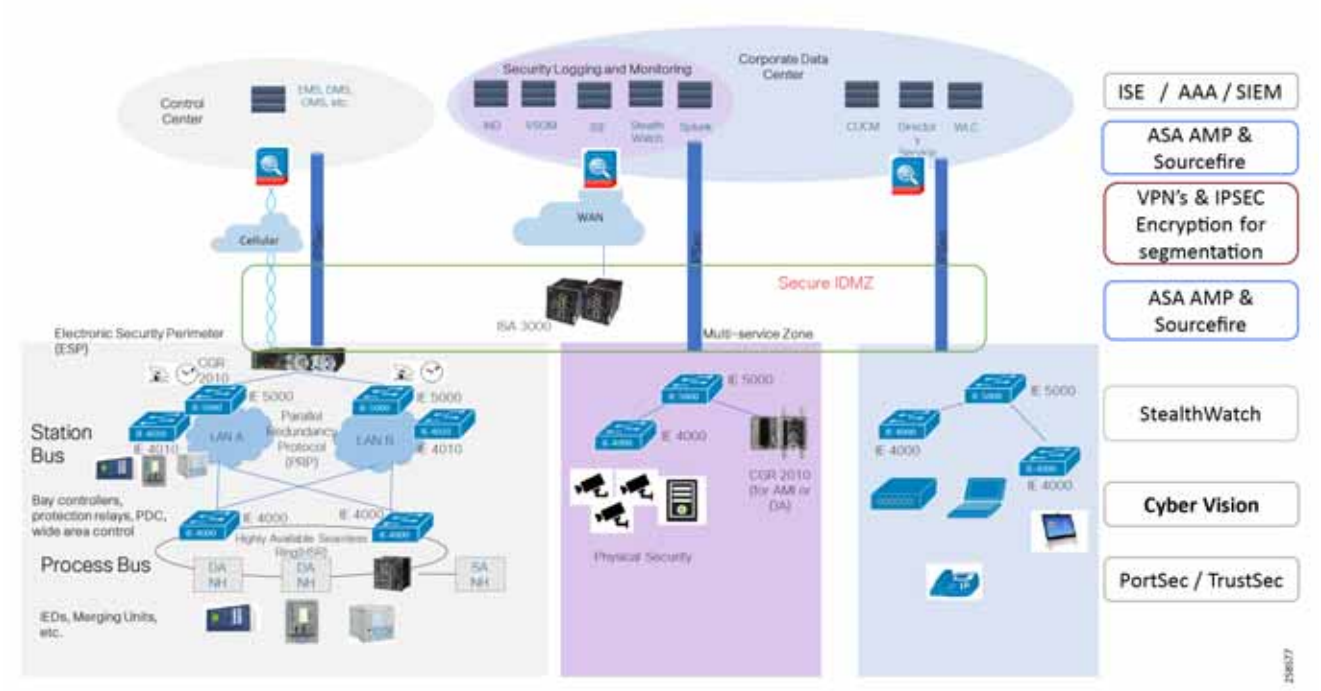
Business Drivers

Security of the grid is quickly gaining global recognition among utility operators, government and legislative bodies, and the media. Utilities across the globe are reporting a significant increase in identified threats and attach attempts at the perimeter of their IT and OT networks.

We have witnessed NERC CIP violations that have impacted a utility with fines in the amount of ~$10M based on seemingly minor violations. Headlines have highlighted business impacts to other organizations totaling $243B in estimated losses because of a ransomware attack. Notable research organizations have stated that approximately 31% of OT-based organizations have suffered a cyber attack. The result of a security breach has far reaching financial implications; the impact of incurred direct loss and potential fines levied may be insignificant to the utility as compared to the damage to its reputation and ability to raise capital in the future.

A well architected and comprehensive security solution can have exactly the opposite financial effect and provide a secure and compliant OT network. See Figure 4. Leveraging best practices and defense-in-depth, such as that defined in this document, can become a financial asset. A single system is easier to maintain, more reliable and trusted, with fewer integration costs and ongoing operational costs, thus reducing both Capex and Opex over the life of the system. Compliance reporting and audit responses becomes easier.

Figure 4 Placement of Cisco Security Tools in the Utility Grid for Maximum Effectiveness



Visibility is key to security and the utility substation, especially brownfield locations in transition. It is difficult to inventory and maintain operational details about its critical infrastructure. The cost to manually inventory is significant and highly suspect due to errors; in some instances such an inventory is physically or logistically impossible.

Classic discovery tools are typically blind to legacy and proprietary devices and often dependent on Layer 3 boundaries. These tools are often disruptive and create problems on a bandwidth sensitive network. For instance, a substation-wide probe on a subnet or on a muticast network can turn into, effectively, a DoS attack and render the connected devices unreachable. So a complete and accurate inventory becomes virtually impossible to obtain and even harder to maintain. The Cisco Cyber Vision continuous passive monitoring, deep packet inspection, and profiling capabilities enable constant and real time inventory of devices, posture, and firmware and software versions with a knowledge base to instantly correlate and identify known vulnerabilities.

For true business impact, a security architecture needs to address more than just asset inventory and visibility. It also requires integration into the security operations center and other systems like AAA services and remediation systems. This guide describes these integrations in later sections and configurations are detailed in the accompanying implementation guide. The data being reported and leveraged for both audits as well as day-to-day operations and the security posture assessment must be secure and trusted in and of itself, with secure transport to a repository or an operations center.

TrustSec with secure group tags (SGTs), encryption, and device authentication for both the reporting devices as well as the numerous potential enforcement points all help to build a secure, robust, and operationally sound infrastructure. Anomaly detection and monitoring of data in flight at the network and application layers via Stealthwatch and Cyber Vision increase security visibility and remediation capabilities.

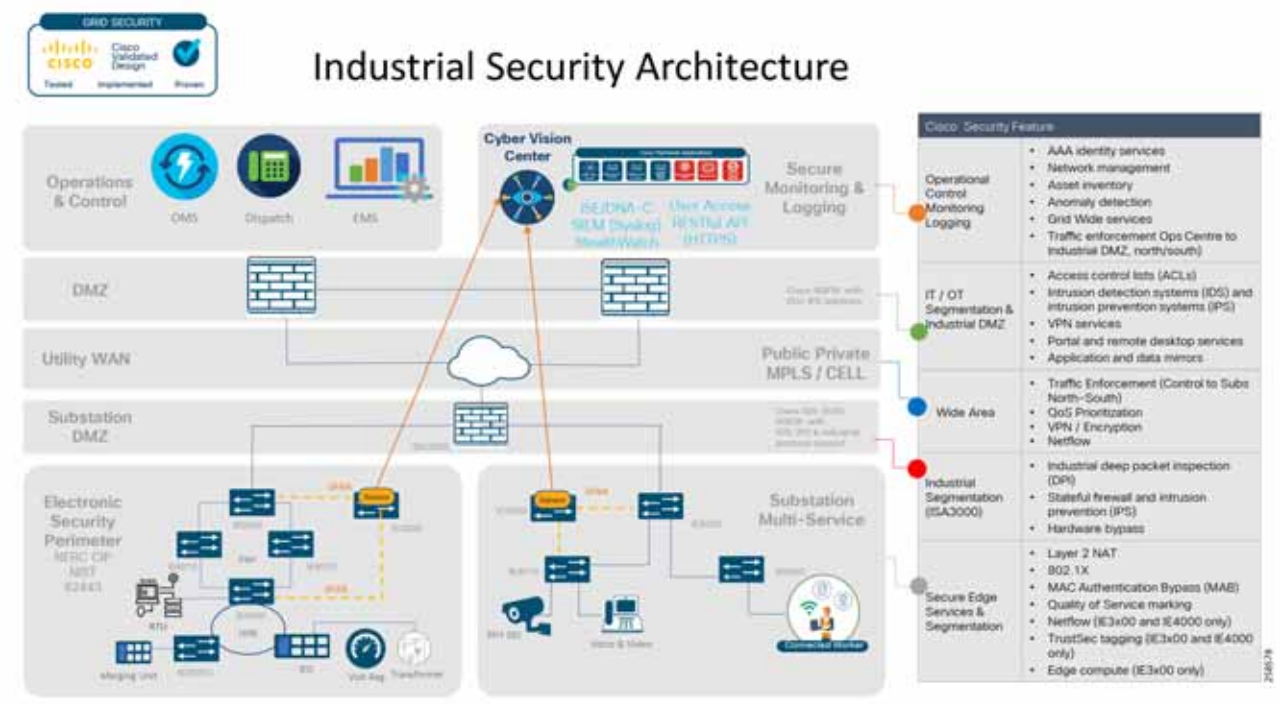
These integrated systems improve operational capabilities and protection to systems. Integration and centralized management significantly reduce operational costs, time, and exposure to the utility as a whole. This is the benefit of one system versus integrating numerous questionable compatibility points from multiple vendors.

System Architecture

Grid Security Solution Overview and Architecture

A solid security architecture leverages a defense-in-depth approach. This guide details the integration of multiple security tools and devices to accomplish this in an OT environment, which Cisco refers to as IoT Threat Defense. In the next section we detail the products and tools leveraged in this architecture. This holistic security solution addresses the unique requirements of the utility network with best practices and compliance requirements like those found in NERC CIP and IEC 62443 and the NIST framework.

Figure 5 Holistic Architectural Model for the Modern Utility Grid



Separation and segmentation are at the heart of these best practices with numerous points of inspection. This architecture accomplishes this in a variety of ways, including VLAN segmentation and micro-segmentation with TrustSec. The architecture leverages these tools in conjunction with segmenting the substation, control center/operations center, and data center with secure DMZs on the Cisco ISA 3000 and Cisco Firepower-enabled firewalls. These Cisco Firepower NGFWs provide segmentation but also a point of deep packet inspection for packets entering, exiting, or traversing between DMZs. Segmentation is continued by mapping networks or even a group of devices into a VRF and carrying that segmented traffic across a secure or encrypted WAN.

Security starts at the edge: trust must be established for the device and the device user before secure access to the network is granted. The Cisco ISE leverages 802.1x and other tools like MAC profiling or DHCP and port profiling to identify edge devices and apply profiles to each edge port.

Cisco ISE can be leveraged as a directory server (AAA) in standalone or integrated with a user authentication server such as Microsoft Active Directory (AD). These IT-based mechanisms are not enough to fully identify OT devices at the edge. Detailed asset probing can be destructive to a fragile operations network. However, Cisco Cyber Vision utilizes a passive approach of deep packet inspection to map edge devices to known device profiles with a comprehensive knowledge base to identify assets at the edge that include detailed protocol knowledge, device types, make and model, as well as software and firmware versions. So a highly detailed asset inventory can be established for the devices at the edge of the most remote locations or in the control and operations centers.

Active and Passive Scanning

There are two approaches to network vulnerability scanning:

- The active approach includes everything an organization does to foil system breaches, such as system and application vulnerabilities.
- The passive (or monitoring) approach entails all the ways the organization oversees system security. The passive approach allows security personnel to monitor:
  - Which operating systems are in use
  - What is being sent to, from, and within the system
  - Which services are available
  - Where parts of the system may be vulnerable to security threats

These two types of protection complement each other.

Active scanning is recommended only after a thorough passive scan is complete, and the underlying architecture is known. Active scanning on an unknown infrastructure can be detrimental to the operations network. A potential workaround to active scanning is to use the existing control system to query a device for software version. Cisco Cyber Vision will see that detailed data in a passive mode and correlate against a knowledge base of device types, make, model, and even known vulnerabilities.

Table 2 displays contrasting characteristics between passive and active scanning.

Table 2 Passive and Active Scanning Comparison

Characteristic	Passive Scanning	Active Scanning
Disruption risk	Very low – Passive scanning does not quiz the asset and merely inspects the packets behaving as a passive observer. The packets do have to be duplicated in order to observe them. One precaution is to ensure that the duplication of observed traffic does not over-subscribe the available bandwidth of the network. There are easy architectural solutions to ensure that such a case does not happen. Cisco has a very effective strategy with our network devices and Cisco Cyber Vision. Essentially the passive scanning sensor will be available within the network element and traffic will not need to be duplicated on the network.	Medium – Active scanning may adversely affect the asset or the network; caution is advised when using active scanning methods. In a production environment active scanning and especially repeated active scanning may cause production outages. Some older controllers and devices may not handle PING/ARP packets efficiently. There is no architecture or design methodology that eliminates the risk completely. Best case is to devise operational methods to contain the risk. For example, active scans can be carried out during production planned downtimes or limited to selected protocols or a very contained subnet. Another caution is to manage the frequency of pings or quiz packets to the devices.
Complete asset discovery	Very effective – If an asset is communicating any packets, then it will be discovered. Of course this depends on the assertion that the sensor element of the passive scanner is able to see the packet. So effective placement of sensors is very important. An asset that neither sends nor receives any packets will not be discovered.	Variable – Some assets are offline during scans and will not be discovered. ACLs may prevent the quiz packets (for example SNMP) from reaching the asset or the subnet and cause the asset not to be discovered. This is one reason why multiple scans are run, however one needs to balance the risk of disruption. The completeness of discovery is highly dependent on the design of the network, ACLs, and ensuring that assets are online and are responsive to the quiz packets. Another challenge is that as new devices come online, unless an active scan is run, it may be a while before such an asset is discovered.

Table 2 Passive and Active Scanning Comparison (continued)

Complete asset information	Indeterminate — Passive scanning by its nature can only determine information that is transmitted by the asset. Some information may not be emitted for a long time, so an asset remains undiscovered. For example, you may know that there is a Rockwell PLC, but the version of the firmware of that PLC may not be known until a specific command causes a packet with the firmware version to be transmitted.	Highly determinate — If an asset is online and reachable and it responds to the quiz commands, then everything pertinent about the asset is discoverable. If an asset is not online or does not respond to all the quiz requests, then it can be marked as "not responsive". But in either case, operators can have very high confidence in knowing what they know and what they do not know.
Timeliness of asset information	Takes time to build a complete picture. Asset discovery of active assets can be instantaneous the moment they transmit a packet. However getting a complete picture of the asset can take time, as the passive scanner needs to wait for the relevant packets to be transmitted that contain the necessary information to complete the picture. This can be sped up by operators instigating benign pings to the asset.	On demand — With active scanning an asset can be quizzed on demand. However indiscriminate quizzing can cause unintended issues with the asset. It could get inundated and perceive it as a DoS attack.
Cisco products	Currently Cisco Cyber Vision focuses on passive scanning. Cisco Stealthwatch is also a passive monitor.	Cisco Industrial Network Director focuses on active scanning in addition to network management.

Cisco IE switches use the same port security features as enterprise class switches, such as MAC address mapping to lock a port to a particular MAC address, the ability to apply Layer 2 MAC address access control lists, and perform MAC filtering and spoofing. All of these tools can be applied on the Cisco IE switches identified as part of this architecture.

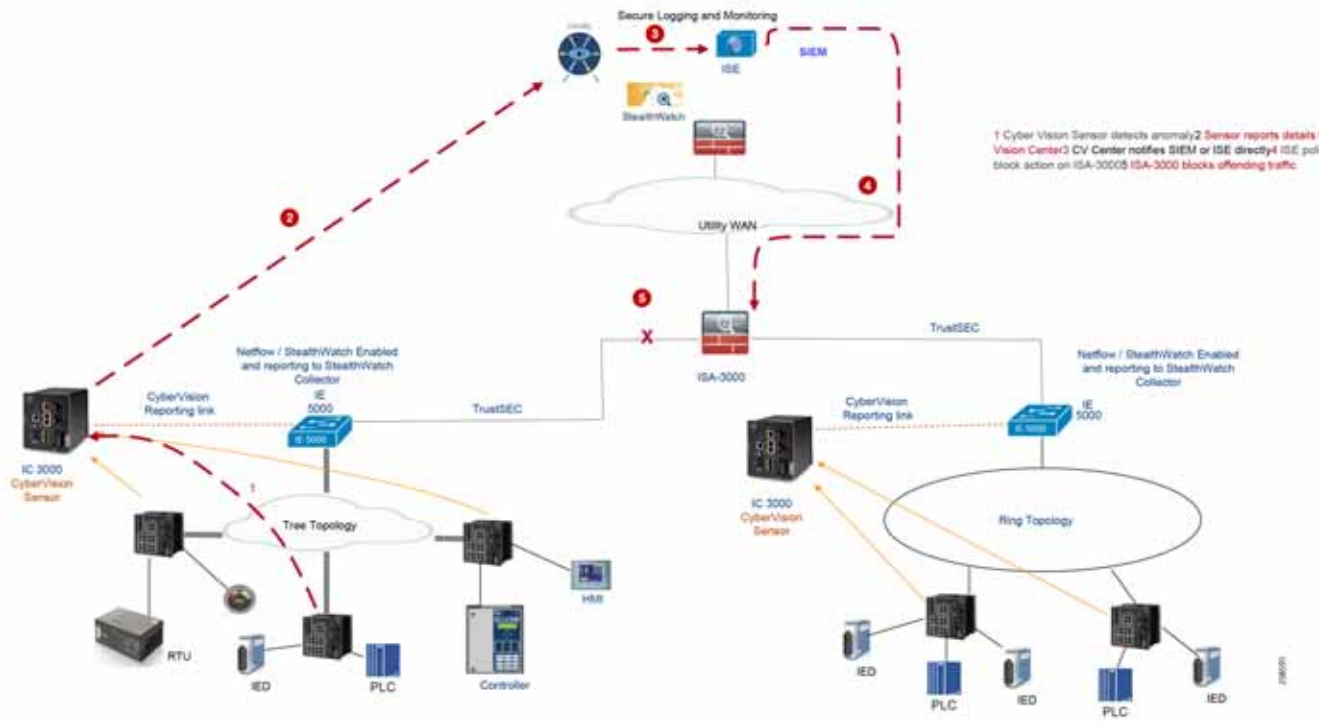
Once the identity of the edge device has been established and the device is on the network, the IoT Threat Defense continues to monitor traffic flows at the network, session, and application layers of the OSI networking model and performs deep packet inspection of both IT and OT specific protocols. Cisco Stealthwatch can be leveraged at every Layer 3 boundary from the edge switches to and through both the IT and OT networks for a full application by application mapping of the packets and data flow from one end of the network to the other—from edge device to server and back.

This inspection of in-flight traffic uses standards-based NetFlow data, well known protocol signatures, and a detailed knowledge base of both IT and OT protocols to monitor traffic as is traverses the network. Once a profile of a device and device peers is established, Cisco Stealthwatch and Cyber Vision become anomaly detection mechanisms. Alerts can be sent to an SIEM such as SPLUNK or IBM QRadar or, as in the case of the case of this CVD, directly to Cisco ISE.

Any device performing an anomalous function, including edge devices inadvertently misconfigured or in an error state, can be flagged. Once a device or traffic flow is identified as non-standard or fails to meet known good behavior and has trigged an alert, an SIEM and or Cisco ISE can dispatch profile-based enforcement to quarantine or block a particular port at the edge or leverage group profiles to block at a gateway or the Cisco ISA 3000 firewall.

Cisco adheres to the concept that every networking device is a security tool, and that approach is clearly evident throughout this architecture. See Figure 6.

Figure 6 Enforcement Scenario Depicting the Benefits of a Fully Integrated Security Architecture



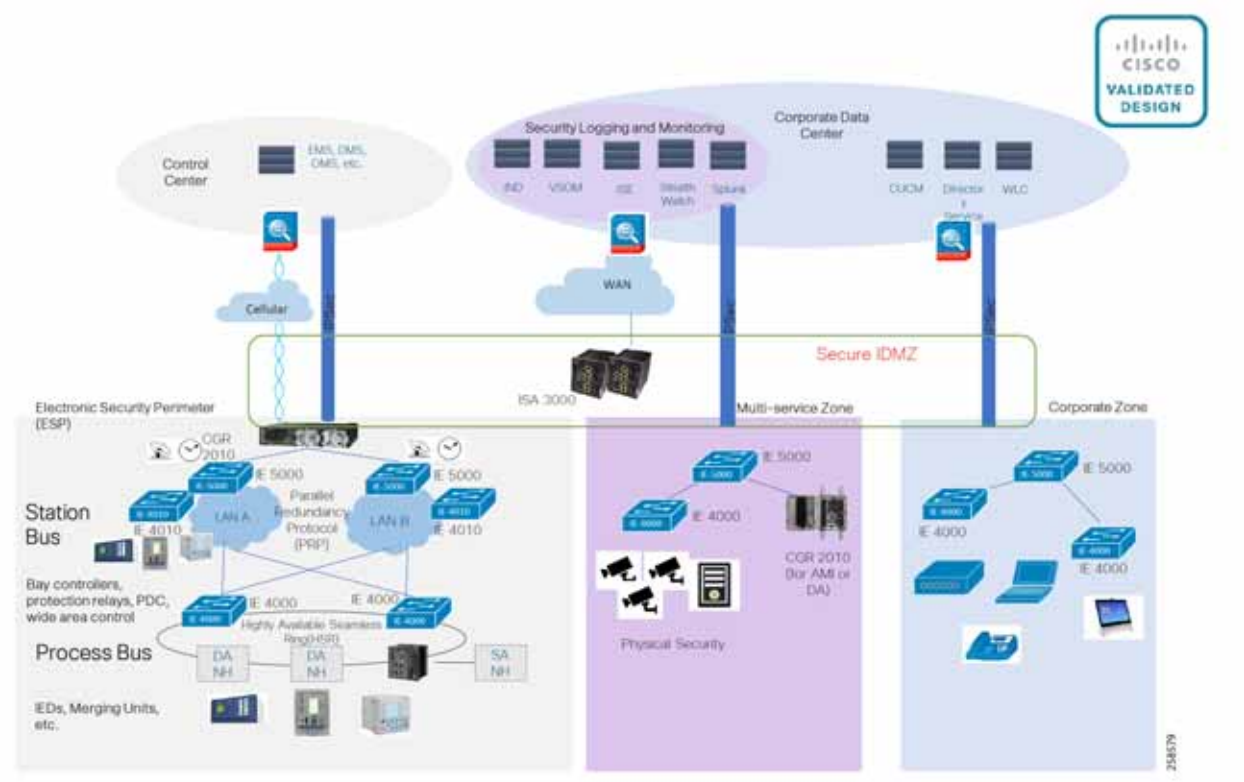
Network Topology

The Grid Security 3.0 architecture and recommendations in this document are the current version of a multi-year iterative process to improve the end-to-end security model for utility operators. Previous validation efforts started with many of the best practices defined earlier in this document and adherence to NERC-CIP, NIST, ISA-99 and IEC-62443 specifications. The initial efforts were implementation of the ISA-3000 in the substation, and segmentation via DMZs. Efforts following the initialization included port security and ISE integrations. See the initial white paper leveraging 802.1x and ISE in the substation titled **IoT Industrial Security – Wired User Access Control.**

Further validation efforts detailed Stealthwatch monitoring and leveraging TrustSec between segments in the substation as well as mapping to MPLS or IPSEC VPN across the wan. The following topology depicts this evolution with Mappings for SCADA and secure connection between the ESP and the control center. Figure 7 depicts and highlights the importance of defining a secure monitoring zone, often in the corporate data center, but certainly viable in the control center. The centralized collection of logs, diagnostic information and security alerts, and results from edge analytics is critical to the scalability of this solution and for any grid operator to acknowledge and trust the data on which they rely to operate the grid.

A secure connection from each of the zones defined in the substation is mapped via TrustSec and PVCs on the Cisco ASRs to the final location in the control center of corporate data center thus maintaining a clear separation of zone communications, security levels, and data integrity.

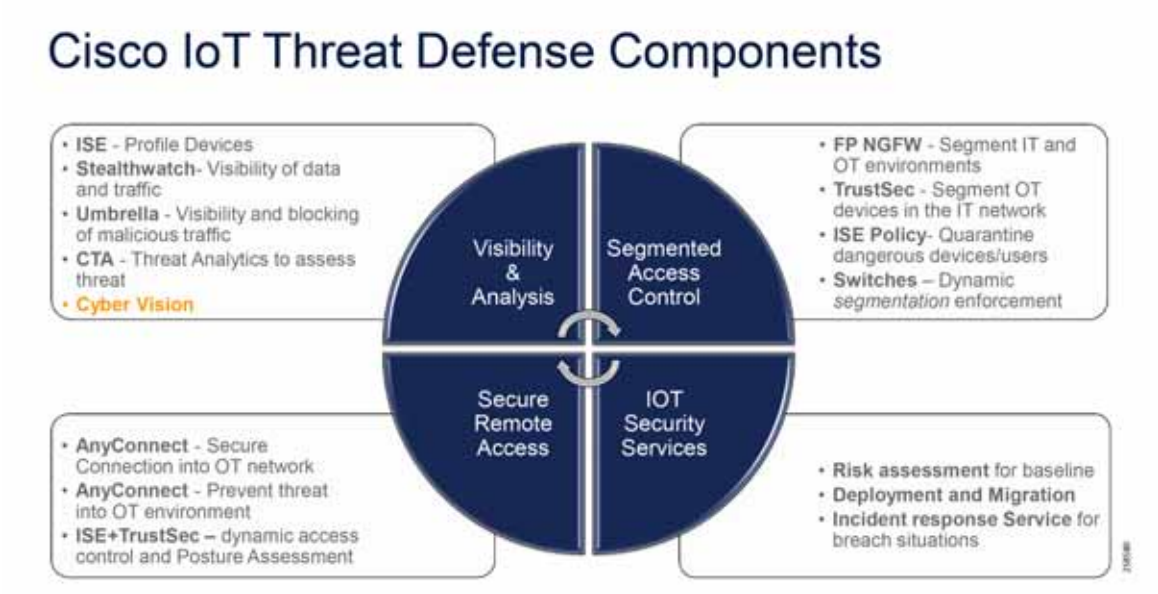
Figure 7 Validated Security Architecture Leverages Segmentation and Data Isolation



System Components

The components depicted in Figure 8 below comprise the Cisco IoT Threat Defense strategy.

Figure 8 Cisco Holistic IoT Threat Defense Components



Cisco ISA 3000 and Firepower

The Cisco ISAs are true industrial firewalls that provide OT targeted protection based on proven enterprise class security.

The Cisco ISA 3000 with four data links is a DIN rail mount, ruggedized appliance that provides the widest range of access, threat, and application controls for the harshest and most demanding of industrial environments. The Cisco ISA 3000 Series starts with the same industrial success of the Cisco IE 4000 switch hardware design and adds the proven security of the Cisco ASA firewall and Firepower Next Generation IPS software. The Cisco ISA 3000 Series is purpose built for industrial Ethernet applications where hardened products are required.

Proper deployment of the Cisco ISA 3000 industrial firewall can fulfill security requirements associated with a variety of industrial standards, regulations, and guidelines such as NERC-CIP, ISA 99, ISA 62443, CFATS, ANSI/AWWA G430, and others.

Managed through either a user-friendly on-box system manager or company wide security management, the Cisco ISA 3000 provides industrial focused, out-of-the-box configuration and simplified operational manageability. These highly customizable management options allows for simplified local operational awareness and higher order IT/OT security convergence for the inevitable mingling of industrial and IT capabilities.

Cisco Identity Services Engine

The Cisco ISE s your one-stop solution to streamline security policy management and reduce operating costs. With Cisco ISE, you can see users and devices controlling access across wired, wireless, and VPN connections to the corporate network.

Cisco ISE allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

Customer Advantages

Cisco ISE offers a holistic approach to network access security; gain for the customer when Cisco ISE is deployed include:

- Highly secure business and context-based access based on your company policies. Cisco ISE uses multiple mechanisms to enforce policy, including Cisco TrustSec software-defined segmentation.
- Streamlined network visibility through a simple, flexible, and highly consumable interface.
- Extensive policy enforcement that defines easy, flexible access rules that meet your ever-changing business requirements, all controlled from a central location that distributes enforcement across the entire network and security infrastructure. Managing switch, router, and firewall rules becomes easier and has shown to help reduce IT operations by 80% and increase time to implement changes by 98%.
- Robust guest experiences that provide multiple levels of access to your network.
- Self-service device onboarding for the enterprise Bring-Your-Own-Device (BYOD) or guest policies.
- Central network device management using TACACS+. Cisco ISE allows you to manage network devices using the TACACS+ security protocol to control and audit the configuration of network devices.

Integrated Solutions

Cisco pxGrid is a highly scalable IT clearinghouse for multiple security tools to communicate automatically with each other in real time. Cisco ISE and Cisco pxGrid 2.0 provide a new WebSockets client and remove dependencies on underlying operating systems and languages. More than 50 integrations are available from Cisco and third-party vendors, notably Cisco Cyber Vision, which uses Cisco pxGrid to provide OT endpoint information to Cisco ISE. Additionally, Cisco pxGrid is used to share IP-to-SGT information about endpoints allowing security products to apply security group access control using SGTs (TrustSec).

Cisco Rapid Threat Containment simplifies and automates network mitigation and investigation actions in response to security events. It integrates Cisco ISE and Cisco security technology partner solutions in a broad variety of technology areas. With Threat-Centric Network Access Control (TC-NAC), it can change user access based on CVSS vulnerability and STIX threat scores. With the Cisco pxGrid Adaptive Network Control (ANC), it gives you the ability to reset the network access status of an endpoint to quarantine, unquarantine, bounce, or shut down a port.

Cisco Stealthwatch

Cisco Stealthwatch Enterprise provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Cisco Stealthwatch Enterprise can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the entire network traffic, even if it is encrypted.

Cisco Stealthwatch enlists the network to provide end-to-end visibility of traffic. This visibility includes knowing every host—seeing who is accessing which information at any given point. From there, it is important to know what is normal behavior for a particular user or “host” and establish a baseline from which you can be alerted to any change in the user's behavior the instant it happens.

Customer Advantages

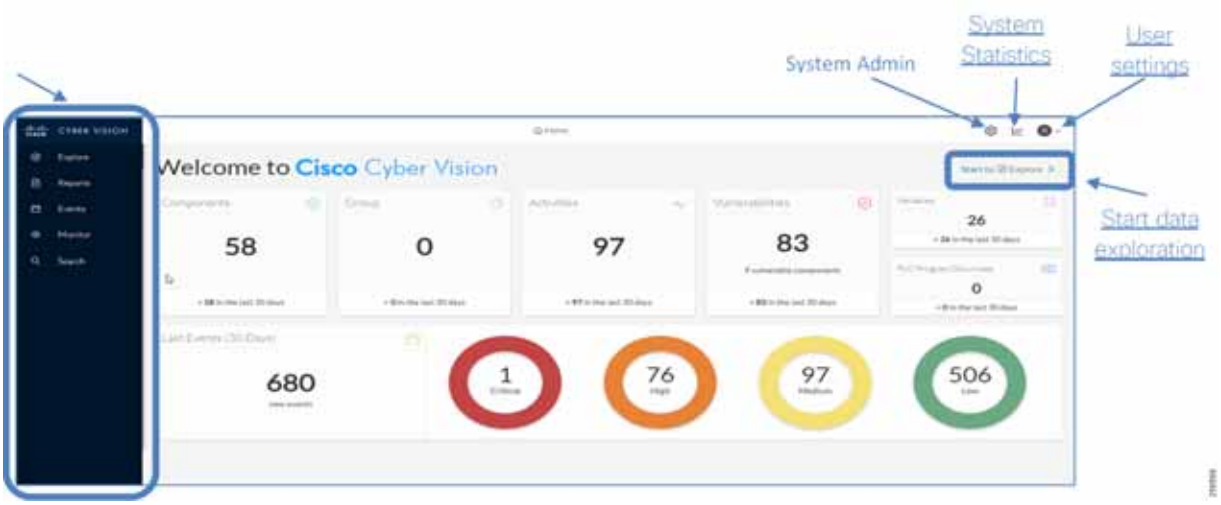
Cisco Stealthwatch offers many advantages when deployed, including:

- No more blind spots—Cisco Stealthwatch is the only security analytics solution that can provide comprehensive visibility in the private network as well as the public cloud and without deploying sensors everywhere.

- Focus on incidents, not noise—Using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, Cisco Stealthwatch reduces false positives and alarms on critical threats affecting your environment.
- Catch them in the act—Cisco Stealthwatch is constantly monitoring the network in order to detect advanced threats in real time.

Cisco Cyber Vision Center

Figure 9 Cisco Cyber Vision Center Dashboard



Cisco Cyber Vision combines a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio. Built into your Cisco industrial network equipment, it can be easily deployed at scale to monitor your industrial assets and their application flows in real-time. It is the ideal solution to feed your IT SOC with OT context, so you can build a unified IT/OT cybersecurity architecture.

Cisco Cyber Vision leverages a unique edge computing architecture that enables security monitoring components to run within Cisco industrial network equipment. There is no need to source dedicated appliances and think about how to install them and no need to build an out-of-band network to send industrial network flows to a central security platform. Cisco Cyber Vision enables the industrial network to collect the information required to provide comprehensive visibility, analytics, and threat detection. Network managers will appreciate the unique simplicity and the lower costs of the Cisco Cyber Vision architecture to deploy OT security at scale.

Visibility

Securing your OT infrastructure starts with having a precise view of your asset inventory, communication patterns, and network topologies. Cisco Cyber Vision gives OT teams and network managers full visibility into their assets and application flows so they can implement security best practices, drive network segmentation projects, and improve operational resilience.

Cisco Cyber Vision automatically uncovers the smallest details of the production infrastructure: vendor references, firmware and hardware versions, serial numbers, PLC rack slot configuration. It identifies asset relationships, communication patterns, changes to variables, and more. This wealth of information is shown in various types of maps, tables, and reports that maintain a complete inventory of industrial assets, their relationships, their vulnerabilities, and the programs they run.

Operational Insights

Cisco Cyber Vision gives OT engineers real-time insight into the actual industrial process status, such as unexpected variable changes or controller modifications. They can take action to maintain system integrity and production continuity. Cyber experts can easily dive into all this data to analyze attacks and find the source. CISOs have all the information to document their incident reports.

Cisco Cyber Vision “understands” the proprietary OT protocols used by automation equipment, so it can track process anomalies, errors, misconfigurations, and unauthorized industrial events. It also records it all to be the “flight recorder” of the industrial infrastructure.

The product uses tags to highlight asset roles and communication contexts, so that any OT and IT team member can easily understand the industrial infrastructure and operational events regardless of the asset brand or references. IT teams can then work with OT staff to drive best practices such as patching vulnerable assets, tracking default password uses, improving network segmentation, and more.

Cisco IC3000 Industrial Compute Gateway

Figure 10 Cisco IC3000

The Cisco IC3000 Industrial Compute Gateway (Cisco IC3000) extends data intelligence to the edge of the IoT network to seamlessly bridge the intent-based network and IoT data fabric in a complete end-to-end solution for applications such as intelligent roadways, smart factories, and so on.

The Cisco IC3000 gateway is built with the same industrial success as the Cisco IE 4000 Series Switches hardware design, but is dedicated to bringing intelligence to the edge. It has two Ethernet ports and two Small Form-Factor Pluggable (SFP) fiber ports in a DIN rail-mounted, ruggedized appliance that provides the widest range of applications for the harshest and most demanding industrial environments.

The Cisco IC3000 gateway delivers the next level of computational power, up from IR 809 and IR 829, for applications that demand more processing power for data analytics and real-time critical decision making at the edge of the IoT network. It enables smart roadway applications such as traffic pattern detection, hazardous weather warnings, and road condition detection. With built-in interfaces that support a wide range of industrial standards and a simple development toolkit, the Cisco IC3000 enables application developers to unleash their creativity in creating applications that harness the wealth of IoT data.

The Cisco IC3000 is fully supported by Cisco IoT Field Network Director for zero- touch deployment, life-cycle management, application management, monitoring, and troubleshooting securely at scale from a single pane of glass. With its support for the Cisco Kinetic™ Edge and Fog Processing Module, which computes data in distributed nodes, it seamlessly integrates with the Cisco Kinetic Data Control Module, which moves the right data from a diverse set of devices to the right cloud-based applications at the right time, according to policy set by the data owner.

Cisco Industrial Ethernet Switches

Figure 11 Cisco IE 4000

Figure 12 Cisco IE 4010

Figure 13 Cisco IE 5000

The Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 Series delivers Gigabit connectivity to Cisco ruggedized switching portfolio with superior high-bandwidth switching capacity and proven Cisco IOS Software. The Cisco IE Switching Series provides highly secure access and industry-leading convergence ring protocols to support resilient and scalable networks while adhering to industry compliance requirements.

The Cisco IE Switching Series is ideal for industrial Ethernet applications where hardened products are required, including manufacturing, energy, transportation, and smart cities. The Cisco IE Switching Series has built-in SW image verification to ensure authenticity of the Cisco software. With improved overall performance, greater bandwidth, advanced security features, and enhanced hardware, the Cisco IE Switching Series complements the current industrial Ethernet portfolio of related Cisco industrial switches, such as the Cisco IE 2000 and Cisco IE 3000.

The Cisco IE Switching Series can be used to easily and securely extend the enterprise network to harsh environments with a software-defined access extension for IoT, enabling connectivity in outdoor areas, warehouses, distribution centers, and roadways using powerful enterprise-grade intent-based network management platform such as Cisco DNA Center.

The Cisco IE Switching Series can easily be installed. with a GUI based Device Manager, it also offers out-of-the-box industrial usage configuration and simplified manageability to deliver advanced security, data, video, and voice services over industrial networks.

The Cisco IE Switching Series executes edge applications using Cisco IOx to transform sensor data into insight and action. With Cisco IOx for customers take advantage of consistent, distributed computing across Cisco IoT network infrastructure.

Substation Router

Figure 14 Cisco ASR900

Figure 15 Cisco CGR-2010

Figure 16 Cisco IR1101

Figure 17 Cisco IR807

Cisco ASR 900 Series Aggregation Services Routers are full-featured, modular aggregation platforms. They are designed for the cost-effective delivery of converged mobile, residential, and business services. You get redundancy, a shallow depth, low power consumption, and high service scale in routers packed with useful features and optimized for small aggregation.

Component Design

The Cisco ASR 900 Series routers are built as fully modular systems with a future-ready design. The router chassis supports online field replacement and upgrades of all components. The Cisco ASR 907 Router is designed to contain one fan tray, up to three power supplies, two route switch processor (RSP) cards, and up to 16 interface module cards. The Cisco ASR 903 Router is designed to contain one fan tray, two power supplies, two RSP cards, and up to six interface module cards. The Cisco ASR 902 Router uses the same design as the Cisco ASR 903 Router, but due to its smaller size, it has four interface module cards and one RSP card. All components support online replacement and field upgrades, with the exception of the RSP card on the Cisco ASR 902 Router, which requires the system to be brought down for a replacement or upgrade.

The Cisco CGR 2010 is a rugged router optimized for use in the multitude of different communication networks found in the energy and utility industries (Figure 15). One example application for the Cisco CGR 2010 is for substation networks in harsh environments common in utility transmission and distribution substations. The Cisco CGR 2010 provides operators with the benefits of improved security, manageability, and network reliability. The Cisco CGR 2010 uses Cisco IOS Software, which is the operating system powering millions of Cisco routers deployed worldwide. Cisco IOS Software delivers the benefits of integrated security for North American Electric Reliability Corporation/Critical Infrastructure Protection (NERC/CIP) compliance, QoS, and network management to help ensure integrity and priority of operational data communications.

Primary Cisco CGR 2010 features:

- Rugged industrial design, featuring no fans or moving parts and an extended operational temperature range
- Substation compliance with IEC-61850-3 and IEEE 1613 for utility substation environments
- Integrated security to help address compliance with critical infrastructure protection mandates
- High availability design for maximum network uptime and redundancy
- Network and device management tools for deployments, upgrades, and remote monitoring
- Advanced QoS capabilities to support mission-critical communications such as substation communications such as SCADA
- Comprehensive network security features based on open standards

System Functional Considerations

Deployment Considerations

This section discusses the critical design considerations when deploying Cisco Cyber Vision solutions in industrial automation environments. Cisco Cyber Vision solution supports two deployment models: offline mode and online mode.

Cyber Vision Offline Mode

The offline mode involves capturing the data packets using a USB stick and then manually loading the data into the Cisco Cyber Vision Center for analysis. This option can be used by an OT engineer to perform a proof-of-concept.

- The offline mode can be used by an OT engineer when there is no Cisco Cyber Vision Center or there is no Layer 3 communication between the Cisco Cyber Vision sensor and the Cisco Cyber Vision Center.
- This option is limited by the storage space of the USB disk and is not a practical solution for long term data storage.

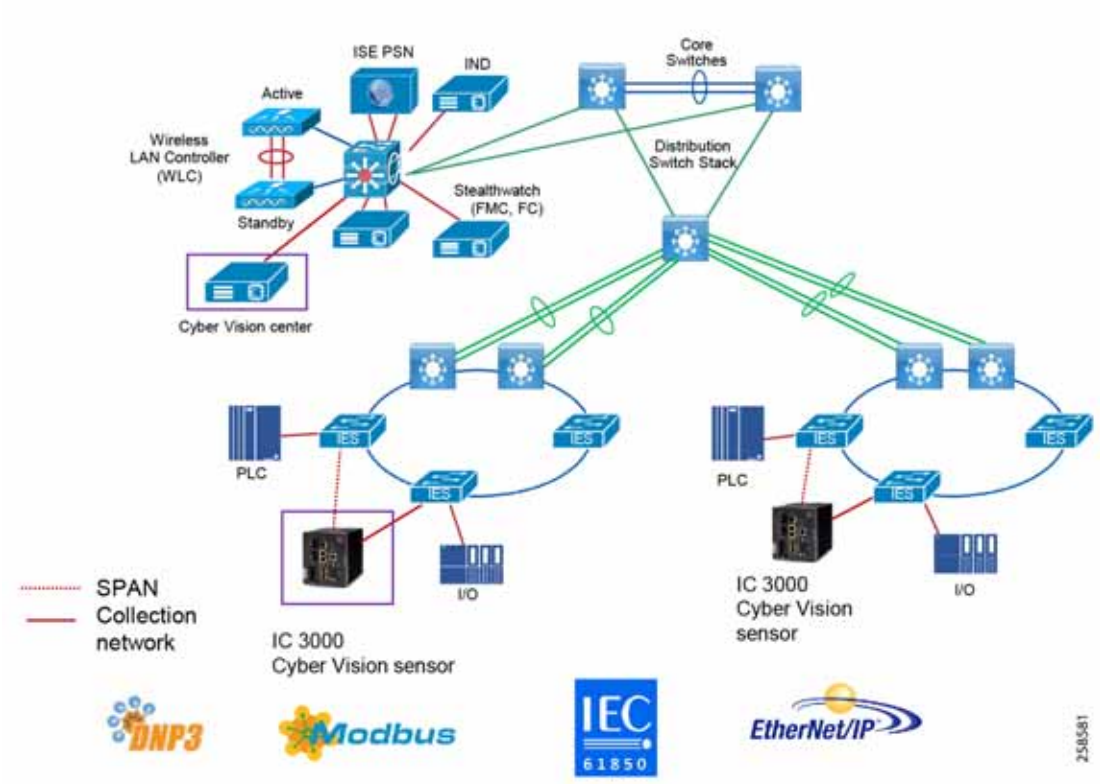
Cyber Vision Online Mode

The Cisco Cyber Vision online mode assumes that there is Layer 3 connectivity between the Cisco Cyber Vision sensor and the Cisco Cyber Vision Center. Online mode is recommended and preferred for the following reasons:

- The online mode ensures that the OT/IT operations teams get a continuous update of the traffic in real time.
- Manual capturing and uploading the data is not required. The data is captured in real-time at the Cisco Cyber Vision Center.

Figure 18 illustrates how the Cisco Cyber Vision solution is deployed in the on-line mode in substation zone.

Figure 18 Cisco Cyber Vision Deployment Model in Online Mode



As shown in Figure 18, Cisco IC 3000 deployed with Cisco Cyber Vision has two distinct set of interfaces: collection interface and mirror interfaces. The collection interface is a Layer 3 interface that is used to transport the metadata to the Cisco Cyber Vision Center. The mirror interfaces collect the SPAN traffic in the network.

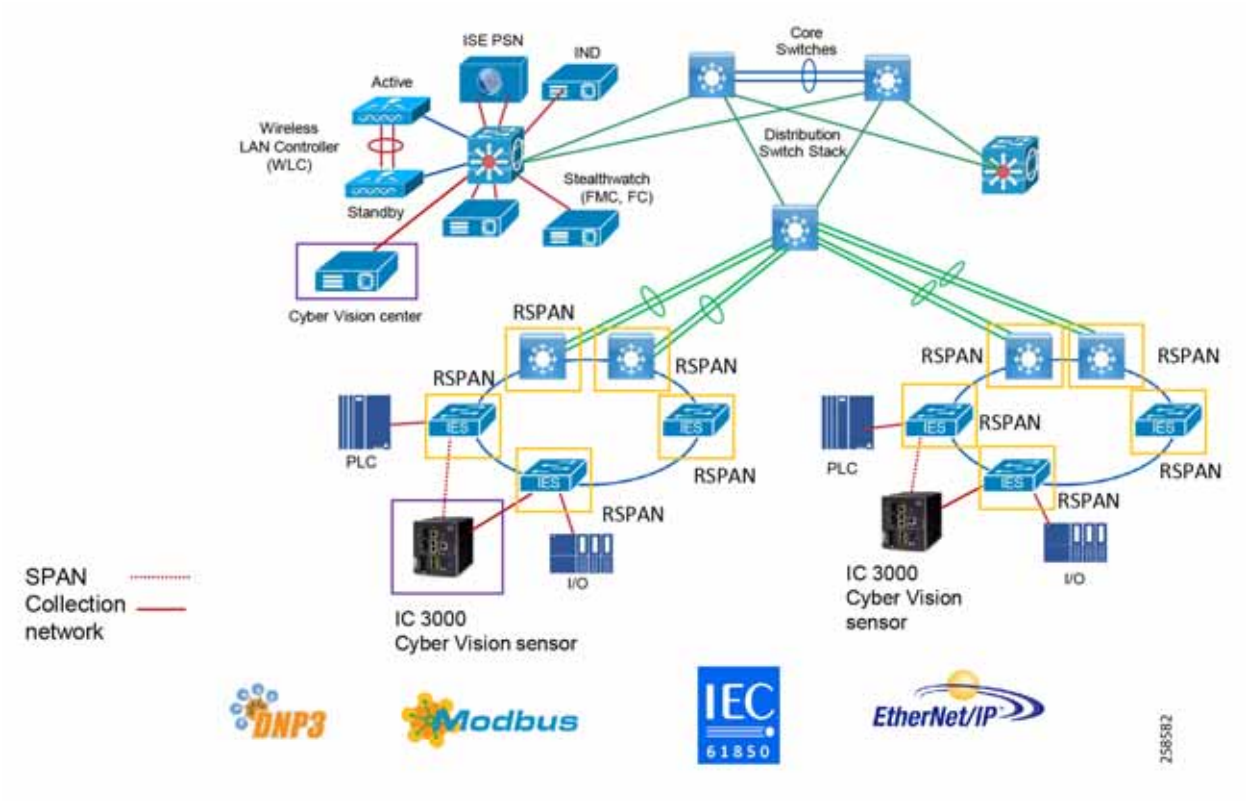
Capture Points

The Cisco Cyber Vision solution success depends on effectively capturing the traffic. Where to capture the traffic is critical. For example, if there are many Cisco ICS devices attached to several switches in the network and it is desirable to monitor the traffic from all those devices, then there are three choices:

- Enable RSPAN on all the switches.
- Enable individual SPAN on each of the switches to be monitored and connect them to a specific switch.
- RSPAN the traffic from the switch to the IC 3000 sensors and selectively monitor the traffic.

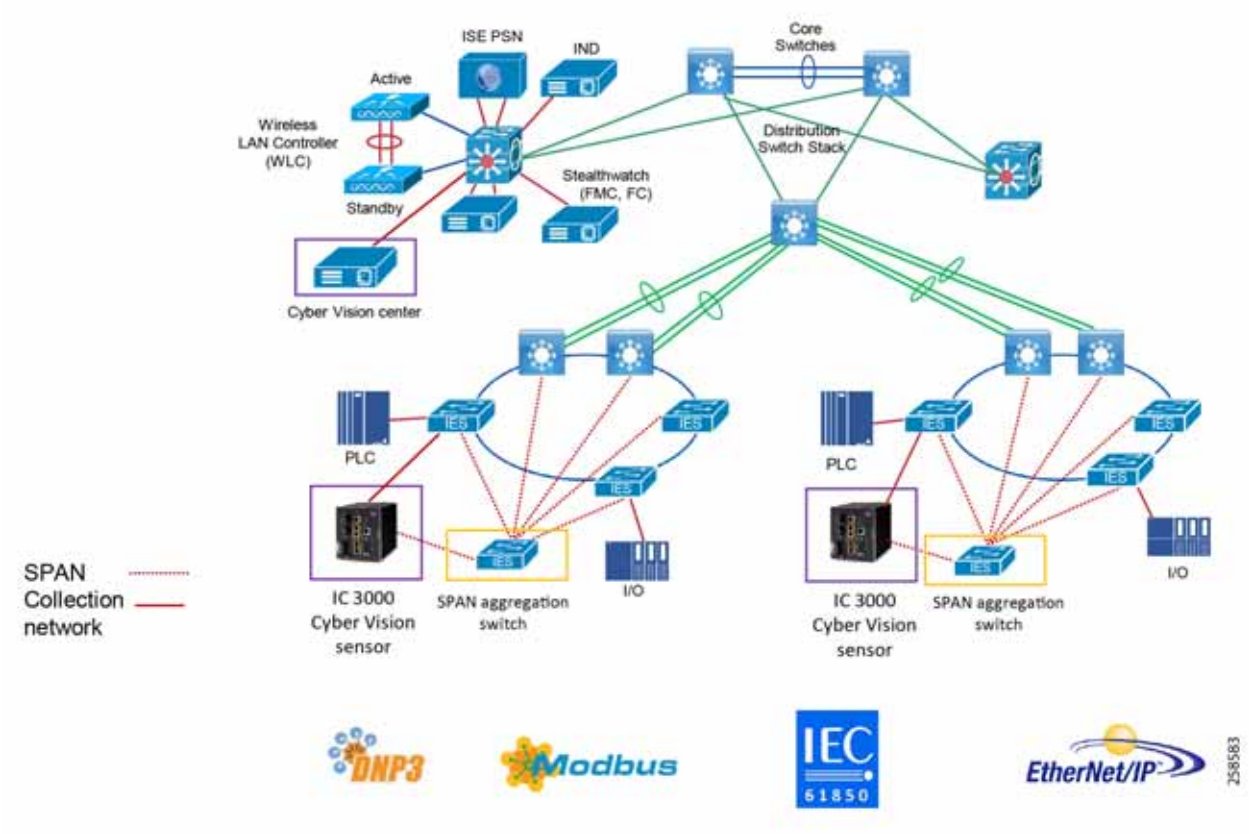
Figure 19 depicts RSPAN enabled on all switches.

Figure 19 Increasing Cisco Cyber Vision Scalability with the RSPAN Feature of Cisco IE Switches



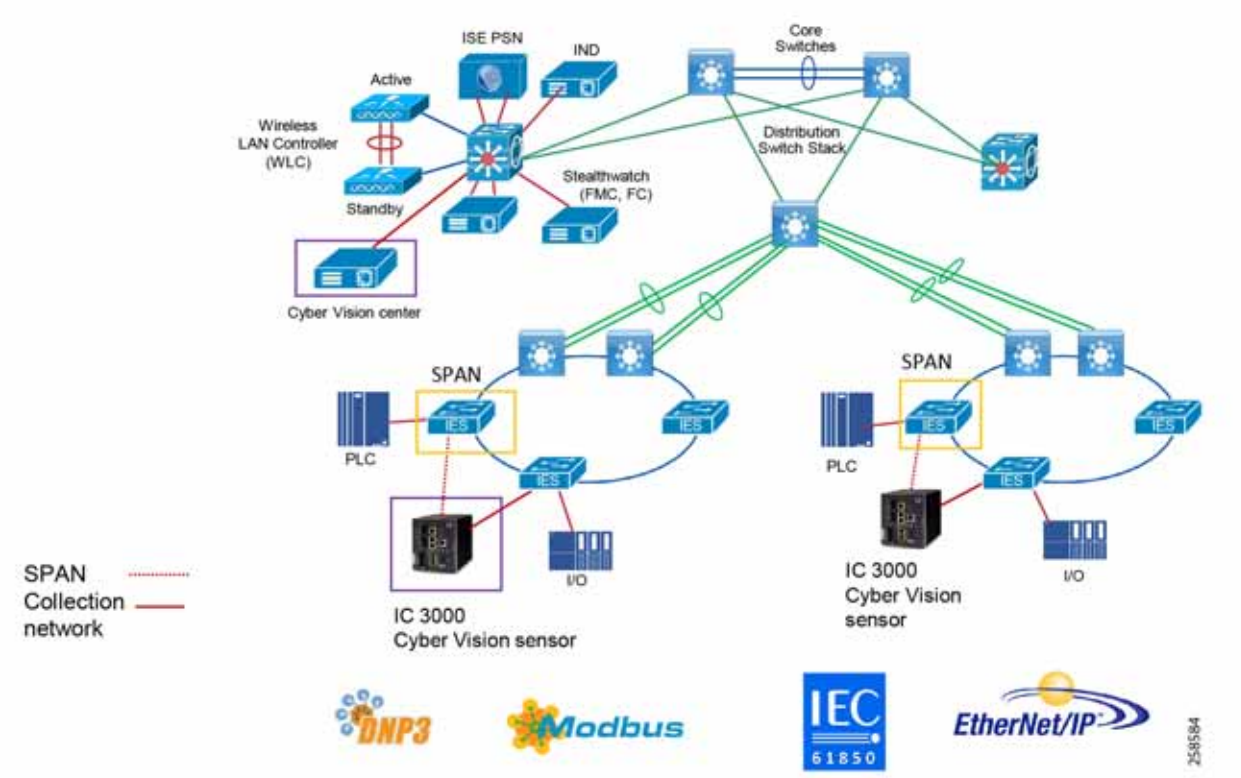
The second option is to aggregate all the SPAN traffic to a SPAN aggregation switch and then direct that traffic to Cisco IC 3000 sensor. See Figure 20.

Figure 20 Increasing Cisco Cyber Vision Scalability with an Aggregation Switch with Local Span and Data Monitoring



The third option is to enable SPAN at selective points. See Figure 21.

Figure 21 Cisco Cyber Vision with Local Span for Data Monitoring and Threat Detection



The third option is recommended for the following reasons:

- The most critical traffic in the substation is the communication between devices in the electronic security perimeter.
- Most security attacks have originated by exploiting the vulnerabilities in the device controllers including the primary substation RTU.

If there is a strong need to monitor all the devices, then the second option is a better choice for deployment.

Topology Considerations

Ring versus Tree/Star

LAN Ring

Lossless Resiliency Protocols – New lossless resiliency protocols and technologies can be considered for deployment across industries with the introduction of Parallel Redundancy Protocol (PRP), High-Availability Seamless Redundancy (HSR), and the HSR/PRP combined box. Industrial automation applications can have very strict availability requirements that must be adhered to and the network resiliency design and network topologies are critical in helping adhere to these requirements. Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 support lossless redundancy protocols HSR and PRP. These aid in keeping the network highly available in supporting the industrial applications within the substation.

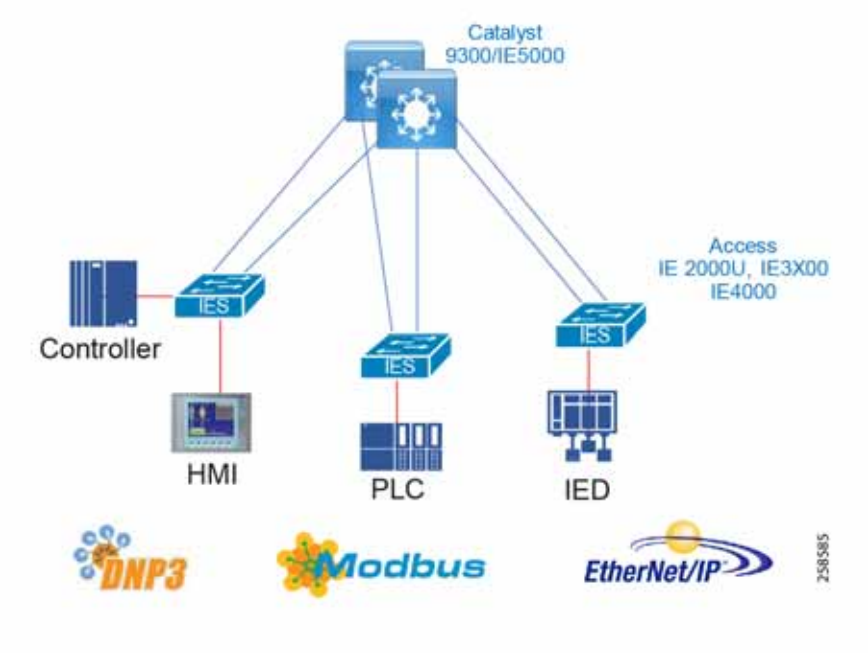
Implementing security in a 61850 operational environment, the network architect must also address multicast requirements, device characteristics, and bandwidth limitations. The above mentioned ring technologies and resiliency protocols become necessary to meet the latency and lossless device and system requirements of 61850, especially within the station bus segment. We are beginning to see the collapse of the station bus and process bus to a single segment of fewer devices. This lends itself to an inherently more secure environment and lessens the burden of the

security architect. It becomes much easier to identify device peers and isolate or micro-segment these devices. It adds a potential point of enforcement and inspection. This micro-segmentation also increases the flexibility for the operations team and increases the overall performance of the multicast end points.

EtherChannel

EtherChannel groups multiple physical Ethernet links into a single logical link between two switches. Traffic traversing the logical link between two switches is load balanced over the physical links. If a physical link fails within the EtherChannel, then the traffic is redistributed across the other available links in the EtherChannel. Although not strictly a resiliency protocol, the EtherChannel can be deployed to provide resiliency when there are multiple links between the same two switches. In industrial automation this is configured as an option for redundant star configurations when connecting between an access switch (for example, Cisco IE 4000) and the distribution switches running StackWise. See Figure 22.

Figure 22 EtherChannel High Availability Model



Cisco Cyber Vision Sensor—Cisco IC3000

It is just as important to define a scalable monitoring network as it is the operational network. The Cisco IC3000 industrial compute platform has 4 Gigabit ethernet ports, each capable of full line rate Gigabit.

With the Cisco Cyber Vision sensor loaded on the Cisco IC3000, its performance has been validated at 12,000 packets per second and with15,000 flows.

Flow-Based Anomaly Detection

This use case describes how an IT security architect can use Cisco Stealthwatch along with NetFlow enabled on Cisco Catalyst 5000 and Cisco Catalyst 9300/9500 acting as distribution switches to monitor the network flows in the substation network. This use case also shows the integration between Cisco Cyber Vision and Cisco Stealthwatch, which helps an IT security architect to understand the context of OT flows occurring in the substation zone. The integration between Cisco Cyber Vision and Cisco Stealthwatch is implemented using the steps described below.

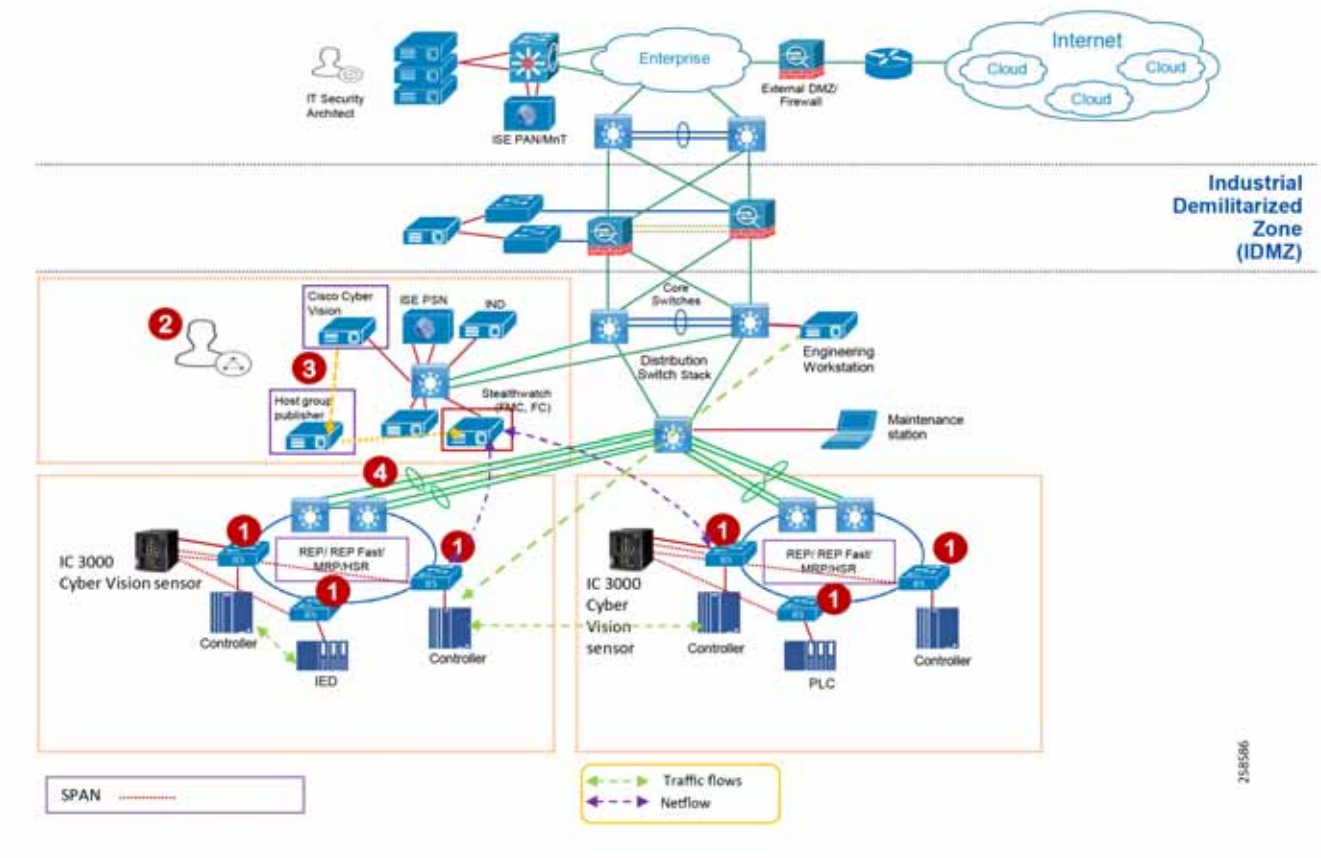
NetFlow is enabled on all substation networking devices to capture the substation traffic flows that are sent to FlowCollector. The Cisco Stealthwatch Management Console (SMC) retrieves the flow data from the FlowCollector and runs pre-built algorithms to display the network flows. It also detects and warns if there is any malicious or abnormal behavior occurring in the network. These three flows are shown to demonstrate the capability of Cisco Stealthwatch using NetFlow:

- Traffic between assets in the zone (intra-substation zone)
- Traffic between assets across the substation zone (East-West or inter-substation zone traffic)
- Traffic between the process bus and station bus assets (North-South traffic)

The IT architect (Figure 23) can complete the following steps to detect the flows:

1. Enable NetFlow on all the Cisco IE switches.
2. Deploy the Cisco Cyber Vision python scripts in a server.
3. Use the python script to connect to the Cisco Cyber Vision Center and download the host group information.
4. Use the python script to connect to the Cisco SMC and publish the host group information.

Figure 23 Gaining Visibility in a Highly Available Network



Security using NetFlow and Cisco Stealthwatch for anomaly detection

This version of Grid Security has design guidance for implementing Cisco Stealthwatch and enabling NetFlow to provide anomaly detection within the substation. Further visibility into the traffic traversing the substation infrastructure can aid with troubleshooting and highlight abnormal behaviors, such as detection of malware that is sprawling across network. With the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000, NetFlow can be enabled on these devices that can provide data flow metrics to Cisco Stealthwatch.

Cisco Stealthwatch takes the flow data from the network and has many inbuilt machine learning algorithms that can assist an IT security professional in detecting possible malware propagation in the network. Cisco Cyber Vision combines protocol analysis, intrusion detection, and behavioral analysis to detect any attack tactic. This holistic approach ensures Cisco Cyber Vision can detect both known and unknown attacks as well as malicious behaviors that could be warning signs of an attack. Cisco Cyber Vision integrates seamlessly with IT SOC so security analysts can trace industrial events in their SIEM for OT/IT correlation and automatically trigger firewall filter rules in the event of an attack.

Network Security

When discussing industrial network security, customers are concerned with how to keep the environment safe and operational. It is recommended to follow an architectural approach to securing the control system and process domain. The Purdue Model of Control Hierarchy, International Society of Automation 95 (ISA95) and IEC 62443, NIST 800-82, and NERC CIP for utility substations are examples of such architectures. Key security requirements in the multiple zones of a substation include device and asset visibility, secure access to the network, segmentation, group-based security policy, and Layer 2 hardening (control plane and data plane) to protect the infrastructure.

- NetFlow export enabled on industrial switches provides network visibility into the traffic within the substation zone. Consuming NetFlow in Cisco Stealthwatch provides anomaly detection to help secure the network. NetFlow is available on the Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches.
- Cisco TrustSec-enabled industrial switches provide scalable segmentation across the industrial automation architecture.
- Network resiliency protocols, such as PRP and HSR, improve availability by providing lossless failover. Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 support PRP and HSR deployments.
- Inserting the Cisco Catalyst 3400 (SDA-capable) and Cisco Catalyst 9300 switches into the architecture provides SDA platform readiness and a potential path to intent-based services.

Switching Platform, Industrial Security Appliance, and Industrial Compute Portfolio for the Substation

An evolution of switching platforms has occurred since previous industrial automation architectures and validated designs like Substation Automation SA1.5 was released. Newer features and hardware capabilities have been added to increase performance, security, and capabilities of the industrial automation architecture. The following highlights some of these capabilities that are extremely relevant in this phase of the architecture and those features with future benefit.

Cisco Cyber Vision Sensor

In this guide, the Cisco IC3000 with Cyber Vision Sensor installed as an application is deployed as a hardware sensor. Cisco IC3000 is an industrial PC capable of having four physical interfaces (int1-in4) in addition to the management Ethernet interface (int0). When Cisco IC3000 is deployed as a hardware sensor, then the management interface is used to transport the information to the Cisco Cyber Vision Center; the four interfaces are used for data collection.

There are two options available to order and deploy Cisco Cyber Vision sensor using Cisco IC3000. First, a customer may have an existing Cisco IC3000 and wants to install sensor as an application in the Cisco IC3000 or a customer orders a new Cisco IC3000 that has the sensor application deployed as an application. Both options are supported, however, the assumption is that in most of the deployments Cisco IC3000 with sensor application software installed will be predominant in the market. The instructions on how to configure a brand new Cisco IC3000 ordered along with Cyber

Vision sensor application is available in the Cisco Cyber Vision Sensor Quickstart Guide: https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Sensor_Quickstart_Guide_Release_3_0_0.pdf

If a customer has an existing Cisco IC3000 and wants to deploy the Cisco Cyber Vision sensor application, then the recommended step is to do a configuration reset of the Cisco IC3000. Refer to the steps mentioned in the section "Installing the Cyber Vision Sensor Application Using Local Manager after a Configuration Reset" in the Cisco Cyber Vision Sensor Quickstart Guide.

Substation Zone Performance and QoS Design

QoS provides classification, prioritization, and preferential forwarding treatment to various traffic flows within the substation zone. Dedicated bandwidth and predictable jitter and latency are required by some ICS applications (real time). QoS can help provide this in the substation zone; ICS real-time traffic flows with the highest performance requirements will be given precedence over all traffic types. This prioritization helps to contribute to network performance, assurance, and predictability which is required to ensure ACS application uptime and efficiency and ultimately contribute to OEE.

Traffic types not involving ICS devices also exist within the substation zone. In reference to the description of traffic flows in the substation zone, Level 3 traffic originating from workstations and servers occurs, such as SNMP and HTTP traffic. An industrial customer may choose to deploy operational support services such as voice or video in the industrial zone on a shared network infrastructure, however this should be evaluated as part of the risk assessment and aligned with a QoS model defined for a converged architecture. In contrast, operational support services can be physically separated from the ICS devices and applications with independent network infrastructures.

Real-time performance and characteristics of the ICS applications should be well understood when designing to provide predictability and consistency in networking performance. As previously stated, the ICS applications and performance are paramount to ensuring uptime, efficiency, and ultimately OEE. A variety of ICS traffic could be deployed within the substation zone which have very different network requirements for latency, jitter, and packet loss. Any unpredictability in the network performance causing too much latency or jitter as well as packet loss could cause ICS system errors or a shutdown of equipment. The following references a defined set of requirements for various types of informational and time-critical I/O traffic classes.

Cisco QoS uses a toolset to provide the priority and preferential treatment for the ICS traffic. The key tools used across the platforms for this version of industrial automation are:

- Classification and marking – Classifying or marking the traffic as it enters the network to establish a trust boundary that is used by subsequent QoS tools, such as scheduling. Class maps and policy maps are the mechanism to provide the network classification.
- Policing and markdown – Policing tools, known as Policers, determine whether packets are conforming to administratively-defined traffic rates and take action accordingly. Such action could include marking, remarking, or dropping a packet.
- Scheduling (queuing and dropping) – Scheduling tools determine how a frame or packet exits a device. Whenever packets enter a device faster than they can exit it, such as with speed mismatches, then a point of congestion or bottleneck can occur. Devices have buffers that allow for scheduling higher priority packets to exit sooner, which is commonly called queueing.

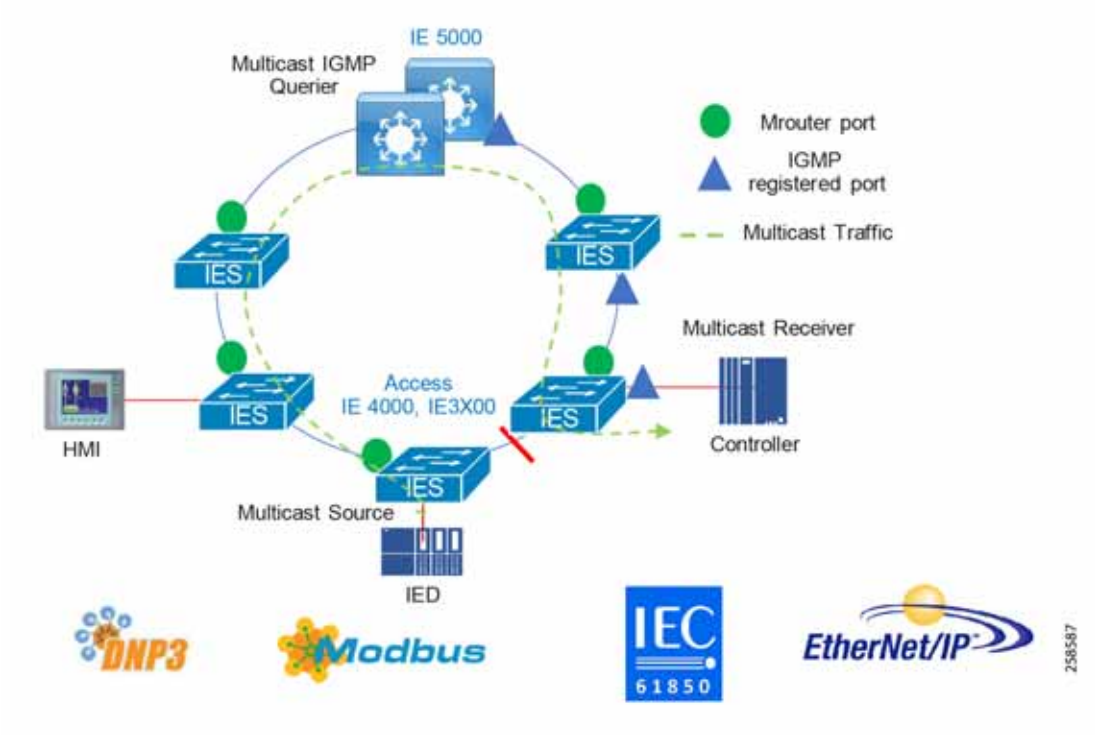
Note: Policing and markdown should **not** be used in the QoS design for control traffic.

Classify and mark all traffic at the access point to the network. Devices that are capable of marking the traffic may be connected to the access switches with trusted ports. Devices not capable of marking their network traffic would need to be classified and marked at the access switch and these network ports would be untrusted. The general guidance is to not trust the CoS/DSCP markings entering the access switch and have the access switch classify and mark all the traffic entering the network. This provides a level of assurance and correct classification at the network edge.

Multicast Management in the ESP

Networking switches within the ESP should facilitate the support of multicast as it is used by some of the ICS protocols. In general, the multicast traffic does not go beyond the ESP. Mechanisms are used in some of the protocols to prevent passing routed boundaries, such as keeping the TTL at 1 within the IP packet. Within the context of a Layer 2 multicast network, Internet Group Management Protocol (IGMP) snooping is used to manage and control the multicast traffic. Figure 24 highlights the components and functions within the zone for supporting ICS traffic deployed with multicast.

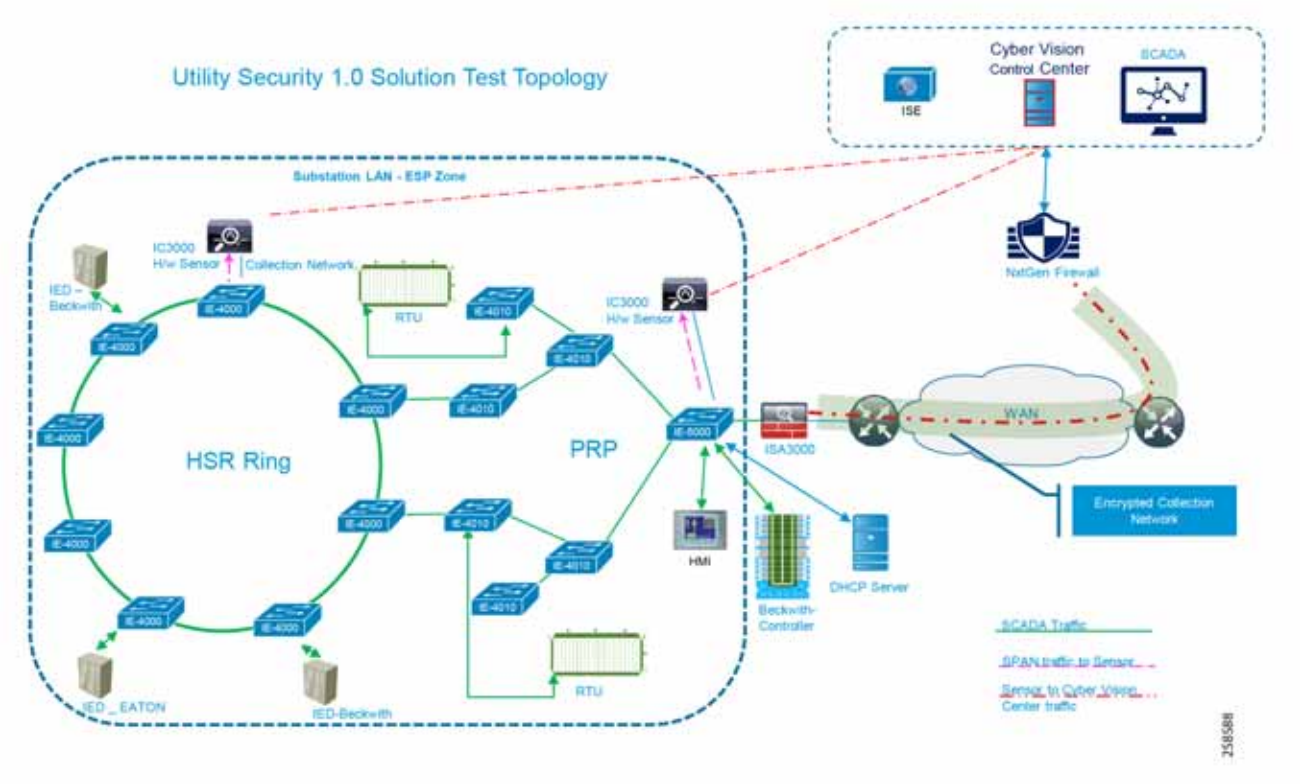
Figure 24 Multicast Support in an Industrial Ring Topology



System Testbed

The architecture proposed in this design guide and the accompanying recommendations and best practices will be thoroughly validated using the system test bed depicted in Figure 25. A detailed test plan highlighting the use cases here and in the solution architecture documents will be validated using this topology and several of those depicted in this document.

Figure 25 Typical Validation Network for Use Case and Performance Testing



Summary

This design guide has described the integration of multiple security platforms to establish a comprehensive defense-in-depth approach to grid security. The design considerations and the detailed validation and configuration information will be in the accompanying implementation guide.

These integrated systems improve operational capabilities and protection for the systems; the integration and centralized management significantly reduce operational costs, time, and threat exposure. This is the benefit of one system versus integrating numerous questionable compatibility points from multiple vendors.

This design guide leverages previous validation efforts and now shows the integration of these as a holistic architecture adding the capabilities of Cisco Cyber Vision.

Cisco Cyber Vision is an asset inventory, network monitoring, and threat intelligence platform specifically designed to secure Industrial Control Systems (ICS). It is embedded into Cisco's range of industrial network equipment to gather real-time information on industrial assets and processes to give visibility into the production infrastructure and enrich security events with industrial context. Cisco Cyber Vision lets IT and OT teams share a common understanding of their industrial networks and operational events. They can work together on network segmentation, threat detection, and remediation to ensure continuity, resilience, and safety of their industrial operations. Fully integrated with the Cisco security portfolio, Cisco Cyber Vision extends the SOC to the OT domain, so that organizations can build and apply security policies to their industrial networks based on operational insights.

Glossary

The following table lists the acronyms and initialisms that may be used in this document.

Term	Definition
A	
ACK	Acknowledgment Frame
AD	Administrative Distance
AF	Assured Forwarding
AMI	Advanced Meter Infrastructure
B	
BGP	Border Gateway Protocol
BMR	Basic Mapping Rules
BR	Border Router
C	
CBC	Capacitor Bank Controller
CCA	Clear Channel Assessment
CDN	Cisco Developer Network
CGM	Connected Grid Module
CGR	Connected Grid Router
CNR	Cisco Network Register
CoAP	Constrained Application Protocol
CSM	Cisco Compute Content Switching Module
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSMP	CoAP Simple Management Protocol
CX	Cisco Customer Experience
D	
DA	Distribution Automation
DAG	Directed Acrylic Graph
DAO	Destination Advertisement Object
DER	Distributed Energy Resources
DHCP	Dynamic Host Configuration Protocol
DIO	DAG Information Object
DIS	DAG Information Solicitation
DMR	Default Mapping Rule
DMS	Distribution Management System
DODAG	Destination Oriented Directed Acrylic Graph
DR	Demand Response
DRU	Dynamic Routing Update
DSCP	Differentiated Services Code Point
E	

EB	Enhanced Beacon
ECC	Elliptic Curve Cryptography
EOC	Energy Operations Center
EST	Enrollment over Secure Transport
ETX	Expected Transmission Count
F	
FAN	Field Area Network
FAR	Field Area Routers
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FLISR	Fault Location, Isolation, and Service Restoration
FMR	Forwarding Mapping Rules
FND	Cisco Field Network Director
G	
GIS	Geographic Information System
H	
HA	High Availability
HER	Headend Router
HSDPA	High-Speed Downlink Packet Access
HSM	Hardware Security Module
HSPA/HSPA+	High-Speed Packet Access
HSUPA	High-Speed Uplink Packet Access
I	
IED	Intelligent Electronic Device
IGP	Interior Gateway Protocol
IID	Interface Identifier
IPS	Intrusion Preventions Systems
IR	Industrial Routers
ISE	Cisco Identity Services Engine
L	
LIR	Local Internet Registry
LLN	Low power and Lossy Networks
LMR	Land Mobile Radios
LoS	Line of Sight
M	
MDM	Meter Data Management
MIMO	Multiple Input/Multiple Output
MOP	Mode of Operations
MPL	Multicast Protocol for Lossy Networks
MQC	modular QoS CLI
MTBF	Equipment Mean Time Between Failures
MTU	Maximum Transmission Unit

N	
NAM	Neighborhood Area Network
NAT-PT	Network Address Translation and Protocol Translation
NPS	Network Policy Service
NS	Neighbor Solicitation
NTP	Network Time Protocol
O	
ODM	Operational Data Model
OF	Objective Function
OFDM	Orthogonal frequency-division multiplexing
OIR	Online Insertion and Removal
OMS	Outage Management System
P	
PAN	Personal Area Network
PER	Packet Error Rate
PKI	Public Key Infrastructure
PMTUD	Path Maximum Transmission Unit Discovery
PnP	plug-and-play
PSDU	Payload Service Data Unit
PSPU	Physical Service Protocol Unit
Q	
QPSK	Quadrature Phase Shift Keying
R	
RA	Registration Authorization
RBAC	Role-Based Access Controls
RFI	Remote Fault Indicator
RIR	Regional Internet Registries
RPL	Request Parameter List
RSSI	Received Signal Strength Level
RTU	Remote Terminal Unit
S	
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SEIM	Security Event and Incident Management
SFD	Start of Frame Delimiter
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSM	Software Security Module

SUDI	Secure Unique Device Identifier
SUN	Smart Utility Networks
T	
TDMA	Time Division Multiple Access
TPS	Tunnel Provisioning Server
V	
VRF	Virtual Routing and Forwarding
W	
WAN	Wide Area Network
Wi-SUN	Wireless Smart Utility Networks
WPAN	Wireless Personal Area Network
Z	
ZTD	Zero Touch Deployment