Industrial Automation in Mining Environments

Executive Summary

Operations in today's mining industry need to be flexible and reactive to commodity price fluctuations and shifting customer demand, while maintaining operational efficiency, product quality, sustainability and most importantly safety of the mine and its personnel. Mining companies are seeking to drive operational and safety improvements into their production systems and assets through convergence and digitization by leveraging new paradigms introduced by the Industrial Internet of Things (IIoT). However, such initiatives require the secure connection of process environments via standard networking technologies to allow mining companies and their key partners access to a rich stream of new data, real-time visibility, optimized production systems and when needed, secure remote access to the systems and assets in the operational environments.

The Cisco® Industrial Automation (IA) Mining solution and relevant product technologies are an essential foundation to securely connect and digitize mining production environments to achieve these significantly improved business operational outcomes. The Cisco solution overcomes top customer barriers to digitization including security concerns, inflexible legacy networks, and complexity. The solution provides a proven and validated blueprint for connecting Industrial Automation and Control Systems (IACS) and production assets, improving industrial security, and improving plant data access and reliable operations. Following this best practice blueprint with Cisco market-leading technologies will help decrease deployment time, risk, complexity, and improve overall security and operating uptime. Figure 1 below highlights key mining telecommunications infrastructure barriers and results of the IA Mining 1.0 solution and how this solution overcomes them.

Figure 1 Why an Industrial Automation – Mining Solution

Trends and Challenges in Mining

The Mining industry faces challenges from many fronts. Constant threat of the commodity price falling below the current production cost at a given location, environmental issues, need for water, power, waste storage, water treatment, regulatory compliance, and site remediation just to name a few.

Operations in today's mining industry need to be flexible and reactive to commodity price fluctuations and shifting customer demand. Digitizing the mine helps provide greater visibility and insights, thus improving decision-making capabilities; helps lower safety risks and operational costs, resulting in increased operational efficiency and productivity.

Safety is paramount in a dangerous, nonstop, 24x7x365 mining production environment. Product grade, quality, worker productivity and overall equipment efficiency (OEE) metrics are key concerns mining companies.

Additionally, Mining is performed in isolated parts of the world, and requires the development of a local ecosystem comprised of infrastructure and services to support the operation. With remote locations, a mining company may be the landlord for housing, an Internet provider, water utility, waste management utility, transporter of people and product, phone company, power provider, with each of these being a necessary component to support the primary mining processes. Operators obtain licenses to mine from governments that impose strict environmental operational requirements, maintain the land lease, and obtain lease extensions for future operations.

The mining process disrupts water tables (reduction, pollution, and redirection), generates dust, impacts flora and fauna, and consumes vast amounts of energy. When transporting the ore from the mine to a processing plant or to a customer location, mines often use railway systems that cross public boundaries and roads. Mine bulk impacts nearby towns (dust, pollutants to marine environments, noise, light). If things go wrong, entire ecosystems can be disrupted – such as tailing dam failures, toxified water tables, land subsistence, and permanently redirected water flows. Ore refineries generate large volumes of unusable material that have to be handled in an environmentally responsible manner. Mines need both social and environmental licenses to operate. They have responsibilities to the communities and geographic areas in which they operate and need to remediate land back to a government in an agreed state at the completion of the mining operations.

The mining sector plays a significant role in global metals, minerals, and energy production supply chains. Mining companies are major employers and contributors to government revenues via royalties and taxes. Smooth, reliable and consistent operations is vital to mining companies, countries and world economies alike. Figure 2 below highlights key objectives and complexities of digitizing mining production environments, from extraction to transportation and all the steps in between.

Figure 2 Mining Customer Objectives and Challenges

Solution Features

This section covers the key benefits of deploying IA for Mining, the key use cases and process stages of mining and identifies how those areas are supported by this or other Cisco Validated solutions.

Benefits of deploying Industrial Automation for Mining

Key benefits of the solution include:

Increased productivity and efficiency, with greater agility to react to production-impacting failures, market trends, industry fluctuations, and shifting demand. Digitizing the mining supply chain from pit-to-port through the adoption of Industry 4.0 and Internet of Things (IoT) sensor connectivity, and leveraging digital technologies to enable critical applications, such as increased automation and remote operations, analytics, machine learning (ML), and artificial intelligence (AI). Enabling these capabilities will allow mine operators to make more informed decisions, improve productivity, and increase efficiency and safety. As an example, adopting remote and autonomous operations, increases productivity with higher asset utilization and reduces risk to personnel, by removing people from dangerous areas. IA Mining is a foundational reference architecture for the plant environment for locations such as Crush/Convey, Concentration, Smelter, Refinery, Port operation, and water treatment.

Managed cyber risk in the Industry 4.0 era, as the fourth industrial revolution is upon us, with the adoption of connecting the unconnected - driving mine digitization by interconnecting the customer and their supply chain from pit-to-port. Because the production output from mining does not vary as much as in the discrete manufacturing world, the emphasis in mining is on integration and optimization of internal supply chains – multiple mines, rail lines, ports, and refineries.

Cybersecurity is a prime concern for mining companies. Mine operation and production cannot risk being affected by cybersecurity breaches. In harsh industries, cyber-attacks could lead to environmental incidents. Security or safety compliance compromises could result in hefty fines, penalties, and potentially a loss of license(s) for a mine to operate.

Equally important in mining is the use of security and secure architectures to protect fragile control equipment from other equipment and to mitigate unintentional impacts -- such as malformed packets, variances in equipment manufacturer protocol implementations, broadcast storms, and network discovery loads, which may cause production failures. Therefore, mining companies are concerned about inadvertent intersystem communications triggering production shutdowns or failures in ever more complex interconnected mining systems. A common issue seen by mining companies is the unintentional outcomes from operator errors and misconfigurations with good intentions in mind. Without a true change control system and ability to control and audit changes operate error can cause catastrophic issues.

Improve the efficiency of high-impact resources such as water usage and energy. This not only assists in the operational efficiency of the mine and cost reductions, it also helps to align the mine with environmental laws and legislations. As the world becomes more environmentally conscious, there is a move for the mining industry to examine and improve environmental impacts. Mines need to adopt measures to improve energy utilization, reduce water consumption, improve water reclamation, reduce their carbon footprint, and become more eco-friendly. Enabling the digital mine, connecting IoT sensors, and leveraging digital technologies for real-time operational visibility and process optimization will assist in realizing these goals. With the ability to converge systems securely and reliably the mines of the future are able to leverage data like never before.

Prioritize safe, healthy, and sustainable operations, with worker and environmental safety as the top priority. In every part in the mining value chain safety is the top priority. The ultimate goal is to achieve zero worker injuries and minimize human error. Autonomous, semi-autonomous, and remote operations are helping achieve this goal today by removing people from high-risk environments. Machine autonomy demands a highly available, deterministic, and secure network infrastructure upon which network-intensive mining systems and applications rely. Slope and seismic activity monitoring allows for production optimization while diminishing safety risk.

Mining Process and Use Cases Overview

The value chain starts with the Exploration/Discovery process. In this phase, a discovery team finds and scopes a body of ore. Team access to geological, drilling and conventional business systems enables better cost reductions, efficiency and improved assay results. Once identified, the rights to extract the ore body is sold to a mining company with oversight from a regulatory body responsible for the region. After a mining company has obtained the right to extract the ore, the planning process of developing a life-of-mine plan is initiated. Interaction between Information Technology (IT) and Operational technology (OT) is paramount. With proper long-term planning, the IT organization, in conjunction with operations, can design a network infrastructure for the physical site with considerations for how the site will be developed, and how the mine will evolve over time.

These general mining processes are shown in Figure 3:

Figure 3 Mining Process and Use Case Overview

Key stages in the mining process are described below.

- Extraction – Mining starts with the removal of “overburden” to expose the ore body. Blasting crews can use explosives to make the rock small enough to fit into the haulage and the crusher. Haulage in most above- and below-ground mines is the movement towards remote and autonomous operations.
- Crushing – make the rocks or ore small enough to go on the conveyor belt and into the rock mill for processing and concentration.
- Beneficiaction/Processing/Concentration – In the mill the ore is broken down to a powder consistency. This powder is mixed with water and chemicals to extract the minerals and then sent to a thickener. This concentrate can then be sent to a smelter to refine further, or sold as a commodity to other companies seeking the concentrate blend.

- Smelting – The concentrate can be sent to the smelter where extreme heat is used to separate the ore from the waste (slag) the slag is then poured off into a dump area where the ore is formed into ingots for further processing in a rod plant or to be sold on the commodities market.
- Refining – is the process of separating the desired ore from the waste this can be achieved with chemical or heat, for example.
- Waste – The part of the rock that is not used is sent to the tailings pond as waste. These tailings ponds, if not properly managed, can become a major environmental risk. Should they fail, they can cause irreversible damage to the environment, severely impact production and the resulting financial penalties can be extremely high if an incident occurs..

In addition to the above, many mining facilities include Utilities, such as potable water production, power generation, and transportation infrastructure. Typically, mine operations are far from general infrastructure and require significant power to run their operations. Therefore, on-site power generation and distribution are key considerations. Additionally, mining product can be moved over long distances depending on where the mine is located and where the market is that the product is being sold. Some common transportation examples are road trucking, train, pipeline, and shipping ports.

At this time, the solution focuses on support for Industrial Automation systems found in the Extraction, Crushing, Processing/Concentration, Smelting and Refinery stages of mining.

This solution does not specifically cover Utilities or Transportation as they are covered in separate Cisco Validated Solutions such as:

- Substation Automation – -https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.html
- Connected Rail – www.cisco.com/go/connectedrail
- Wireless sensor networks in Refining and Waste Management stages of the mining process covered by the Oil & Gas Wireless sensor solution

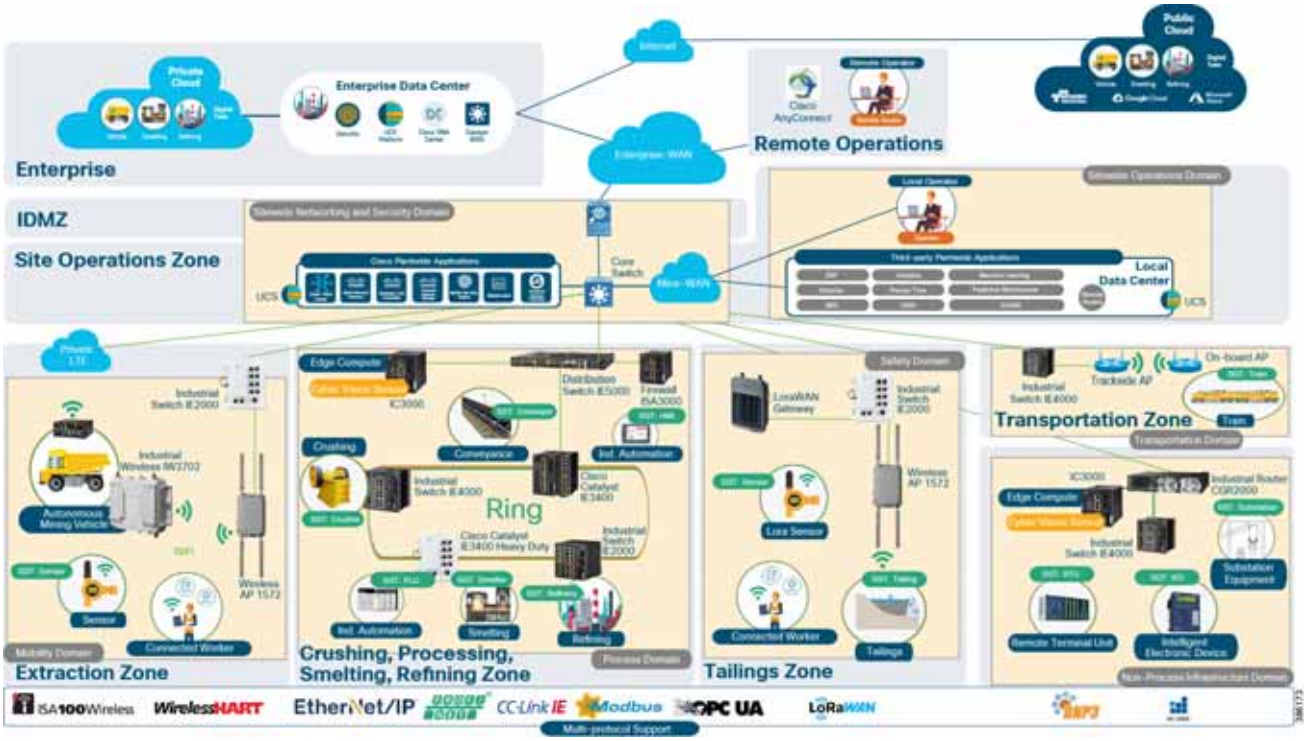
This release of the mining solution does not currently cover the following, but it will be addressed in future releases:

- Wireless deployments for autonomous vehicles, for example during Extraction

Solution overview

Industrial Automation Reference Architecture

Figure 4 Industrial Automation - Mining Reference Architecture



This Cisco Mining Industrial Automation CRD defines a reference architecture shown in Figure 3 above to support multiple operational and non-operational services over a secure, robust communications infrastructure. The architecture applies to the wired portion of industrial areas within the mining value chain, establishing a foundation for network design, security, and data management technologies for process manufacturing environments. The reference architecture in Figure 3 is a blueprint for the security and connectivity building blocks required to deploy and implement digitized process control environments to significantly improve safety and business operation outcomes. The building blocks include:

- Wired process control networks with safety and energy management systems
- Industrial network security throughout the plant including the Industrial DMZ.

The use cases and building blocks described in this guide provide a complete end-to-end view of the reference architecture, although the focus of this guide is on the use cases and architecture enabled through the wired connectivity and security technologies.

Note: The wired network and security architecture is sourced from the Industrial Automation CVD: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html.

The reader may be familiar with the architectural guidance and design principles in that guide, although there are some slight differences between the mining process control environment and the industrial automation design which are highlighted in Industrial Automation Reference Design.

Solution Features

The Mining Industrial Automation solution applies the best IT capabilities and expertise tuned and aligned with OT requirements and applications and delivers for industrial environments:

- High Availability for all key industrial communication and services
- Real-time, deterministic application support with low network latency, packet loss, and jitter for the most challenging applications, such as motion control
- Deployable in a range of industrial environmental conditions with Industrial-grade as well as commercial-off-the-shelf (COTS) IT equipment
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s of IACS devices) deployments
- Intent-based manageability and ease-of-use to facilitate deployment and maintenance especially by OT personnel with limited IT capabilities and knowledge
- Compatible with industrial vendors, including Rockwell Automation, Schneider Electric, Siemens, Mitsubishi Electric, Emerson, Honeywell, Omron, and Schweitzer Engineering Labs (SEL)
- Reliance on open standards to ensure vendor choice and protection from proprietary constraints
- Distribution of Precise Time across the site to support motion applications and Schedule of Events data collection
- Converged network to support communication from sensor to cloud, enabling many Industry 4.0 use cases
- IT-preferred security architecture integrating OT context and applicable and validated for Industrial applications (achieves best practices for both OT and IT environments)
- Deploy IoT application with support for Edge Compute
- OT-focused, continuous cybersecurity monitoring of IACS devices and communications

Mining Solution Overview and Use Cases

Reference Architecture Overview

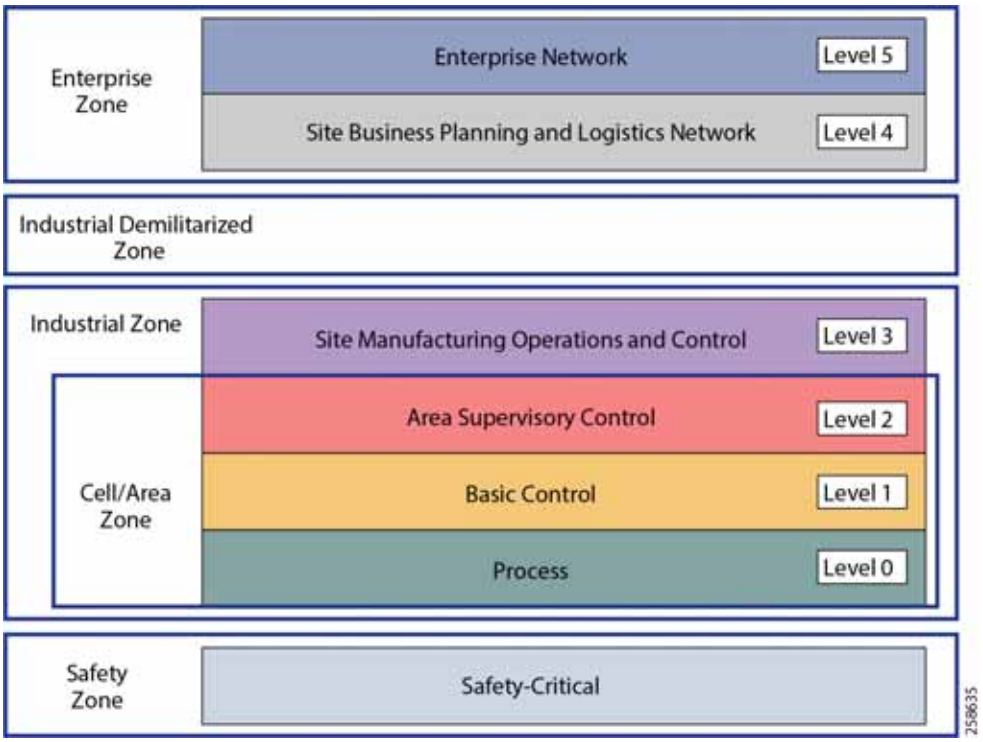
The *Cisco Industrial Automation for Mining Cisco Reference Design (CRD)* defines a reference architecture to support multiple mining process and non-process services over a secure, reliable, robust communications infrastructure. The architecture applies to wired and wireless network designs, security and data management technologies across the mine. The reference architecture provides a blueprint for the essential security and connectivity foundation required to deploy and implement the various building blocks for a mine. The architecture is applicable for both open pit and underground mining operations. This solution is therefore key to digitizing mining use cases to achieve significantly improved safety and business relevant outcomes. The use cases and building blocks are described subsequently to provide a complete end-to-end view of the reference architecture for on-site and remote operations, though the focus of this CRD is on the use cases and architecture provided for the wired plant infrastructure supporting the process plant operations.

Plant Logical Framework

There are fundamental design considerations when looking at supporting the industrial process and operations across all industrial verticals including mining. The Plant Logical Framework (PLF) is well known throughout the industry, where the framework's concepts are continuously referred to within the document.

To outline the security and network systems requirements, this CRD 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.

Figure 5 Purdue Model for Control Hierarchy



The model shown above identifies levels of operations and the subsequent definitions below highlights its function. Greater details into the model can be found in the Industrial Automation CVD here: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.html

Safety Zone

Safety in the process control systems is so important that not only are safety networks isolated from the rest of the process control, they typically have color-coded hardware and are subject to more stringent physical and performance standards. In addition, Personal Protection Equipment (PPE) and physical barriers are required to enhance safety.

Cell Area/Zone

The Cell/Area Zone is a functional area within a plant facility and many plants have multiple Cell/Area Zones. Larger plants might have “Zones” designated for fairly broad processes that have smaller subsets of control within them where the process is broken down into multiple distributed subsets. Zones are typical of a distributed control system as defined earlier.

Level 0 Process

Level 0 consists of a wide variety of sensors and actuators involved in the basic industrial process. These devices perform the basic functions of the Industrial Automation and Control System (IACS) as part of the physical process, such as driving a motor, measuring variables such as temperature and pressure, and setting an output.

Level 1 Basic Control

Level 1 consists of controllers that direct and manipulate the local process, primarily interfacing with the Level 0 devices (for example, I/O, sensors and actuators).

IACS controllers are the intelligence of the industrial control system, making the basic decisions based on feedback from the devices found at Level 0. Controllers act alone or in conjunction with other controllers to manage the devices and thereby the industrial process.

Level 2 Supervisory Control

Level 2 represents the applications and functions associated with the Cell/Area Zone runtime supervision and operation, including DCS, HMI; supervisory control and data acquisition (SCADA) software. Depending on the size of the plant some of these functions may reside at the site level (Level 3). An example could be control room workstations monitoring process sitewide.

Industrial Zone

The Industrial zone comprises the Cell/Area zones (Levels 0 to 2) and site-level (Level 3) activities. 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.

Level 3 Site Operations and Control

Level 3 is where the applications and systems reside that support plant wide control and monitoring. A centralized control room with operator stations monitoring and controlling many systems within the plant would be situated at this level. Level 3 IACS network may communicate with both Level 1 controllers and Level 0 devices, function as a staging area for changes into the Industrial zone, and share data with the enterprise (Levels 4 and 5) systems and applications via the demilitarized zone (DMZ), described later. Examples of services at this level would be site Historians, control applications, network and IACS management software, and network security services. Control applications will vary greatly on the specifics of the plant.

Enterprise Zone

Level 4 Site Business Planning and Logistics

Level 4 is where the functions and systems that need standard access to services provided by the enterprise network reside. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. Although important, these services are not viewed as critical to the IACS and thus the mining operations. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the IACS network. Example of applications may include Internet access, email, non-critical plant systems such as Manufacturing Execution Systems (MES) and access to enterprise applications such as SAP.

Level 5 Enterprise

Level 5 is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services typically reside at this level. The IACS must communicate with the enterprise applications to exchange manufacturing and resource data. Direct access to the IACS is typically not required or recommended.

Industrial DMZ

Although not part of Purdue reference model, the mining solution includes a DMZ between the Industrial and Enterprise zones. New industrial security standards such as ISA-99 (now also known as IEC-62443), NIST 800-82, and Department of Homeland Security INL/EXT-06-11478 include an Industrial DMZ as part of a security strategy. The IDMZ provides a buffer zone and segmentation between the enterprise zone and the industrial/plant zone. Data must be securely passed between the Industrial Zones and the Enterprise.

The IDMZ architecture provides termination points for the Enterprise and the Industrial domain and then has various servers, applications, and security policies to broker and police communications between the two domains and permit remote access services. Downtime in the IACS network can be costly and have a severe impact on revenue; the Industrial zone cannot be impacted by any outside influences, as availability of the IACS assets and processes are paramount. Network access is not permitted directly between the enterprise and the plant; data and services are required to be shared between the Industrial zone and the enterprise. A secure architecture for the industrial DMZ to provide secure traversal of data between the zones is required.

Mine Site Building Blocks and Use Cases

Figure 6 Industrial Automation Mining Architecture

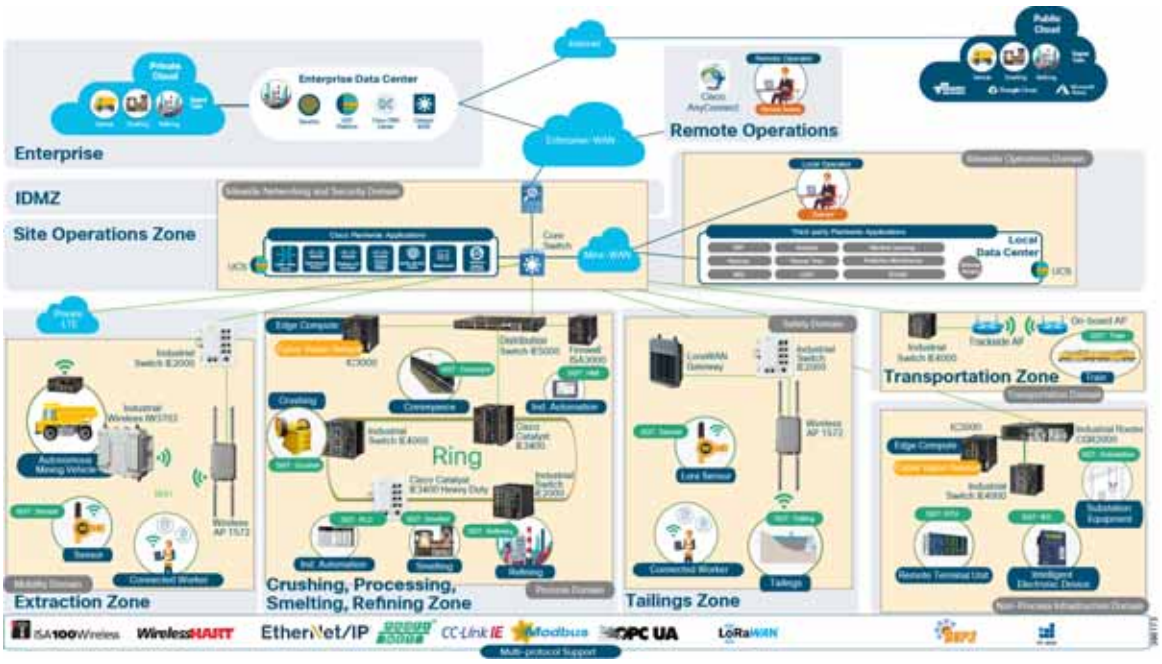


Figure 6, above, highlights OT and IT segmentation, outlines typical mine process areas identifies operational domains to support different control areas in the mining process. An operational domain represents network areas that support key functions of the mine process and are segmented (physically and logically) from each other to avoid outages or breaches to impact other mine processes and areas. These operational domains are based around the attributes and the support needed for the mining use cases in the industrial zone and is supported over a secure robust wired and wireless infrastructure. The different domains are highlighted from a logical perspective rather than a physical perspective. These building blocks within the reference architecture include the following:

- Remote Operations – Supporting remote control and visibility across pit-to-port operations from a centralized location, including use cases such as drill control, digital dispatch for the mining fleet and train control.
- Enterprise Wide Area Network (WAN) – Supporting connectivity to the Remote Operations Center and providing connectivity across the value chain pit-to-port

- Sitewide Networking and Security Services – Includes Enterprise WAN interface via an Industrial DMZ, Mine Core networking, and on-site Data Center support for network and security management,
- Mine-wide Applications – These applications support the mining process and may include Historians, Asset Management systems, SCADA applications, and local operational centers
- Specific on-site Mining operational domains include:
  - Process – Includes fixed wired and wireless infrastructure that supports the industrial automation and controls systems in a variety of Mine process areas (such as Crushing, Smelting, Refining, etc.)
  - Mobility – Supporting the connectivity demands of the mining Fleet for use cases such as autonomous and semi-autonomous operations (Haulage, Dozers and Drills) and local personnel
  - Non-Process Infrastructure (NPI) – Supporting systems and processes not directly related to the process but essential to support the operations within the mine. Examples include Water treatment, and power/electrical management for the mine.
  - Transportation – Supporting transportation control systems often with specific regulatory compliance requirements to be segmented.
  - Safety and Regulatory – This includes use cases that protect the mine, miners and the surrounding environment. Use cases include dam monitoring and dust monitoring.

The operational domains may exist in multiple mine process areas. The following table highlights these use cases and where they apply within the framework of the on-site operations.

Table 1 Mine Site Domains / Operations

	Extraction	Processing	Tailings	Utilities	Transportation
Process		X			
Mobile	X	X	X		
NPI				X	
Transportation					X
Safety & Regulatory			X		

Remote Operations Centers

Remote Operations Centers (ROCs) allow mining companies to centralize their monitoring and controls of mines without having to put people in harms' way at the mines, improving safety. The more functions that can be performed in the ROC increases operational efficiency and effectiveness while improving safety. For example, the adoption of remote control and autonomous equipment operations the ability to have high reliable paths without the chance of human error has dramatically decreased the number of safety incidents involving the mobile fleet and allowed for a smaller number of operators to manage a larger fleet at much lower cost.

Under traditional circumstances, because most mines are in very remote areas, companies need to build housing for the employees working at the mine and also transport them to and from the mine location (fly-in, fly-out). Creating the ROCs in metropolitan areas where the work force lives and can operate the mine, offers huge benefits such as, reduced housing needed on site, easer to attract skilled workforce, reduction in non-productive travel time, superior work-life balance for employees, plus many other benefits. Digital transformation changes many of the perceived negative aspects of placing personnel in the mine, as it is no longer a dirty and dangerous environment. People work from clean, conditioned spaces mining safely and more productively.

Sitewide Services

The OT Sitewide Networking Services can be thought of as the foundational block providing a primary set of functions; interface to the WAN infrastructure, sitewide networking and security services and the IDMZ, which provides segmentation and security between the IT and OT domains. These blocks are essentially components of the fixed wired infrastructure this building block is required to support all of the key mining operational domains. These services align with plant operations and control zone which reside at Level 3 of the Purdue model.

Core Network

The core network is designed to be highly reliable and stable to inter-connect all the elements in the operational plant. It consists of typically Layer 3 devices, with high speed connectivity, redundant links, and redundant hardware interconnecting the operational domains over wide-areas. Within the context of the mine architecture, the core aggregates all of the operational domain zones and provides access to the industrial DMZ, centralized Networking and Security services sitewide applications and enterprise WAN for connectivity for offsite functions such as the ROC. The core applies segmentation techniques to keep the domains separated, typically extending the VPN segmentation from the ROC and WAN into the OT fault domains. Any cross pollination of traffic between the domains must be considered as the core layer provides policy-based connectivity between the functional operational domains.

Wide Area Network

WAN services extend connectivity across the entire Mining value chain from Pit-to-Port, provide connectivity to support communications between the ROC and the OT domains on Site and finally to extend Enterprise support services to many sites. The physical infrastructure is, in most cases, shared physical infrastructure; the WAN needs to support and extend Segmentation between the IT and OT services as well as between OT operational domains. Technologies such as MPLS VPN, SD-WAN and VRF technologies are typically employed to provide these services across the shared WAN.

Sitewide Networking and Security Services

The sitewide networking and security services required across the plant include network and security management platforms such as Cisco Identity Services Engine (ISE), Cisco StealthWatch, and Cisco Cyber Vision Center.

Mine-wide Applications

A host of sitewide applications that are required to manage and operate a mine, including local operation centers, dispatch applications, historians, asset management systems, SCADA applications among many more. These applications rely on the core network to connect the to the various operational domains. The applications also require local data center services such as compute and storage platforms and specific data center networking capabilities to interconnect them.

Industrial DMZ

The **Industrial DMZ** is deployed within the mining environments to separate enterprise and operational domains, and separate operational domains of the production site environment. Typical services deployed in the IDMZ include Remote access servers and Mirrored services. Further details on the design recommendations for the industrial DMZ are included later in this guide.

Mine Operational Domains

This section will outline the key mine operational domains and the mine processes they support and describe the network capabilities.

Mobility Operational Domain

The Mobility operation domain primarily supports the Extraction process. Below is a basic description of the extraction process. Afterwards the specific mobility use cases and their networking requirements are described.

Drilling

After the overburden is removed and stored for use at the end of the life of the mine. The drills are used to create the blasting pattern. Drills create holes which range in size from 8-20 inches (20-50 cm) in diameter and 15-30 feet (4.5-9 meters) deep depending on the material being mined. Using remote operations over a reliable wireless network enables autonomous or semi-autonomous drilling, this shift from traditional drilling saves time, money and improves safety by allowing operators to control the drill outside of the danger zone.

Blasting

Blasting is typically performed with ammonium nitrate and fuel oil using exciter /blasting caps. The process is to use sufficient explosive to make the ore small enough for the haulage. If the rocks are smaller than needed, then blasting materials are wasted. If the rocks are too big for haulage a rock breaker is required -- this too is a waste of resources and time. The use of mobile worker capabilities (enabled with wireless coverage throughout the mine) allow the planning, staging, and digital sign off on work orders to help the blasting team be in the right place at the right time, stay on schedule and helps to keep the site safe during blasting.

Haulage

After blasting, loaders / shovels and haul trucks are used to move the ore body and waste to the proper location either the crusher or the waste pile. The optimization of the haulage is critical for the mine profitability. Digitalization plays a major role in the route planning, road maintenance and equipment utilization.

Mobility Use Cases

Currently, most heavy equipment operations in a mine are performed with an operator located within the mining equipment. Not only is this costly, but it also puts personnel into potentially hazardous situations such as equipment rolls or collisions.

For underground mines, transportation from personnel housing to mine operator staging areas can take over an hour one way. Workers are required to wear special personal protective equipment (PPE), which requires a significant amount of time to maintain and change into. In some underground areas that are extremely dangerous and unstable, such as wet muck underground tunnels, or even in extremely hot or cold mine locations, mine personnel can be directly exposed to dangerous environments for only limited amounts of time. The use of remote operations for mining also gives better visibility to location and health of the equipment, reducing time during shift change and improving the overall usage of the high value assets.

Mining operations are driving toward fully autonomous operational models throughout the supply chain. Removing humans that manually operate equipment will improve productivity, improve product quality, increase worker safety, and help reduce the overall cost of operations. Use cases today involving autonomous vehicles and equipment are either fully automated, without any direct human interaction, or semi-automated, with equipment that is remotely operated and monitored. Remote operations centers can be either located close to the mine site or located completely offsite and far away from the mine.

Digital dispatch

Digital dispatch processes connect mobile fleets to the mine network, thus allowing for proper route calculations and ensuring that operators unload the correct materials in the right spots, properly sending only high-grade ore to the crusher and appropriately delivering overburden to the correct dump. Digital dispatch requires connecting the mine fleet over a wireless network. Having the ability to optimize the haul routes is a huge savings for the mining operators and is the first step in digitizing the mine.

Semi-Autonomous

Semi-autonomous (Remote command) machine operations include loaders in a one-to-one or one-to-many remote operator to machine ratio. One use case is a haul truck operator who can control a loader from inside the cab of the truck to load ore into his truck, thus eliminating the need for an additional operator who would be sitting idle the entire time that the truck is in transit. A ratio of one-to-one or one-to-many allows remote personnel to operate the equipment from a safe location.

Allowing operators to work from a control room located *aboveground* while operating machinery located in a high-risk environment *underground* improves operational efficiency by eliminating some of the travel time, reducing downtime during shift change, improving visibility of equipment location, removing the need for PPE, and most importantly, removing personnel from harm's way. In addition, remote operators can now simultaneously manage more than one machine, thus reducing the number of operators needed.

Autonomous

Likewise, autonomous trucks can haul resources from shovels or front-end loaders in a mine to a crusher area. When fully automated, trucks may continuously operate at optimum performance, thus reducing engine wear and improving tire performance and fuel efficiency. This reduces maintenance costs and downtime and increases productivity.

Reliable network performance is critical to ensure continuous operation of equipment. IT personal strive to minimize packet loss and roaming times to achieve optimal application performance. Any computer network issues, or prolonged roaming times can initiate safety systems that result in the vehicle or equipment stopping, ultimately affecting productivity and production. Cisco's portfolio of industrial and outdoor wired and wireless products plays an integral part in providing a high-performing, highly available, and secured networking infrastructure for supporting autonomous systems in the mine.

Connecting the mine vehicle fleet to the network allows vehicle intelligent monitoring systems (VIMS) to feed a large data engine. Analysis of VIMS data by mine operators enables better equipment monitoring and proactive maintenance. Cisco's solution has helped mining companies improve predictive maintenance, and it has also provided visibility into issues such as problems with engine oil pressure or faulty cooling systems before they escalated. Discovering and addressing these issues before a failure occurs can typically save hours of downtime and costly engine replacements.

The key networking capabilities required to support the mobility domain include:

- Resilient, reliable and mobile wireless networks to connect key assets and personnel
- Wireless backhaul and WAN technologies to interconnect the extraction zones to local sitewide operational services and Remote Operations Centers.

Process Domain

At a high level the Process Domain supports the mining processes to prepare the extracted ore or resource before transportation to external markets. The use cases depending on the type of mine and resources can include conveyance, milling, and smelting.

Conveyance

The mining plant environment and process can span large geographical areas in harsh industrial environments. Conveyance systems can span kilometers across a mine from crushers to process plants. The processing use cases include conveyance, crushing, ore processing, flotation and these areas may deploy a number of different systems to automation and control as well as to ensure safety and reliability.

The transportation of the ore body and overburden in a safe, efficient and environmentally friendly way is a major concern to mining companies. In-pit or underground crushing and conveying plays a major role in this process. By some estimates, transportation of the material can be more than 50% of the total operating cost for the mine.

Using a primary crusher, close to the ore body, with a conveyance system to move the material to separate processing areas, reduces the fuel used in the haulage and also greatly reduces the dust caused by the large haulage trucks. A distributed approach reduces the need for the water track and lowers fuel consumption as well. The waste can also be moved with conveyors to an overburden area where it can be used for reclamation when the mine has ended it active mining time. These conveyor systems can extend for several miles / kilometers and have the capability of moving material at 10-15 miles (16-25 km) per hour. This provides a consistent feed to the process plant, where the ore is extracted, and waste is then transported to the tailings ponds.

The use of mobile conveyors or hoppers, allows for the transportation of the ore body to a leach pad for extraction and creates flexibility to use a stacker with a conveyance system to build out the leach pad with full autonomy. Many mining companies consider In-pit crushing and conveying (IPCC) as a way to reduce the haulage fleet significantly. After the blast is done, a mobile crusher is moved into the area and the mobile conveyors are then joined in a chain to move the ore to the next processing stage. Not only does a IPCC reduce the need for road construction and related maintenance, but is also not effected by weather like haulage can be. Conveyors can operated at a much higher grade, around 30%, as compared to haulage that is limited to grades averaging 10%.

According to the Encyclopedia of Occupational Health and Safety, using steeper grades lowers the need to remove low-grade overburden and may reduce the requirement to build high-cost haulage roads. Connecting the crusher and the conveyance system to monitor vibration, heat corrosion allows mine operators to optimize equipment efficacy and adjust maintenance for equipment as needed.

Milling

Milling is done on the ore body to reduce the size of the rocks to a manageable size if the ore is being sent to the leach pads the rock size is relatively large (up to several inches in diameter). This will then be mixed with a solvent to extract the desired minerals and sent to the stackers via a conveyor system and put into a leach pad. Is flotation is used for extraction the ore bode is milled extremely small like a talcum powder and sent the concentrators.

Leach pads tanks house

The leach pads use solvent and gravity to remove the desired material from the ore body. As the solvent moves through the ore body it dissolves the desired material into the solvent called Pregnant Leach Solution (PLS). The PLS is pumped to the tank house for Electrowinning and the final product called cathodes for sale on the commodities market. The cathodes can also be sent to the smelter to be mixed with concentrate to achieve a level of purity required for customer needs.

Flotation

The flotation process is used to remove the desired minerals from the waste. This is done with the use of several flotation tanks. The desired minerals are sent to the dryers and the finished product is concentrate. This concentrate can be sold on the open market or sent to a smelter for further processing. The waste is sent to a tailings pond as its final destination.

The key networking capabilities required to support the mobility domain include:

- Resilient, reliable wired and wireless networks to connect the industrial automation and control systems

- WAN technologies to interconnect the process zones to local sitewide operational services and Remote Operations Centers.

NPI Operational Domain

The Non-Process Infrastructure (NPI) supports key utilities that are required to be on-site due to the remoteness of the mine, such as power generation and water/waste-water processing.

Power generation

Because of the remote location for most of the mines and the massive amount of power they consume it is not uncommon for mining companies to build and operate their own power generation plants. It is not uncommon for mining companies to build power generation plants and turn them over to the local country to provide power to the communities in which the mine is operating.

Even if power utilities can support the massive demand of a mine on the power distribution system, mines still have extensive power distribution systems inside the mine. Although critical to the mine, utility use cases, reference architectures, design and implementation guidance are found in separate Cisco Validated Designs.

Refer to Utility Substation Automation and Distributed Automation CVDs for more specific reference architectures and validated design and implementation guidance here: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html#~all-industries-guides

Safety and Regulatory Operational Domain

Currently, many mining operations monitor tailing ponds manually. Operations management send personnel to tailing ponds; however, prior approval is typically required for access. Acquiring approval for access can take time, as does the drive to and from the tailing pond, which can take an hour in some facilities. Additionally, supervisors require that personnel check valves and place discharge hoses. Ultimately, a large amount of time is expended prior to the movement of any water or waste product.

Enabling connectivity and visibility into water and waste flow from the process plant to the tailing ponds improves production efficiency, resource utilization, monitoring for safety, and environmental compliance. Being able to monitor valve positions remotely allows operators to proactively identify where waste would be delivered without having to dispatch personnel to visually inspect valve conditions along the lengthy pipes that run between the processing plant and the tailing ponds. This capability will speed up the waste management process and improve safety with the knowledge that waste is being sent to the correct location. Otherwise, waste could cause instability if sent to an incorrect tailing pond and may potentially lead to environmental impact.

Digital permitting / work orders

Tailing dams require seismic and dam wall monitoring. Mobile mine workers want full coverage via remote access to production and corporate systems when working in and around tailing dams.

Dust control is a major concern around mines and at tailing areas, because tailing ponds are made of very small particles of earth. Environmental impact is a major concern, as not only could dust have a negative impact on the environment but it also could result in large fines from the local environmental supervisory agency. By automating dust control sprays and employing distributed air-quality sensors ND video to demonstrate dust control, a mining operation can limit the financial impact from penalties imposed should dust-related issues occur. Other places where automated dust control is needed include ore heaps and shipping ports.

Environmental regulations and safety concerns are a primary focus of mining companies operating globally. All mining companies need to meet or exceed the environmental regulations in the host country they are operating in. Dust management is a major environmental concern for both health and safety issues and regulatory compliance. Dust issues can be broken into two major categories, dust that effects the environment (affecting wildlife, streams, water tables, and so on) and dust that effects works and humans directly, either from breathing it or absorbing it through the skin. The U.S.

Mine Safety and Health Administration (MSHA) considers respirable coal dust to be one of the most serious occupational hazards in the mining industry today. This is not just a coal mining issue. In hard rock mining, on average, the rock in hard rock mining contains 40% silica content, and human exposure to silica dust can cause silicosis, a form of lung disease. Major contributors to dust include but not limited to:

- Haul road maintenance
- Ash piles
- Tailing piles
- Open pits
- Conveyor belts
- Over burdens
- Parking lots
- Blasting
- Backfill process
- Shotcreting
- Crushing
- Drilling and bolting

There are several methods of dealing with dust, but using the network to connect environmental sensors and cameras for real time monitoring is critical for compliance. Also, having records of monitoring can save companies considerably when an incident occurs that is not related to the mining operations.

Slope monitoring

Monitoring the stability of the mine area is critical to operations in the mine. In underground mines, cave-ins are just as dangerous as slope movement in open-pit mines. If the failure mechanisms are properly deployed, understood and monitored in a timely manner, the risk of slope failure can be scientifically reduced. Historically, slope engineers would monitor slope stability would drive to embedded sensors to record measurements on paper, and upon return to the office, would record their findings, compare them to the historical trend of readings and make a decision if there was an issue or not.

This extremely time-consuming process would lead to long intervals in which personal and equipment were and are not protected. With the use of different network technologies, LoRaWAN (900 MHz) Wi-Fi, Cellular, VSAT and PtMP sensors can be connected 24/7 and alert the mine operators when an event is happening, to better understand the stability of the slope and to support decisions to repair the area or evacuate personal and equipment to prevent future damage and injury.

Some of the newer sensors are extremely bandwidth intensive, supporting functions such as ground penetrating radar, GPS sensing for movement and thermal imaging to detect any movement. The images and data are then sent over the network to a monitoring station that can make comparisons and determine the stability of the slope. Key networking capabilities required to support the safety and regulatory domain include:

- Resilient, reliable wireless networks to connect the sensing and condition monitoring applications and support any operational personnel that may be working in these areas
- WAN technologies to interconnect the process zones to local sitewide operational services and Remote Operations Centers.

Transportation Operational Domain

The output of mine processes is a product that must be transported to customers or distributors over long distances. Often mining companies are required to operate rail or port facilities to get their product to market. These transportation functions are generally considered to operate in separate operational domains, both for safety and regulatory as well as operational segmentation reasons.

Although critical to the mine, the use cases, reference architectures, design and Implementation guidance are found in separate Cisco Validated designs.

Refer to Transportation CVDs here:
https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html#~all-industries-guides

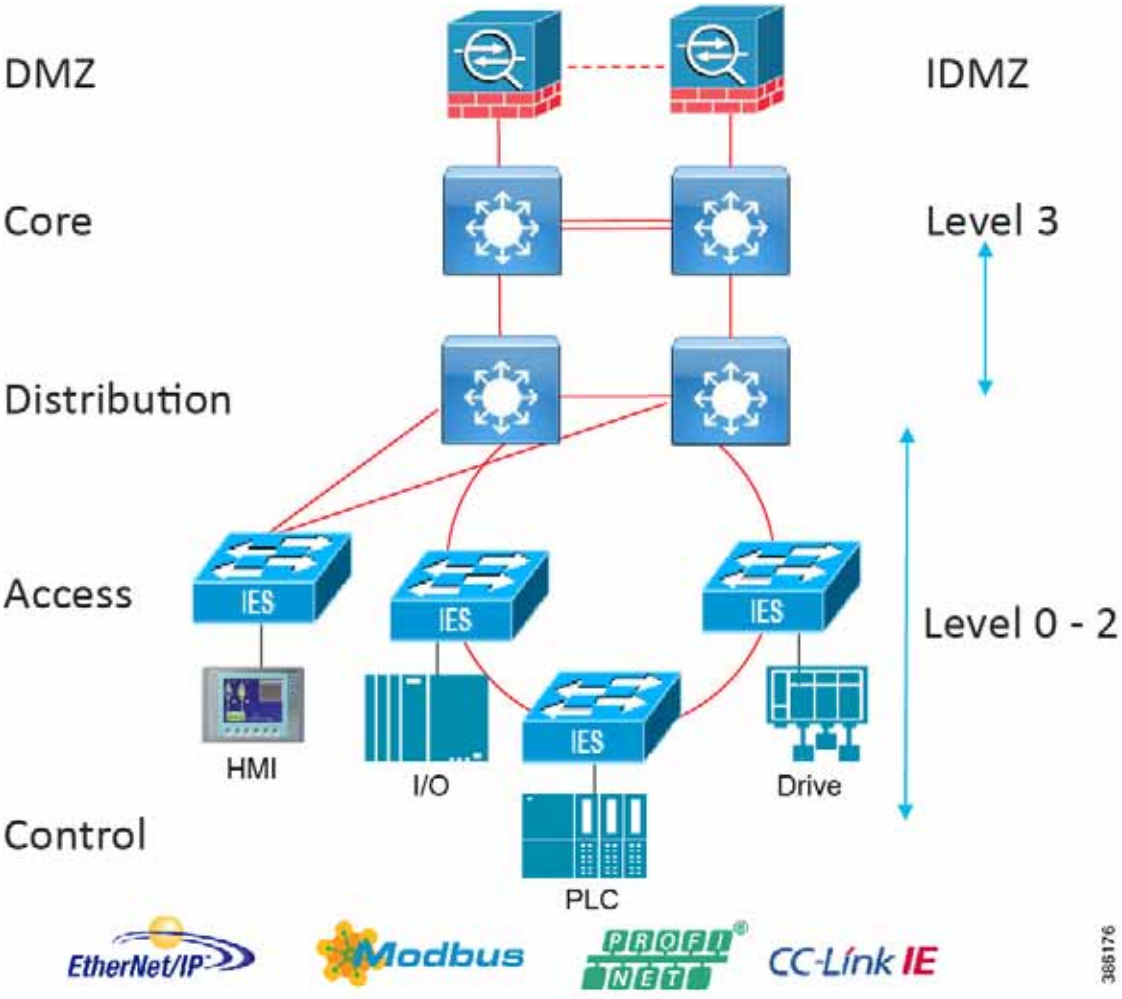
Sitewide Mining Reference Design

The Sitewide Mining Reference Design will at this time primarily focus on the wired network design supporting plantwide operations. The design will accommodate and support other technologies that fit into this model. Examples include IEEE 802.11 WiFi for autonomous haulage and drilling operations, LoRA or WiFi mesh designs for Tailing Dam monitoring, however the specific designs for these use cases are currently outside the scope of this document.

The wired network design supporting process control, and safety networks is very much aligned with the Industrial Automation CVD. The Mine reference wired design is builds on the Industrial Automation CVD as a foundation where any differences will be highlighted in this reference design. This section provides a high-level view of the architecture and identifies differences from the Industrial Automation design as it relates to the mining sitewide operations.

The typical enterprise campus network design is ideal for providing resilient, highly scalable, and secure connectivity for all network assets. The campus model is a proven hierarchal design that consists of three main layers: core, distribution, and access. The DMZ layer is added to provide a security interface outside of the operational plant domain. Figure 7, below, highlights the alignment between the Purdue model and the enterprise campus model.

Figure 7 Purdue and Enterprise Models



Segmentation Strategy Across Mine Site Operations

The mining site as previously discussed has multiple operational domains supporting the process directly such as the wired Process plant and autonomous Haulage, or supporting non-process infrastructure and safety, such as tailings monitoring or water management services. All these operations are critical for supporting the mining operations, and therefore security and segmentation are critical. Segmentation is on a much larger scale than previously detailed within the Industrial Automation Solutions where VLANs, multiple firewalls and a level 3.5 DMZ have been deployed. An approach where the use of Virtual Route and Forwarding (VRF) networking is proposed that can provide the following benefits supporting a scalable and manageable sitewide security segmentation architecture for the mine.

Pros

- Separated routing contexts using VRFs provide partitioning of the networks into logical units and provide major mine network isolation. This fits well with segmenting the operational domains into these operational units such as separate VRFs for the PCN, Mobile Fleet, Non-Process Infrastructure and Safety operations across the mining site.
- VRFs can further be beneficial in providing segmentation of IT and OT when the mine infrastructure needs to support both production and non-production transport.

- Using Layer 3 VRF segmentation reduces the large VLAN based segmentation typically seen in a mine environment. These are difficult to scale, have large broadcast domains and are complex to manage.
- Within the VRFs Multiple VLANS are still deployed at the access control layers but provide more of the networking functions that they were designed for which is restricting Broadcast domains, restricting network sizes etc.
- VRF route leaking can be used to provide any inter VRF communications and help control or restrict communications. This helps restrict potential proliferation of networking or security issues in one operational domain impacting other domains.
- Containment of data traffic.
  - ACLs perform egress filtering: packet traffic already carried within the fabric to destination, or SGACL enforcement point in the path.
  - VRF membership totally contains data traffic to service VRF serving switches only.
  - Security demands – VRF segmentation, with Intrusion Protection/Detection security for all inter-VRF traffic, versus relying on ACL management only to achieve segmentation.
  - Leads to Business function policy management analysis and awareness which can be an introduction or pathway into SDA with Policy Extended nodes.

Cons

- Careful consideration of scoping the number of VRFs to support the mine site operations is required as VRF configuration can be labor intensive. Keeping the number of VRFs to a maximum of 10 is generally recommended.

The architecture will reference VRFs deployed for major segmentation and Scalable Group Tagging will be employed for micro-segmentation both within and across VRFs.

High Level VRF Design concepts for the mine

The following figure highlights the VRF design concepts and functional components.

Figure 8 VRF Design Concepts and Functional Components

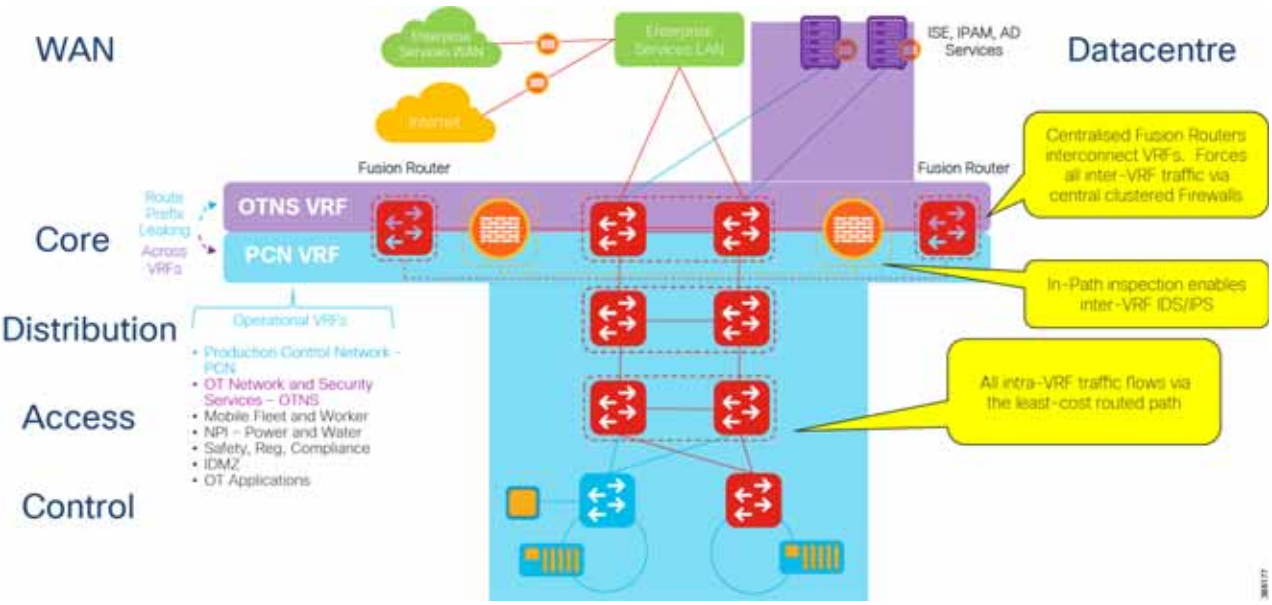


Figure 8 depicts a PCN contained within the segmentation of a VRF and the OT networking Services that would contain security and networking services for the site in its own VRF.

Inter VRF

Any Inter VRF traffic is forced through the centralized Fusion Routers. In this instance traffic flows from the PCN to the OT networking services VRF. Any Inter VRF traffic will flow via the Fusion routers where route leaking is administered between VRFs to control inter VRF traffic flow patterns. If further inspection of traffic is required of traffic flows outside of a VRF domain then a firewall can be deployed at this layer to provide in path inspection of any inter-VRF traffic with IPS/IDS.

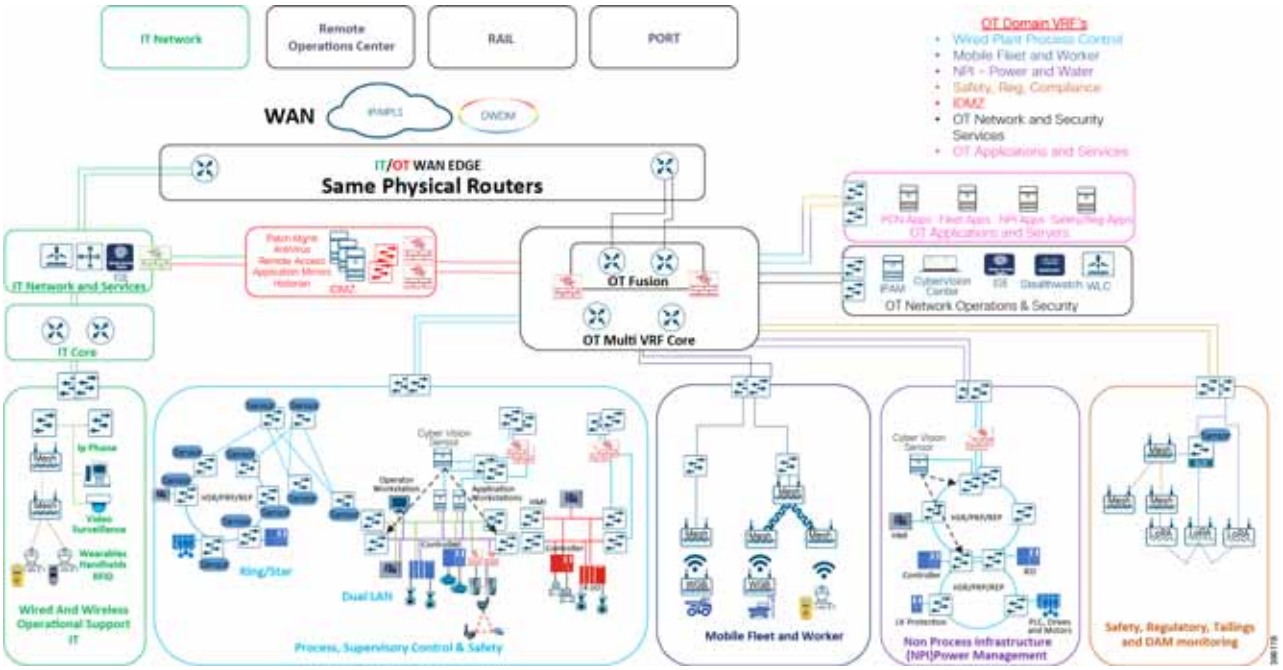
Intra VRF

Within the VRF traditional VLANs will be provisioned to scope and size address space and control broadcast domain sizes. Trustsec and SGT's would be deployed to administer policy within the VRF domain and any traversal of VLANS within a VRF would be routed at the distribution/core layer.

Segmentation VRF Design for the Mine

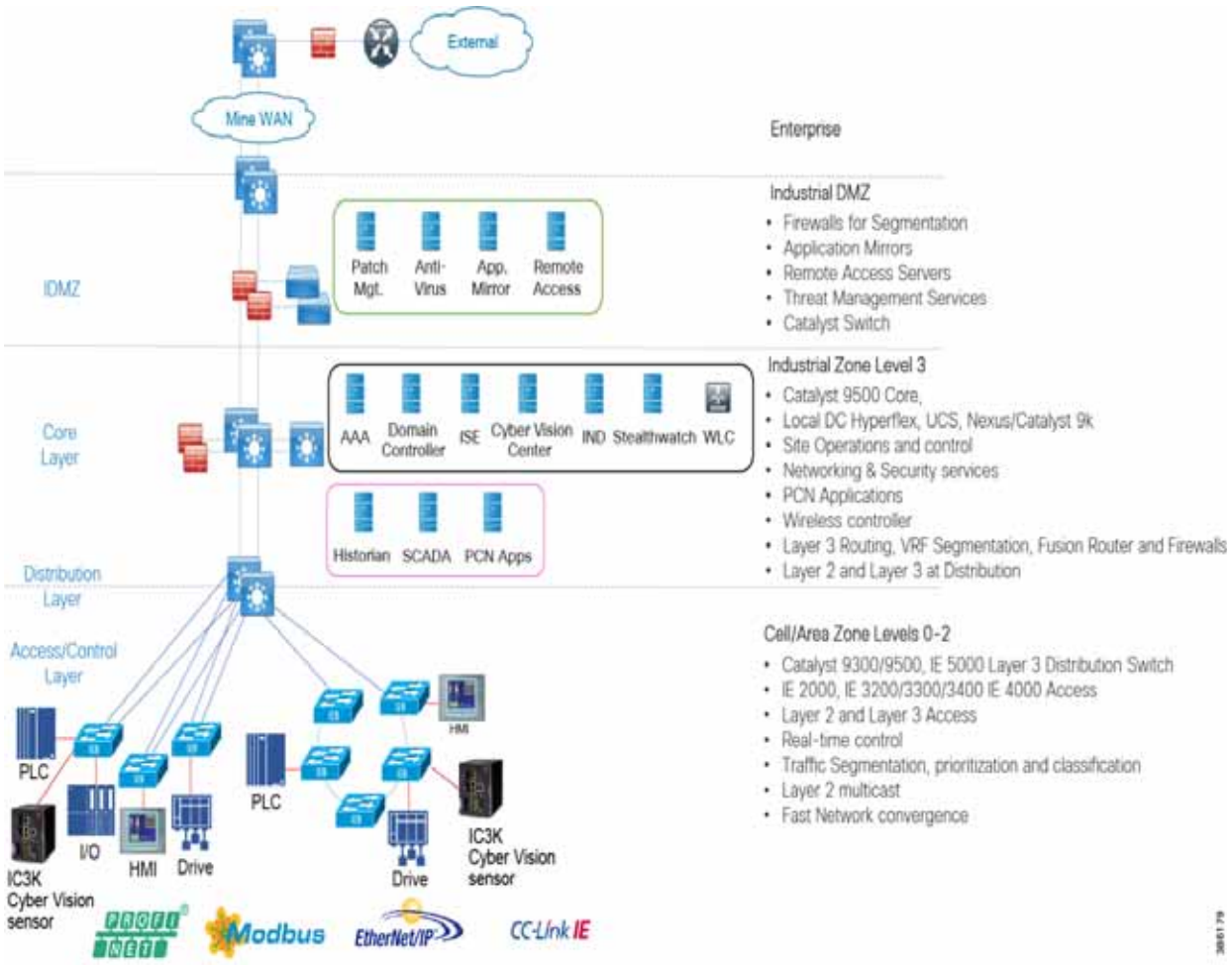
The sitewide figure below depicts the VRF concept across a mining site. The different domains are highlighted from a logical perspective rather than a physical perspective. The same physical distribution and access switches may connect networking and equipment from multiple domains. In smaller mines OT/IT services may be forced to use the same physical network infrastructure. The use of this segmentation architecture fully supports this requirement.

Figure 9 Mine Site Architecture - Logical Domains



Mine Process Control Network Reference Design

Figure 10 Industrial Automation Process Control Network Reference design



Level 3 Mine Sitewide Operations and Control – Level 3

Level 3 aligns closely with the core and sitewide services provided for all operational domains. Most industrial plant facilities are in a different physical environment supporting the wired plant at this layer of the architecture compared to process control Level 2 and below.

The real-time performance networking characteristics are less intense for industrial protocols and the equipment is in an environmentally controlled area, cabinet, or room. The core distribution networking platforms and data center services are deployed at this layer. The industrial Data Center houses plantwide applications such as site historians, asset management, plant systems visualization, monitoring, and reporting services. Network management, sitewide networking, and plant security services are housed in the industrial Data Center, which includes IND, Cyber Vision Center, Cisco ISE, and Cisco StealthWatch. Level 3 provides the networking functions to route traffic between the Process Control Cell/Area Zones and the applications within the Site Operations and Control.

Core/Distribution Layer Cisco Platforms:

- Catalyst 9000 Series switches

- Catalyst management through Cisco DNA Center
- Cisco ISE, Cisco Cyber Vision, Cisco StealthWatch, AMP for endpoints
- Cisco Hyperflex, Cisco UCS Data center and compute platforms
- Cisco Nexus switching in the data center

Process Control Levels 0-2

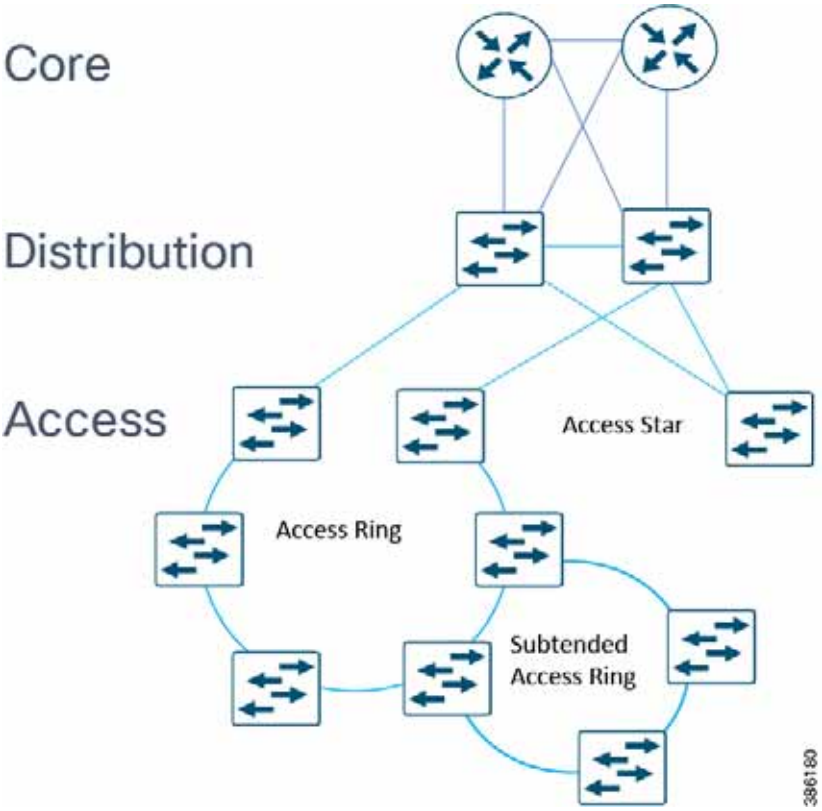
The Process control network is where IACS devices and controllers are executing the real-time control of an industrial process. This network connects sensors, actuators, drives, controllers, and any other IACS devices that engage in real-time I/O communication. It is the major building block within the process control network architecture.

Within the process control levels 0-2, there are key requirements and industrial characteristics that the networking platforms must align with and support. This aligns with the Cell/Area Zone design and recommendations later in this document.

Environmental conditions such as temperature, humidity, and invasive materials require different physical protections than a networking platform. Continuous availability is also critical to ensure the uptime of the industrial process and minimize impact to revenue. Industrial networks differ from IT networks in that they need IACS protocol support to integrate with IACS systems.

In open pit mining, typically the access level switches are connected directly to the distribution switches. In underground mining the access ring switches may be in another ring extended off a traditional ring – a configuration referred to as *Subtended rings*. See Figure 11 below.

Figure 11 Subtended Rings



Recommended Cisco Platforms for the access and process control networks:

- IE 3200, IE 3300, IE 3400, IE 4000, IE 4010 and IE 5000
- Carpeted access with no industrial protocol support Cisco Catalyst 9000 series switches
- Cisco Cyber Vision, Cisco ISE, TrustSec, Cisco StealthWatch
- Industrial Network Director (IND) providing OT network management support.

Distribution Layer Switches

At the distribution layer in the architecture, the wired mining architecture is closely aligned with the Industrial Automation CVD. The distribution layer facilitates connectivity between the access layer and other services. In smaller plants the distribution and core layer can converge onto the same platform (collapsed core), where it may also provide site or plant wide connectivity.

The distribution switches are generally housed in controlled environments such as control rooms so may be more aligned with traditional enterprise switching unless certain industrial protocols are required such as in power networks, then Industrial Ethernet switches may be used at this layer. These switches provide the networking interface at the Level 2 and 3 within the Purdue Model and in smaller plants may be collapsed into the Level 3 function of a collapsed core distribution deployment.

Resiliency is provided by physically redundant components like redundant switches, power supplies, switch stacking, and redundant logical control planes HSRP, VRRP, stateful switchover. Extending segmentation with technologies such as VRF may be required at this layer too to promote segmentation, and fault domain isolation.

Across the mine there are going to be potentially multiple distribution switches due to the geographical dispersity of the process control and access layer switches. Think of Crush through convey back to the process plant. There are multiple process control systems across the mine that would fit into the realms of process control.

Distribution Layer Cisco Platforms

- Catalyst 9000 Series switches
- Industrial Ethernet 5000, 4000, 4010, 3400 Series switches
- Catalyst management through Cisco DNA Center.

The Industrial DMZ

The Industrial Zone (Levels 0-3) contains all IACS network and automation equipment that is critical to controlling and monitoring plant-wide operations. Industrial security standards including IEC-62443 recommend strict separation between the Industrial zone (levels 0-3) and the Enterprise/business domain and above (Levels 4-5). Such segmentation and strict policy helps to provide a secure industrial infrastructure and availability of the Industrial processes. Data is still required to be shared between the two entities such as ERP data and security networking services may be required to be managed and applied throughout the enterprise and industrial zones.

A zone and infrastructure is required between the trusted industrial zone and the untrusted enterprise zone. The IDMZ, commonly referred to as Level 3.5, provides a point of access and control for the access and exchange of data between these two entities.

- The IDMZ architecture provides termination points for the Enterprise and the Industrial domain and then has various servers, applications, and security policies to broker and police communications between the two domains. Key functions of the IDMZ include:
- Best practices of no direct communications between the Enterprise and the Industrial Zone. There will be application mirror, replication or proxy services providing a non direct controlled data path. However in some instances where there is not a replication service that can proxy applications between the Industrial Zone and the Enterprise zone a direct path with appropriate firewall rules may be deployed. ISE design is an example. See the CPWE IDMZ design CVD.
- An IDMZ providing secure communications between the Enterprise and the Industrial Zone using mirrored/replicated servers, “jump-hosts” and applications located within the IDMZ
- An IDMZ securing remote access service flows from the external networks into the Industrial Zone
- An IDMZ providing a security barrier to prevent unauthorized communications into the Industrial Zone and, therefore create security policies to explicitly allow authorized communications (ISE between Enterprise and Industrial Zone)
- No IACS traffic passing directly through the IDMZ (Controller, I/O traffic).

The IDMZ design for Process Control is aligned with Industrial Automation. The design guidance is detailed in the Industrial DMZ reference chapter and detailed implementation can be found in the Converged Plantwide Ethernet CVD at: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

IDMZ Cisco Platforms include:

- Cisco ASA and Cisco Firepower Firewalls
- Catalyst 9000 Series switches
- Cisco Hyperflex, Cisco UCS and data center platforms.
- Nexus switching in the data center

Mine Process Plant Network Design

The Industrial Automation (IA) Cisco Validated Design is a cross industry reference architecture that also addresses the requirements for mining operations within the PCN. It has validated key Networking and Security functionality that is utilized within mines today. This Chapter will highlight the IA validated design concepts that apply to the mining environment. The key IA design section relevant to mining operations is the Cell Area Zone. Further releases of this Mining CRD will target other areas of the Mine Reference architecture the Core Distribution and Fusion router design aligned with the overall site operations detailed in Mine Process Control Network Reference Design.

Industrial Networking and Security Design for the Cell/Area Zone

The Industrial zone contains the Site Operations (Level 3) and the Cell/Area Zone (Levels 0-2). The Cell/Area Zone comprises the systems, devices, controllers, and applications to keep the mining process control networks running. It is extremely important to preserve smooth mining operations, therefore security, segmentation, and availability best practices are key components of the design. There are some key Industrial characteristics of a mine and its operations that will drive certain products and design concepts. As with all designs there needs to be a balance between network, security and product feature parity with overall mine requirements in creating the best fit for purpose design.

At a high level, key deliverables in this guide include providing Cell/Area Zone network and security design and laying the foundation for mining IACS applications that will reside on this framework. The validation focuses on the Cell/Area Zone networks in these mines with resiliency protocol support, quality of service, and network management. The design also introduces market-leading industrial cybersecurity with IACS device and communication visibility with Cisco Cyber Vision, micro-segmentation in the Cell-Area zone and anomaly detection. The relies upon Cisco Industrial Ethernet switches portfolio, Industrial firewall, Enterprise-class core and distribution switches and a set of network and security management software. Key functions include:

- **SDA-Ready Platforms**—Introduction and validation of the Cisco Catalyst 9300 and 9500 switches as the core and distribution switches. The Cisco Catalyst 9300 and 9500 platforms support SDA today. SDA is the industry's first intent-based networking solution for the enterprise built on the principles of the Cisco Digital Network Architecture (DNA). SDA provides automated configuration and end-to-end segmentation to separate user, device, and application traffic without redesigning the network. SDA automates user access policy so organizations can make sure the right policies are established for any user or device with any application across the network. Ease of management and intent-driven networking with policy will be valuable additions for the industrial plant environments. Cisco is leveraging SDA in our Cisco IoT Extended Enterprise solutions for non-carpeted spaces where IT manages portions of industrial plants, warehouses, parking lots, roadways/intersections, etc. Refer to www.cisco.com/go/iotcvd.

  However, **SDA is not yet validated for deployment to support industrial automation and control (the control loop) applications in the Cell/Area Zone in this solution**. The new IE platforms are being positioned in the architecture to prepare for when SDA is able to support Cell/Area Zone industrial automation and control application requirements and protocols. The architecture is promoting SDA switch ready.

- **Next Generation Industrial Ethernet Switching**—The Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 are Cisco next generation Industrial Ethernet switches. These switches are inserted into the Cell/Area Zone for Industrial Automation. The IE3400 provides industry-leading security functions, resiliency and edge computing support. As part of the SDA readiness the Cisco IE 3400 switch will be the industrial Ethernet switching platform that will support the SDA Fabric edge switch functionality. The Cisco IE 3400 and Cisco Catalyst 9300 switches will provide a foundation to move towards SDA in the wired infrastructure. This will provide a platform to enable SDA features as they become available. Today these platforms will be deployed as non-SDA enabled switches, performing traditional network switching functions.

- **Lossless Resiliency Protocols**—New lossless resiliency protocols and technologies that 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 Industrial Ethernet platforms 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 Cell/Area Zone.

- **Network Visibility and OT Management**—Visibility and identification of IACS devices, assets, and communication in Cell/Area Zone(s) with Cisco Cyber Vision and the Cisco Industrial Network Director (IND). Cisco Cyber Vision gives OT teams and network managers full visibility of their assets and application flows so they can implement security best practices, drive network segmentation projects, and reduce security risks. Cisco Cyber Vision automatically uncovers the smallest details of the production infrastructure: vendor references, firmware and hardware versions, serial numbers, PLC rack slot configuration, and so on. It identifies asset relationships, communication patterns, changes to variables, and more. This detailed information is shown in various maps, tables, and reports that maintain a complete inventory of industrial assets, their relationships, their vulnerabilities, and the programs they run, providing operations-centric network management for industrial Ethernet networks.

  The system supports industrial automation protocols such as ODVA, Inc. Common Industrial Protocol (CIP), PROFINET, OPC-UA, Modbus, BACnet, and so on to discover automation devices such as PLC, IO, HMI, and drives and delivers an integrated topology map of automation and networking assets to provide a common framework for plant OT and IT personnel to manage and maintain the industrial network. This information can be presented to Cisco StealthWatch to provide context to assets and help with attribution for security monitoring

- **Cisco Cyber Vision**—Gives OT engineers real-time insight on 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 everything and so serves as a kind of "flight recorder" of the industrial infrastructure.

  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 (Security Operation Centers) so security analysts can trace industrial events in their SIEM for OT and IT correlation and automatically trigger firewall filter rules in the event of an attack.

- **TrustSec and Enhanced Segmentation**—A key component for security implementations and detailed in IEC 62443-3-3 is segmentation of assets into group-based policies. What assets and users need to communicate within a Cell/Area Zone and external to the Cell/Area Zone across an industrial plant needs to be defined. Cisco Cyber Vision provides the visibility of the connected assets to Cisco ISE. Cisco ISE creates and administers the policy defined by the security and OT teams across a Cisco infrastructure. This guide includes recommendations and validation for assets discovery, policy definition, and TrustSec application across a Cisco-managed infrastructure for an industrial plant which can be deployed across industries.

- **Security using NetFlow and StealthWatch for Anomaly Detection**—This guide includes design recommendations for implementing StealthWatch and enabling NetFlow to provide anomaly detection within the Industrial zone of a plant for multiple industries. Further visibility into the traffic traversing the plant infrastructure can aid with troubleshooting and highlight abnormal behaviors such as detection of malware that is sprawling across a plant. With the Cisco IE 3400, Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 switches, NetFlow can be enabled to provide data flow metrics to StealthWatch. 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.

Industrial Characteristics and Design Considerations

The Cell/Area Zone is an access network, but has very different requirements than a traditional IT access layer network. There are key requirements and industrial characteristics that the networking platforms must align with and support across the mining process control network.

Environmental conditions such as temperature, humidity, and invasive materials require different physical attributes from a networking platform. In addition, continuous availability is critical to ensure the uptime of the industrial process to minimize impact to revenue. The design supports secure convergence with Enterprise networks, but was fine-tuned to prioritize IACS traffic. Finally, industrial networks also differ from IT in that they need IACS protocol support to integrate with IACS systems.

The following highlights the key design considerations for the Cell/Area Zone for mining operations, which will directly impact the platform selection, network topology, security implementation, and overall design:

- **Industrial Characteristics**—Environmental conditions, plant layout, and cabling costs all impact the platform choices and network topology in the design. Industrial plants and processing facilities across the mine generally require physically hardened platforms in the Cell/Area Zone. Mines are subject to harsh physical conditions that an IT networking platform cannot withstand. Hardened platforms are equipped for extended temperature ranges, shock and vibration, and invasive materials closer to the process and operation.
- **Interoperability and Interconnectivity**—Within the Industrial Zone, Ethernet provides the best technology to interconnect IACS devices and protocols. IACS vendors are adopting the OSI model with Ethernet as the standard to provide communication for a mixture of IACS devices, controllers, and management servers over the network. However, the network must be engineered to support the IACS implementations with an emphasis on real-time communications, availability, and segmentation.
- **Real-Time Communications, Determinism, and Performance**—Packet delay and jitter within an IACS network can have significant impact to the underlying industrial process. Depending on the industrial application, a delay or variance and lack of determinism in the network can shut down an industrial process and impact its overall efficiency. Achieving predictable, reliable packet delivery is a fundamental requirement for a successful network design in the Cell/Area Zone. A design will need to factor the number of network hops, bandwidth requirements, and network QoS and prioritization to provide a greater degree of determinism and performance for the real-time applications and functions.
- **Availability**—Availability of the critical IACS communications is a key factor that contributes to the productivity and bottom line of the mine. Quite simply the less downtime the greater raw product can me mined and processed. Network topologies, geographic diversity and resiliency design choices, such as QoS and segmentation, are critical in helping maintain availability of IACS applications, reducing the impact of a failure or security breach.
- **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 Cell/Area Zone include device and IACS 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.
- **Management**—Mine infrastructures are becoming more advanced and connected than ever before. Within the mines at the cell area level, there are two personas and skillsets taking on responsibility of the network infrastructure, namely IT and OT staff. OT teams require an easy-to-use, lightweight, and intelligent platform that presents network information in the context of automation equipment. Key functions at this layer will include plug-and-play, easy switch replacement, and ease of use to maintain the network infrastructure.
- **Traffic types**—The IACS traffic within the Cell/Area Zone is predominantly local and stays within the same Layer 2 domain. Cyclical I/O data communicated on very short intervals (milliseconds) from devices to controllers and workstations or HMIs occurs all on the same LAN or VLAN. Layer 2 multicast is also used in IACS networks. Traffic may go across the distribution layer interlocking PLCs for example in a mine this could be part of connecting multiple conveyors.

Cell/Area Zone Components

Cisco has an extensive range of Industrial Ethernet switches. Within the Cell/Area Zone at the access layer, environmental conditions as described earlier are usually a key factor in selecting a hardened, DIN-mountable access switch, such as a Cisco IE 3400, Cisco IE 4000. The Layer 3 distribution switch may have less stringent requirements, allowing for models

such as the Cisco Catalyst 9300 and 9500 if distribution switch is located in a controlled environment. If industrial protocols are still required or there are harsh environmental conditions then the Cisco IE 5000 or Cisco IE 4010 could be deployed for non-conditioned aggregation such as underground mines.

Figure 12 Cell/Area Zone Components: Pure Layer 2 Access and Validated TrustSec Design

Switching Platform, Industrial Security Appliance, and Industrial Compute Portfolio for the Cell/Area Zone

The following highlights some of the capabilities from Industrial Automation that are relevant in this version of the CRD for Mining for the Cell Area Zone.

Table 2 details an extensive industrial switching portfolio for industrial automation plant environments. Multiple platforms are available to accommodate various feature requirements. Cisco IND is the management platform to support the industrial switches in the industrial plant environments.

Table 2 Industrial Switching Portfolio for Industrial Automation

	Cisco IE 2000 access	Cisco IE 4000 access/dis-tribution	Cisco IE 4010 access/dis-tribution	Cisco IE 5000 access/dis-tribution	Cisco IE 3200 access	Cisco IE 3300 access/dis-tribution	Cisco IE 3400 access/ distribution	Cisco Catalyst 9300
19 inch	No	No	Yes	Yes	No	No	No	Yes
Din-Rail	Yes	Yes	No	No	Yes	Yes	Yes	No
TrustSec	No	Yes	Yes	Yes	N/A	N/A	Yes	Yes
dot1X	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
QoS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NetFlow	No	Yes	Yes	Yes	No	HW Ready	Yes	Yes
REP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HSR (-SAN & -PRP)	No	Yes	Yes	Yes	No	No	HW Ready	No
PRP (Red box)	No	Yes	Yes	Yes	No	No	HW Ready	No
PROFINET	Yes	Yes	Yes	Yes	HW Ready	HW Ready	Yes	No
MRP	Yes	Yes	Yes	Yes	HW Ready	HW Ready	Yes	No
IND support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SDA Extended Node	No	Yes	No	Yes	No	HW Ready	Yes	Yes
SDA fabric edge node	No	No	No	No	No	No	Yes	Yes
Cisco DNA support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: Table 2 shows the software features and capabilities supported at the time of this CRD release. Refer to the product data sheet for the latest feature support:

https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html

Cell/Area Zone IP Addressing

IP addresses are assigned statically or via a DHCP service. Manual DIP switches or dials for addressing IACS devices are still deployed and static addressing is still a common requirement and practice in the cell/zone. Assigning IP addresses to IACS devices using DHCP allows for easier automated IP address management however there may still be a requirement for a particular controller to have the same IP address. DHCP persistence is recommended to be enabled. It allows the same IP address to be provisioned so that upon replacement of an asset, the same IP address is provisioned. In the static nature of IACS this helps with ease of use and replacement

Cell/Area Zone Traffic Patterns and Considerations

Within the IACS networks, there are two traffic types—real-time traffic flows and non-real-time traffic flows:

- Real-time traffic flows are typically between IACS devices and controllers or between two controllers. This traffic is extremely chatty and driven by cyclical I/O data being communicated on very short intervals between devices and controllers on the same VLAN. The only exception is with interlocking controllers where traffic for real-time data transfer would be between VLANs through one Layer 3 switch hop. An example in mining could be for intra controller communication along large conveyor systems. Some IACS protocols only support Layer 2/Ethernet for real-time traffic (PROFINET). This, combined with requiring determinism and predictability, lends itself to keeping the majority of this traffic for real-time at Layer 2.
- Non-real-time traffic is not as critical to the IACS communications and does not have the same constraints or network requirements as the real-time traffic. It is typically informational in nature and would flow between workstation or server in Level 3 operations and devices in Levels 0–2. This traffic is IP/TCP or IP/UDP and is typically routable.

Multicast traffic is an important consideration of a Cell/Area IACS network because it is used by some of the key IACS communication protocols. In IACS systems data packets are usually non-routable and so stay within the Cell/Area Zone.

Cell/Area Zone Performance and QoS Design

QoS provides classification, prioritization, and preferential forwarding treatment to various traffic flows within the Cell/Area Zone This prioritization helps to contribute to network performance, assurance, and predictability which is required to ensure mining IACS application uptime and performance. Highlighted in the Cell area zone traffic patterns there are other non-real time packet flows between Level 3 and the cell area zone all traffic flows need to be understood in creating a QoS model for these industrial environments.

Real-time performance and characteristics of the IACS applications should be well understood when designing to provide predictability and consistency in networking performance. Any unpredictability in the network performance causing too much latency or jitter as well as packet loss could cause IACS system errors or a shutdown of equipment. The following tables reference a defined set of requirements for various types of informational and time-critical I/O traffic classes.

Table 3 IACS Application Requirements Example

Requirement Class	Typical Cycle Time	Typical RPI	Connection Timeout
Information/Process (for example, HMI)	< 1 s	100 - 250 ms	Product dependent
Time critical processes (for example, I/O)	30 - 50 ms	20 ms	4 intervals of RPI, but =100 ms
Safety	10 - 30 ms	10 ms	24 - 1000 ms
Motion	500 µs - 5ms	50 µs - 1 ms	4 intervals

Table 4 IACS Application Requirements Example—PROFINET

Requirement Class	Typical Cycle Time	Typical RPI	Communication Class
Information/Process	< 1 s	100 - 250 ms	Non-Real Time (NRT)
Process/Discrete	30 - 50 ms	20 ms	Real Time (RT)

The tables above highlight the key IACS performance requirements are machine/process cycle times and the Request Packet Interval (RPI), which if not met can cause a connection timeout or shutdown of the equipment/process. These are usually defined as:

- Machine/process cycle times - The processing time in which industrial automation system application makes decisions.
- I/O update time - The processing time at which input/outputs are sent/received.

The QoS design for Industrial Automation followed the guidelines and standards outlined by ODVA, Inc. for a QoS Model with Common Industrial Protocol (CIP) and Precision Timing Protocol (PTP) traffic. This model has been validated and is supported. This version of the mining architecture aligns with these recommendations for QoS for the IACS traffic.

- Prioritization for IACS traffic over non-IACS traffic in the Cell/Area Zone if deployed on a shared infrastructure.
- IACS real-time traffic over IACS non-real-time traffic in the Cell/Area Zone. Within real-time services further differentiation may be required to support higher performance applications such as Safety and Motion.
- QoS deployed plant wide in a consistent manner. Network devices across the plant need to adhere to the same policy.

Table 5 ODVA, Inc. QoS Model for CIP and PTP Traffic

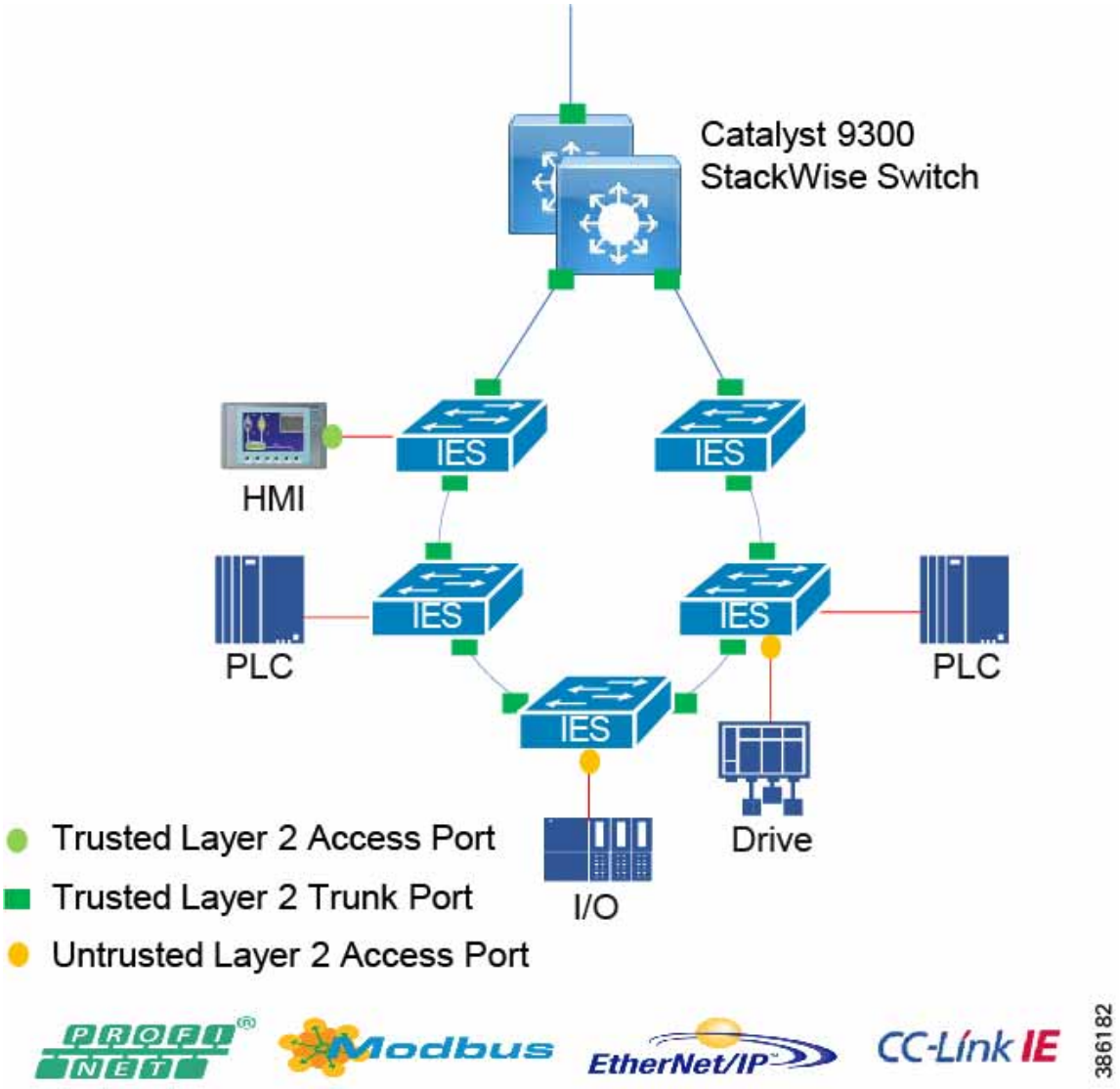
Traffic Type	CIP Priority	DSCP Layer 3	CoS Layer 2	CIP Traffic Usage
PTP event (IEEE 1588)	N/A	59	7	PTP event messages, used by CIP Sync
PTP General (IEEE 1588)	N/A	47	5	PTP management messages, used by CIP Sync
CIP class 0 / 1	Urgent (3)	55	6	CIP Motion
	Scheduled (2)	47	5	Safety I/O I/O
	High (1)	43	5	I/O
	Low (0)	31	3	No recommendations at present
CIP UCMM CIP class 3	All	27	3	CIP messaging

Cisco QoS uses a toolset to provide the priority and preferential treatment for the IACS 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 is not used in the QoS design for IACS traffic as we do not want to impact control traffic.

Figure 13 QoS Trust Boundaries



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.

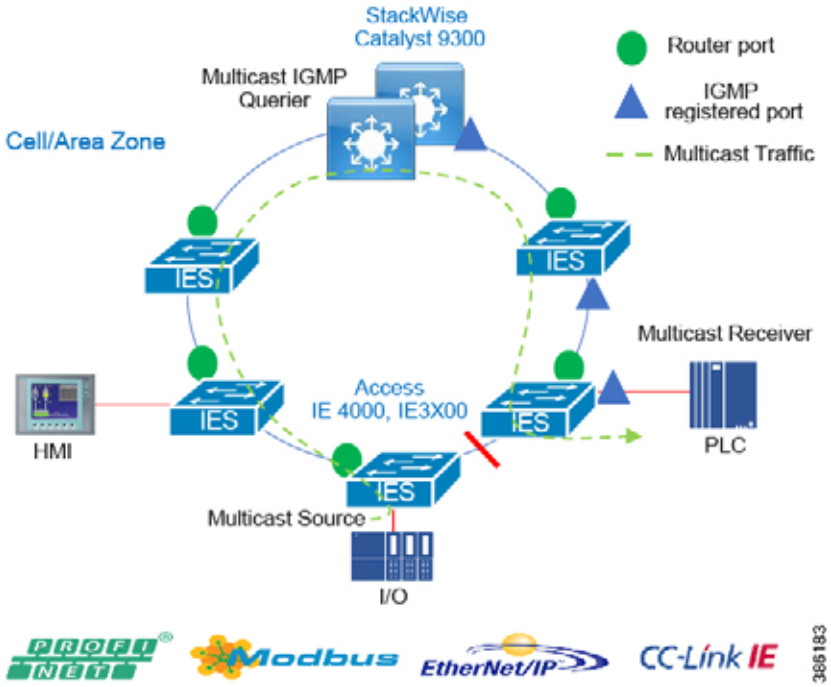
Once classified and in the network, the uplink and outbound ports on the network switches can be trusted and configured to schedule traffic according to the QoS profile. Figure below highlights the trusted versus untrusted description.

Configuration details and an in-depth description of the scheduling mechanisms for all the switches can be found in Quality of Service Design and implementation section of the Industrial Automation CVD. The switches evaluated in this round of testing included the Cisco IE 2000, Cisco IE 4000, Cisco IE 3200, Cisco IE 3400, and the Cisco Catalyst 9300.

Multicast Management in the Cell/Area Zone and ESP

Networking switches within the Cell/Area Zone should facilitate the support of multicast as it is used by some of the IACS protocols. In general, the multicast traffic at Cell/Area Zone does not go beyond Layer 2. 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 14 highlights the components and functions within the Cell/Area Zone for supporting IACS traffic deployed with multicast from Industrial Automation.

Figure 14 Cell/Zone Multicast



Recommendations for Deploying Multicast in the Cell/Area Zone

The same design principles are valid for mining IACS applications deploying multicast in the cell area zone as have been validated in Industrial Automation. The following are the recommendations

- Enable IGMP snooping and querier on all the industrial Ethernet switches as well as the distribution switch/router. Do not change any of the IGMP snooping default settings.

- Configure the IGMP querier on the distribution switch, central to the Cell/Area Zone topology. When multiple IGMP queriers are on a VLAN, the IGMP protocol calls for the querier with the lowest IP address to take over the querier function. Therefore, the distribution switch should have the lowest IP address in the subnet.

Availability

Availability of the industrial automation process affects the business directly and is therefore a critical component. Ensuring the uptime of the IACS applications requires a robust, resilient network. This section provides network design to support availability for IACS applications with platform protocol and path redundancy.

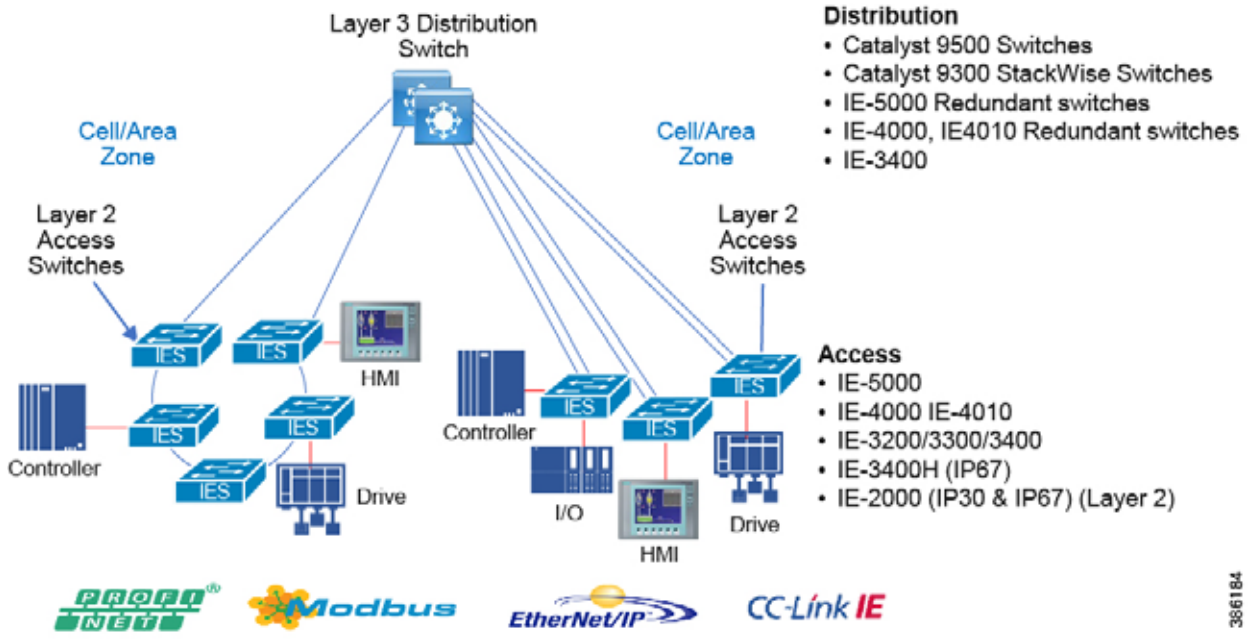
Across a mine the resiliency architecture is often dictated by the environment and where fiber can be physically run. Fiber will be the medium in almost all cases to interconnect network platforms due to distance of runs, however In open pit where fiber cannot be run to provide connectivity, wireless backhaul technologies are deployed. This backhaul connectivity is outside the scope of this design.

Rings and star topologies are relevant and seen within the architecture. Geographical placement of physical platforms is often a requirement, especially at the distribution and core layers. Redundant pairs of platforms could be seen located in different physical locations to provide added resiliency to the architecture. The following section details the various protocols and deployments validated within Industrial Automation that are relevant to the mining design.

Distribution Switch Resiliency

This section provides validated options for the Industrial Automation Solution that are relevant for mining. The following figure provides an overview.

Figure 15 Overview of Distribution Switch Resiliency



Cisco StackWise-480

Although mentioned earlier about mines requiring geographical diversity for the distribution layers there may still be some mines that deploy stacked switching in the distribution. The primary platform is the Ctalyst 9300. A switch stack can have up to eight stacking-capable switches connected through their StackWise-480 ports. The stack members work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network. A

switch stack always has one active switch and one standby switch. The active switch will provide control of the management plane for the stack. If the active switch becomes unavailable, the standby switch assumes the role of the active switch and keeps the stack.

For more information on switch stack configuration and features for the Cisco Catalyst 9300 see: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/stck_mgr_ha/b_169_stck_mgr_ha_9300_cg/managing_switch_stacks.html

Hot Standby Redundancy Protocol

Hot Standby Redundancy Protocol (HSRP) is an alternative to StackWise-480 for the distribution switch. HSRP provides high availability through redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router sends packets; the standby router takes over the routing duties when an active router fails or when preset conditions are met. For the CRD, two Layer 3-enabled switches were deployed for HSRP scenarios, one active and one standby. HSRP deployed switches can help support the requirement for geographical diversity of redundant switches at the distribution layer.

StackWise Virtual

Another platform resiliency option at the distribution layer is StackWise Virtual. The Cisco Catalyst 9500 switch supports StackWise Virtual, where two switches are connected through redundant 10 or 40 Gigabit links and operate as a single switch with active and standby nodes. Much like StackWise-480, Layer 2 and Layer 3 functions operate from the single "virtual" entity and the control, management, and data planes are integrated. The limitation for StackWise Virtual is the lack of support for REP, RSPAN, and SDA, therefore StackWise Virtual configurations were not validated.

Horizontal Stacking – IE5000

Horizontal stacking, also referred to as long-reach stacking, allows you to stack between two to four IE 5000 switches that are far apart, potentially up to a few kilometers.

Horizontal stacking provides resiliency and optimal convergence in industrial Ethernet networks. All switches appear as a single logical switch with a single IP address. Benefits of stacking include ease of management due to fewer stand-alone devices, increased port density, increased redundancy, and flexibility to add devices as required. All manageable entities (for example, Ethernet interfaces and VLANs) on all physical switches can be configured and managed from the logical switch.

The IE 5000 horizontal stacking was not validated in Industrial Automation CVD.

Distribution options validated as part of the Industrial Automation CVD relevant to mining are:

- Catalyst 9300 with StackWise and REP
- Catalyst 9300 with HSRP and REP
- IE 5000 with HSRP and REP
- Catalyst 9300 StackWise with Ether channel

Distribution options NOT validated as part of the Industrial Automation CVD relevant to mining are:

- Catalyst 9500 HSRP with REP Rings
- Catalyst 9500 StackWise Virtual with Star Connectivity
- IE 5000 Horizontal Stacking with REP rings
- Catalyst 9500 Stackwise Virtual with REP no neighbor Configured REP rings

Not Supported:

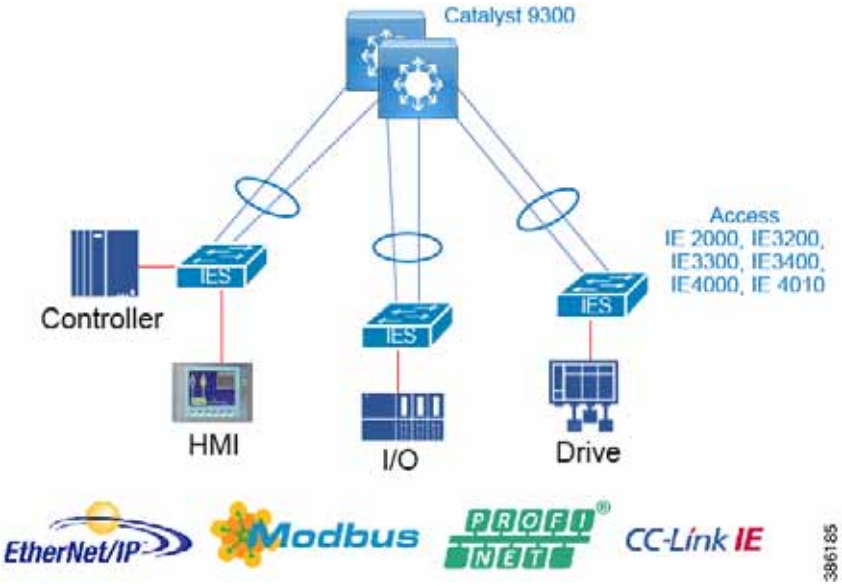
- Catalyst 9500 StackWise Virtual with REP rings

Redundant Star Topology

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. 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.

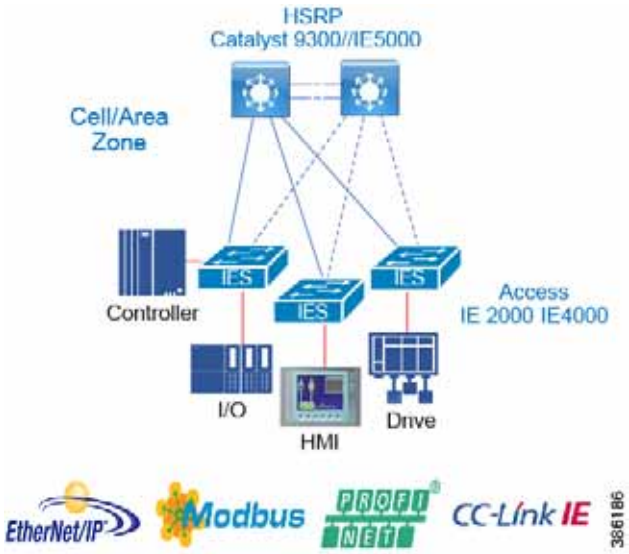
Figure 16 Cell/Area Zone Redundant Star Topology



Flex Links

Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels), in which one interface is configured to act as a backup to the other. This feature provides an alternative solution to the Spanning Tree Protocol (STP) and is deployed between an access switch and a distribution switch. The active link is used to forward and receive frames and the standby link does not forward or receive frames, but is in the up/up state. When a failure is detected on the active link, the standby link moves to active and all MAC addresses and multicast entries move to the standby link. On restoration of the failed link it will again become the standby link. Note: The Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 switches do not support Flex Links in the software used for this CRD.

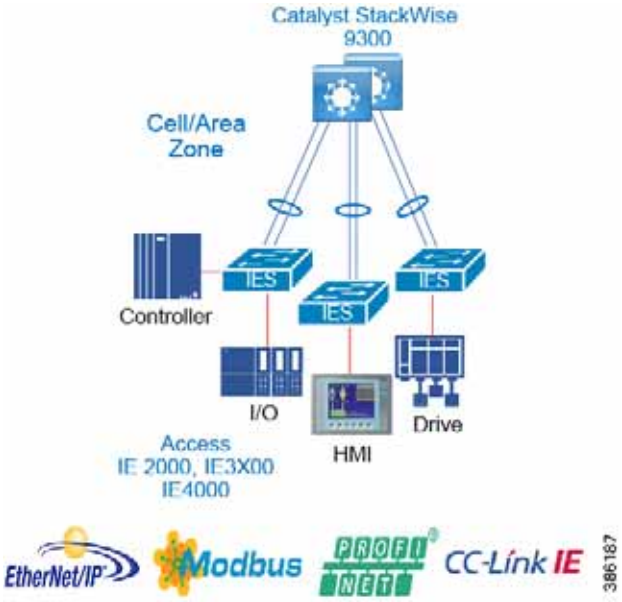
Figure 17 Cell/Area Zone Flex Links



Redundant Star Design and Validation

The Industrial Automation validation has results and recommendations for Redundant star configurations with the Catalyst 9300 evaluated with the Cisco IE 3200/Cisco IE 3400 and Cisco IE 4000 switches in a redundant star configuration with EtherChannel.

Figure 18 Redundant Star Design and Validation



The table provides details of the convergence results for multiple types of failures. Link disruptions refer to a single link failure in the ether channel. Switch failures refer to a primary distribution switch failure where the backup switch would assume the active role. Multiple link and switch failures were conducted where the maximum and average convergence times were recorded. Simulated traffic and real IACS devices were used during validation. The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

Table 6 Star Topology with Cisco Catalyst 9300

Disruption Type	Traffic Type	Convergence Cisco IE 3200/Cisco IE 3400 Fiber		Convergence Cisco IE 3200/Cisco IE 3400 Copper		Convergence Cisco IE 4000 Copper	
		Max	Average	Max	Average	Max	Average
Link	L2 Multicast	90	69	320	95	94	53
	L2 Unicast	90	69	320	95	94	53
	L3 Unicast	90	69	320	95	94	53
Switch	L2 Multicast	238	48	733	170	102	44
	L2 Unicast	106	41	152	60	102	44
	L3 Unicast	106	48	152	64	102	44

The convergence for link failures using the Cisco Catalyst 9300 copper downlinks with Cisco IE 3200/Cisco IE 3400 were much higher than with the Cisco IE 4000.

Fiber testing for the Cisco IE 3200/Cisco IE 3400 was much improved in these scenarios with both the Cisco Catalyst 9300 as the distribution switch. In mining the main connectivity medium will be fiber.

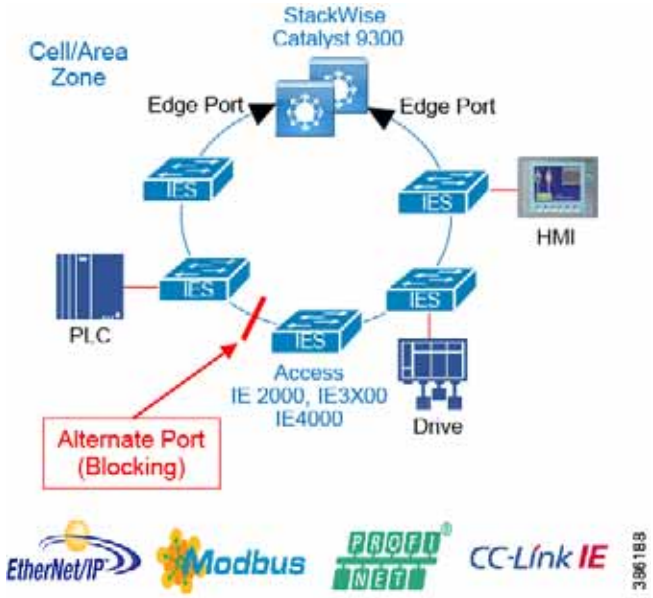
- With Cisco Catalyst 9300 as the distribution switch, Cisco IE 3200/Cisco IE 3400 is not recommended with copper media for IACS applications with outliers that may cause connection timeouts.
- With the Cisco Catalyst 9300 the distribution switch failure may cause higher convergence time for Layer 2 multicast traffic (238ms) and cause connection timeouts for IACS applications that use multicast. The applications can be tuned to accommodate or potentially not use multicast for the application.

Ring Resiliency Protocols

REP

REP is a Cisco proprietary protocol that provides an alternative to STP to control network loops, handle link failures, and improve convergence time. REP runs a single redundancy instance per segment or physical ring. One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment and each segment port can have only one external neighbor. Each end of a network segment terminates at a neighboring Cisco IE access switch or distribution switch. The port where the segment terminates is called the edge port.

Figure 19 REP Overview



Loop prevention in the ring is maintained with one port in the segment being in a blocked state, also known as the alternate port. If a failure in the segment is detected, then the alternate port will move to a forwarding state allowing traffic to traverse the alternate path avoiding the network failure.

For REP basic operations and failover descriptions please read the following REP documentation: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG/Industrial-AutomationDG.html#pgfId-279814

Rep Ring Validation in Industrial Automation validation was tested with

- IE 5000 as the distribution switches running HSRP
- Catalyst 9300 IP address as the distribution switch

Table 7 REP Ring with Cisco IE 5000 in Distribution HSRP

Disruption Type	Traffic Type	Convergence Cisco IE3x00 Fiber		Convergence Cisco IE3x00, IE4000 Fiber		Convergence Cisco IE3400H Copper	
		Max (ms)	Average (ms)	Max (ms)	Average (ms)	Max (ms)	Average (ms)
Link	Layer 2 Multicast	344	88	380	93	538	259
	Layer 2 Unicast	344	92	212	99	558	266
	Layer 3 Unicast	344	70	484	149	732	282

Switch	Layer 2 Multicast	500	114	234	117	4368	990
	Layer 2 Unicast	502	119	234	126	4368	995
	Layer 3 Unicast	1224	387	1322	546	4368	951

Result Considerations

- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same physical ring.
- Link disruptions refer to a single link failure in the ring. Switch failures refer to power interruption of a single switch at a time; distribution and IE switches were reloaded during testing.
- Simulated traffic and real IACS devices were used during validation.
- The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic. Three REP rings:
  - Mixed ring—Cisco IE 3200, Cisco IE 3300, Cisco IE 3400, and Cisco IE 4000 (12 nodes)
  - IE 3x00 ring—Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400 (11 nodes)
  - IE 3400H ring—Cisco IE 3400H (4 nodes)

REP Ring with Cisco Catalyst 9300 in Distribution

Recommendations for this topology:

- It is recommended to use fiber links since it provides faster convergence than copper links.
- When using StackWise for distribution with a REP ring it is a good practice to locate the alternate port in between access switches to achieve higher Layer 3 convergence in case of primary stack member power failure.

Figure 20 REP ring with Cisco Catalyst 9300

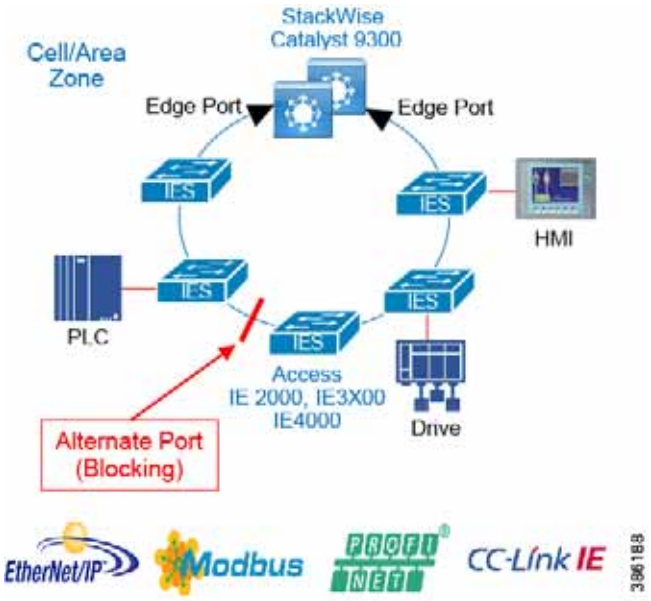


Table 8 REP Ring with Cisco Catalyst 9300 in Distribution

Disruption Type	Traffic Type	Convergence Cisco IE3x00 Fiber		Convergence Cisco IE3x00, IE4000 Fiber	
		Max (ms)	Average (ms)	Max (ms)	Average (ms)
Link	Layer 2 Multicast	118	45	374	77
	Layer 2 Unicast	116	44	284	75
	Layer 3 Unicast	116	43	284	72
Switch	Layer 2 Multicast	616	171	220	132
	Layer 2 Unicast	618	164	216	142
	Layer 3 Unicast	972	436	1002	413

Result Considerations

- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same ring.
- Link disruptions refer to a single link failure in the ring. Switch failures refer to power interruption of a single switch at a time; distribution members and IE switches were reloaded during testing.
- Three REP rings were evaluated with the following switches:
  - Mixed ring—Cisco IE 3200, Cisco IE 3300, Cisco IE 3400, and Cisco IE 4000 (12 nodes)

  - IE3x00 ring—Cisco IE 3200, Cisco IE 3300, and Cisco IE 4000 (11 nodes)
  - IE3400H ring—Cisco IE 3400H (4 nodes)
- The Cisco Catalyst 9300 distribution node contained two Stack members.
- Simulated traffic and real IACS devices were used during validation. The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

The Cisco Catalyst 9300 distribution StackWise configuration with Cisco IE 3x00 access switches should be considered as the best choice for REP deployments for IACS environments, though considerations should be given to the outlier Max results for convergence which could cause a connection timeout for IACS applications.

REP Fast

The REP Fast feature supported on the Cisco IE 3x00 switches follows the same functionality as REP but improves failure detection time among the participating switches. The switch executes two timers for each REP Fast interface to determine successful transmission; the first timer runs every three milliseconds as the switch sends a beacon frame to the neighbor node. If the frame is received, the timer is reset. If the frame is not received, the second timer begins and lasts for ten milliseconds. If the frame is still not received, the switch sends a link down notification. The REP Fast convergence specification is 50 milliseconds, whereas traditional REP ranges from 50-250 milliseconds.

The Cisco IE 3x00 series switches support REP Fast for copper and fiber and both media produce similar link failure convergence times. In addition, REP and REP Fast can be used in the same ring to connect Cisco IE 3x00 switches with other models that do not support REP Fast. This validation of REP Fast was done with a hybrid REP and REP Fast ring, using traditional REP to connect the Cisco IE 3x00 switches to the respective distribution switches.

Figure 21 REP and REP Fast Ring with Cisco Catalyst 9300 in Distribution

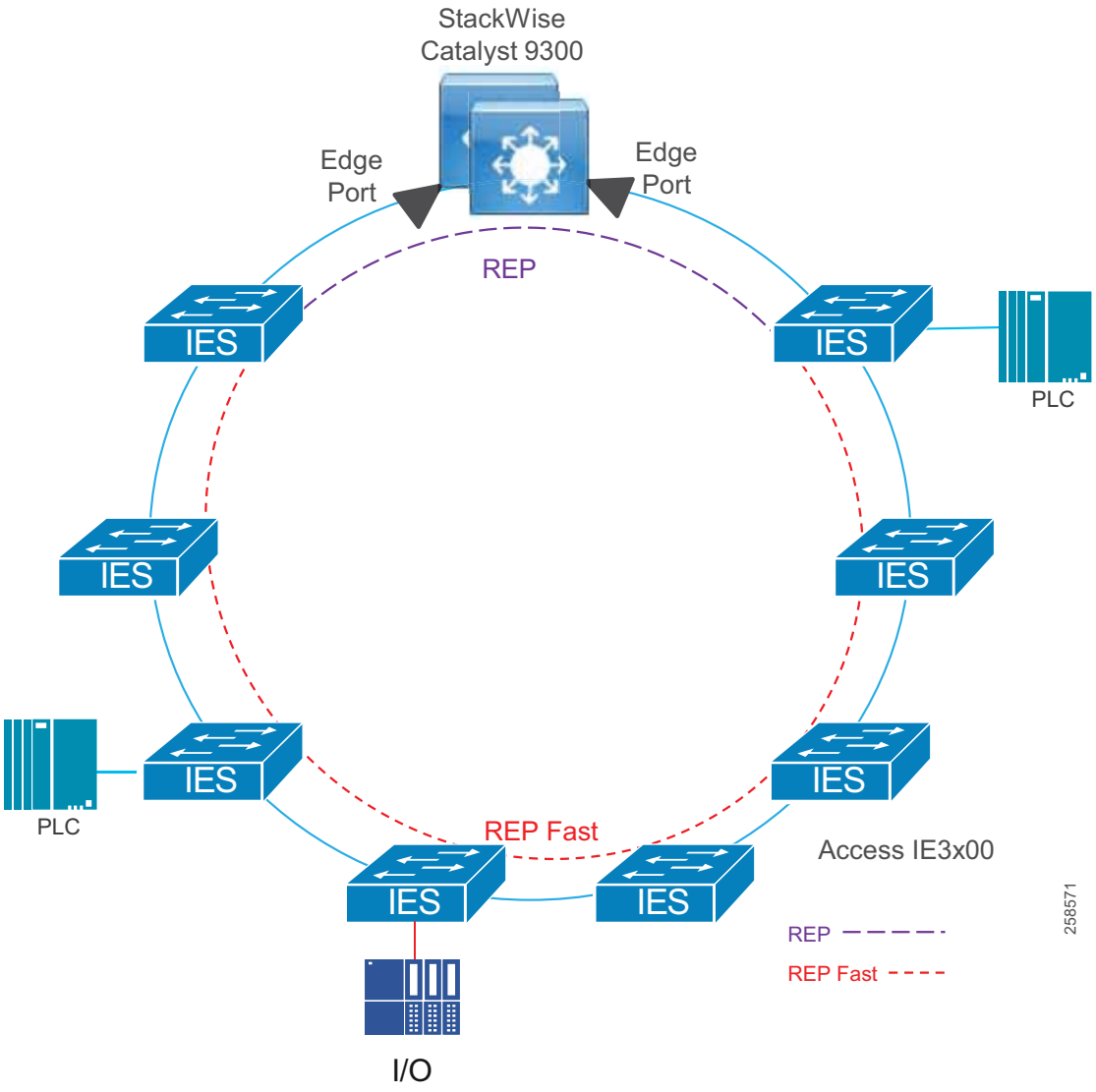


Table 9 REP and REP Fast Ring with Cisco Catalyst 9300 in Distribution

Disruption Type	Traffic Type	Convergence Cisco IE3x00 Fiber		Convergence Cisco IE3400H Copper	
		Max (ms)	Average (ms)	Max (ms)	Average (ms)
Link	Layer 2 Multicast	118	61	62	32
	Layer 2 Unicast	166	58	44	16
	Layer 3 Unicast	166	55	48	23

Switch	Layer 2 Multicast	212	72	4310	1002
	Layer 2 Unicast	212	62	750	240
	Layer 3 Unicast	212	77	846	432

Figure 22 REP and REP Fast Ring with Cisco IE 5000 in Distribution

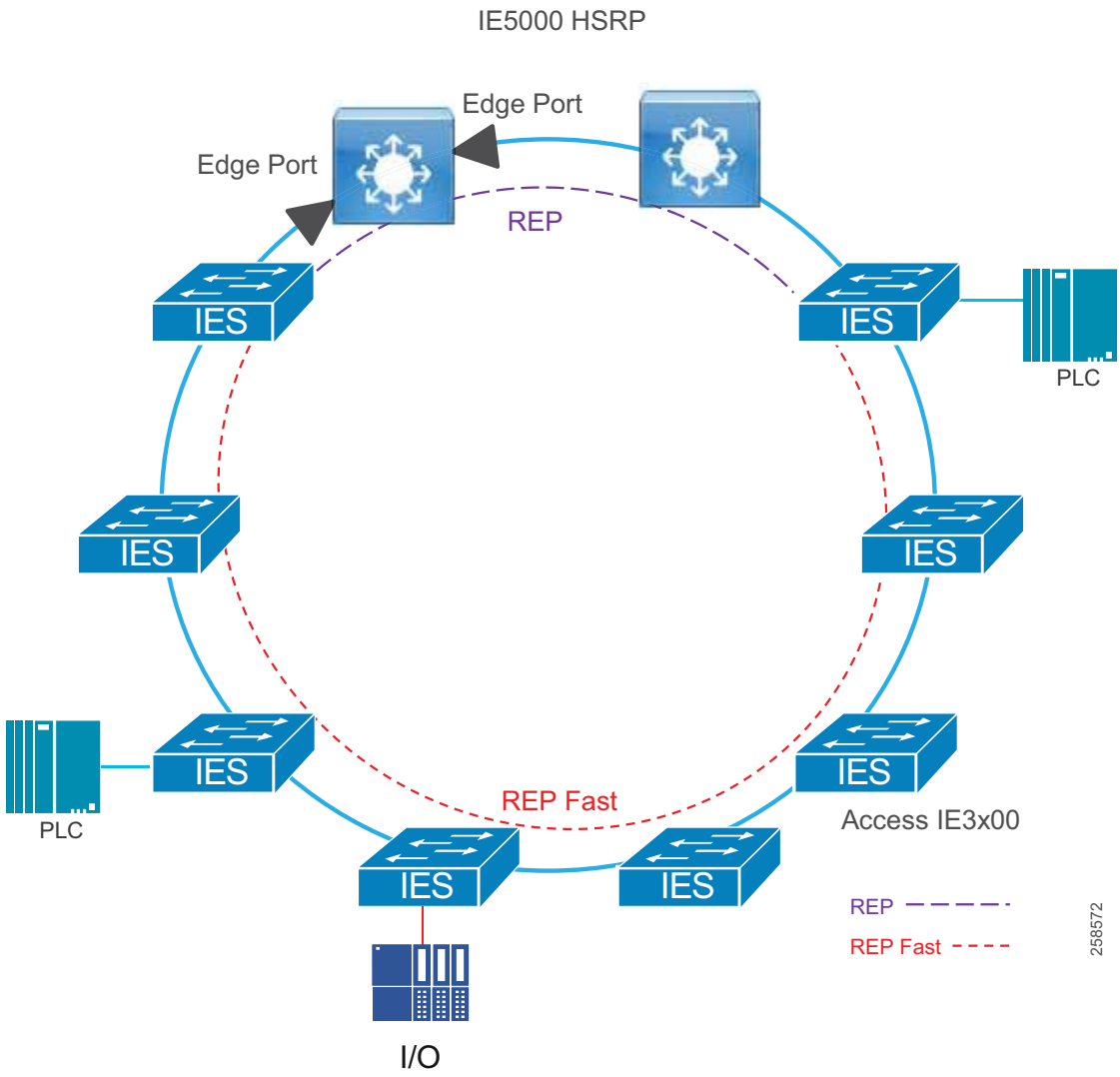


Table 10 REP and REP Fast Ring with Cisco IE 5000 in Distribution

Disruption Type	Traffic Type	Convergence Cisco IE3x00 Fiber		Convergence Cisco IE3400H Copper	
		Max (ms)	Average (ms)	Max (ms)	Average (ms)

Link	Layer 2 Multicast	210	76	70	24
	Layer 2 Unicast	210	78	56	15
	Layer 3 Unicast	210	79	66	23
Switch	Layer 2 Multicast	58	32	3554	662
	Layer 2 Unicast	80	35	376	193
	Layer 3 Unicast	1040	268	1066	480

Result Considerations

- The two rings tested contained IE switches of the following types:
  - IE 3x00 (11 nodes): Cisco IE 3200, Cisco IE 3300, and Cisco IE 3400
  - Cisco IE 3400H (four nodes)
- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same ring.
- Link disruptions refer to a single link failure in the ring. Link failures were conducted at varying points in the ring in both the REP and REP Fast areas. Switch failures refer to power interruption of a single switch at a time; distribution members and IE switches were reloaded during testing.
- Simulated traffic and real IACS devices were used during validation.
- The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

High Availability Seamless Redundancy (HSR)

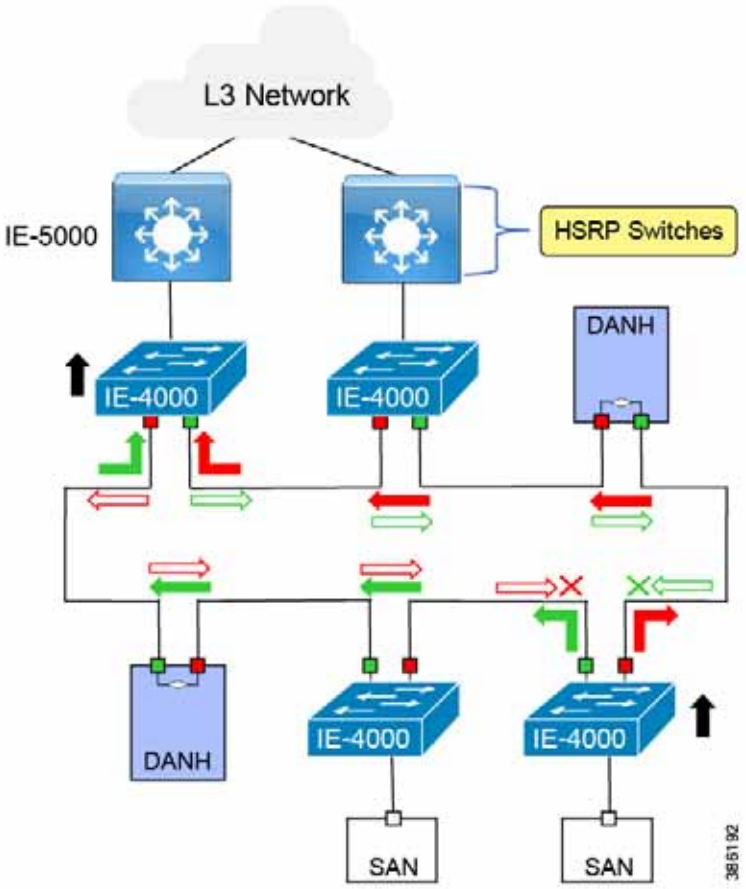
HSR is defined in International Standard IEC 62439-3-2016 clause 5. HSR has been seen primarily in utility IEC 61850 substation architectures, however, its lossless redundancy features make it a viable option for other plant-based environments where IACS applications require better ring convergence than REP. HSR is similar to Parallel Redundancy Protocol (PRP) but is designed to work in a ring topology. Instead of two parallel independent networks of any topology (LAN-A and LAN-B), HSR defines a ring with traffic in opposite directions. Port-A sends traffic counterclockwise in the ring and Port-B sends traffic clockwise in the ring. The duplicated packet mechanism provides lossless redundancy under a single failure within the ring.

To allow the switch to determine and discard duplicate packets, additional protocol-specific information is sent with the data frame. The HSR header contain a sequence number, which is the primary data used to determine if the received frame is the first instance or a duplicate instance.

The non-switching nodes with two interfaces attached to the HSR ring are referred to as Doubly Attached Nodes implementing HSR (DANHs). Similar to PRP, SANs are attached to the HSR ring through a RedBox The RedBox acts as a DANH for all traffic for which it is the source or the destination. The switch implements RedBox functionality using Gigabit Ethernet port connections to the HSR ring.

Figure 23 shows an example of an HSR ring as described in IEC 62439-3. In this example, the RedBoxes are Cisco IE 4000 switches. As of today the Cisco IE 4000 or Cisco IE 4010 and Cisco IE 5000 switches are the only switches that will support an HSR deployment. Note that in the figure the IE5000 switches are not partaking in HSR but aggregation/Distribution HSRP switches.

Figure 23 HSR Overview and Packet Flows



Devices that do not support HSR out of the box (for example, laptops) cannot be attached to the HSR ring directly as all devices on the ring must be able to support HSR. These nodes are attached to the HSR ring through a RedBox. As shown above, the RedBox has two ports on the DANH side. Non-HSR SAN devices are attached to the switch ports.

HSR Summary

- Lossless redundancy over a ring topology
- All nodes in the ring **must** have special hardware to support HSR and all nodes in the ring must support HSR.
- Useful for networks that require faster convergence than REP as it provides lossless redundancy
- Supported on Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000 only
- Bandwidth available in ring is reduced by up to half due to duplicate packets
- In a typical implementation, the receiving node removes both packets from the HSR Ring.

HSR Validation

Cisco Catalyst 9300 StackWise REP and HSR with Cisco IE 4000 Switches

This topology uses StackWise for distribution redundancy. It uses REP for connectivity between the access ring and the distribution as shown in Figure 39. HSR is implemented in the access ring topology. REP is used between the links which directly connect the IE access and Cisco Catalyst 9300 distribution switches. REP edge ports are configured on the access switch uplinks as shown in figures below. A disruption in this topology has zero downtime for traffic in the ring. A failure in the REP ring will have an impact on Layer 3 traffic according to REP convergence times. This topology without REP will result in network loops.

Validated HSR Topologies

Figure 24 Cisco Catalyst 9300 StackWise REP and HSR with Cisco IE 4000 Switches

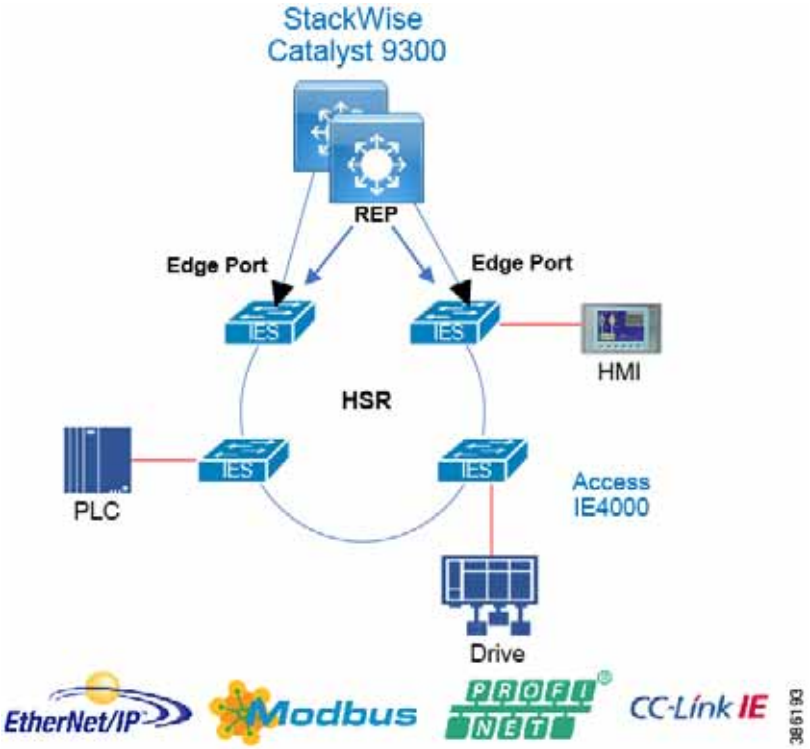


Table 11 HSR Ring

Disruption Type	Traffic Type	Convergence	
		Max	Average
Link	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	0	0
Switch	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	780	405

Note: Link or switch failures outside of the HSR rings, in other words the links to the distribution or the distribution switches themselves, caused Layer 3 unicast packet loss for the switches in the HSR rings. The convergence time for these failures aligns with expectations for REP convergence over copper links.

HSR-HSR

HSR rings can also be implemented in such a way that key switches are participating in two HSR rings, using four interfaces to connect the respective rings, which is known as HSR-HSR or Quadbox. When the HSR-HSR mode is licensed and enabled, the switch shuts all non-HSR ports to avoid traffic interference. Connectivity to the HSR-HSR switch can be done through the HSR-HSR ports or the out-of-band console interface. Mining has subtended ring architectures where this design could be applicable.

Figure 25 HSR-HSR Ring with Cisco Catalyst 9300 in Distribution

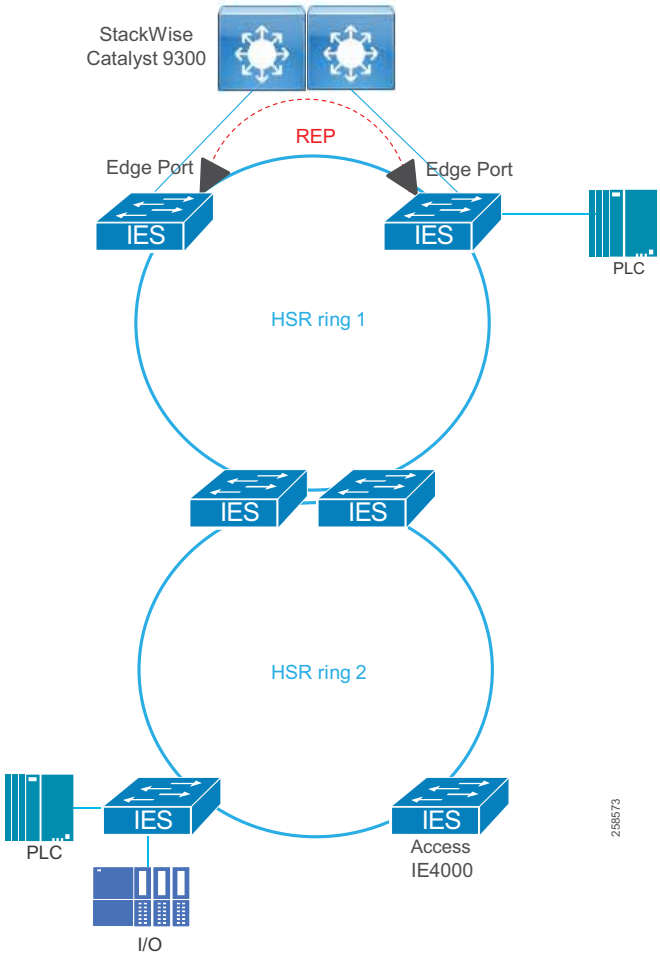


Table 12 HSR-HSR Ring with Cisco Catalyst 9300 in Distribution

Disruption Type	Traffic Type	Convergence	
		Max	Average
Link	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	0	0
Switch	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	0	0

Figure 26 HSR-HSR Ring with Cisco IE 5000 in Distribution

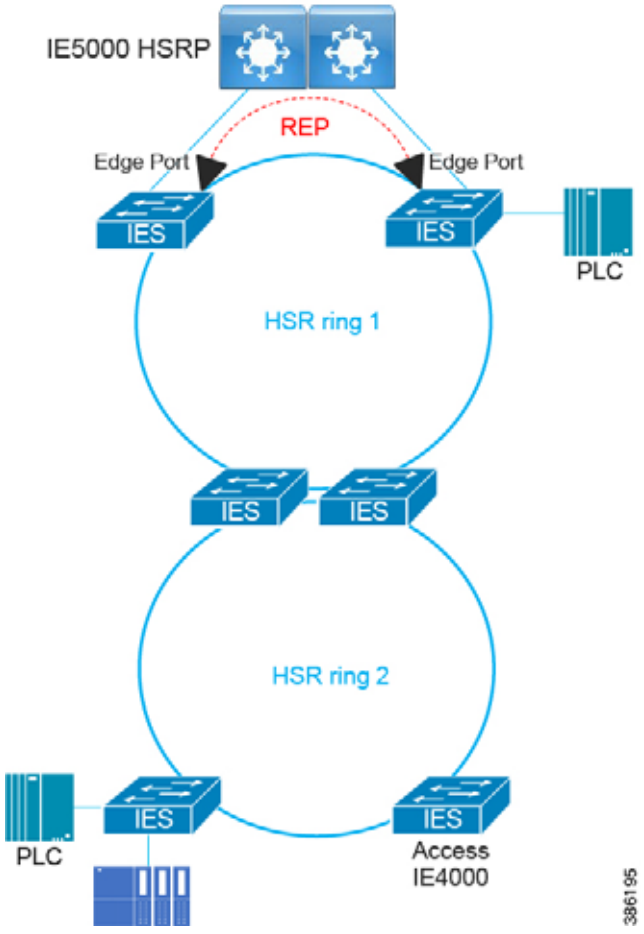


Table 13 HSR-HSR Ring with Cisco IE 5000 in Distribution

Disruption Type	Traffic Type	Convergence	
		Max	Average
Link	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	0	0
Switch	Layer 2 Multicast	0	0
	Layer 2 Unicast	0	0
	Layer 3 Unicast	0	0

Result Considerations

The validation of HSR-HSR was done with two rings containing Cisco IE 4000 switches connected with copper Ethernet. An open REP segment connected one HSR ring to the distribution switches using copper Ethernet.

- Convergence was validated for Layer 2 traffic within a VLAN and Layer 3 traffic between VLANs in the same ring.
- Link disruptions refer to a single link failure in the ring. Link failures were conducted at varying points across both HSR rings. Switch failures refer to power interruption of a single switch at a time; distribution members and IE switches were reloaded during testing.
- Link or switch failures outside of the HSR rings, in other words the links to the distribution or the distribution switches themselves, caused Layer 3 unicast packet loss for the switches in the HSR rings. The convergence time for these failures aligns with expectations for REP convergence over copper links.
- Simulated traffic and real IACS devices were used during validation.
- The scenario was run with 250 MAC addresses, 200 multicast groups, and inter- and intra-VLAN traffic.

Media Redundancy Protocol (MRP)—PROFINET Deployments

The media redundancy protocol (MRP) is a data network protocol standardized by the International Electrotechnical Commission (IEC) as IEC 62439-2. The MRP allows rings of Ethernet switches to overcome a single failure with recovery time much faster than achievable with traditional STP.

Roles—Cisco Industrial Ethernet switches support the following two roles:

- Media Redundancy Manager (MRM)
- Media Redundancy Client (MRC)

In a ring topology, only one switch or industrial automation System device can act as an MRM; all other devices will act as an MRC. The purpose of an MRM is to keep the ring loop free and provide redundancy when failure happens. The MRM does this by sending a control packet from one ring port and receiving them on its other ring port in both directions. If it receives the control packets then the ring is in an error-free state.

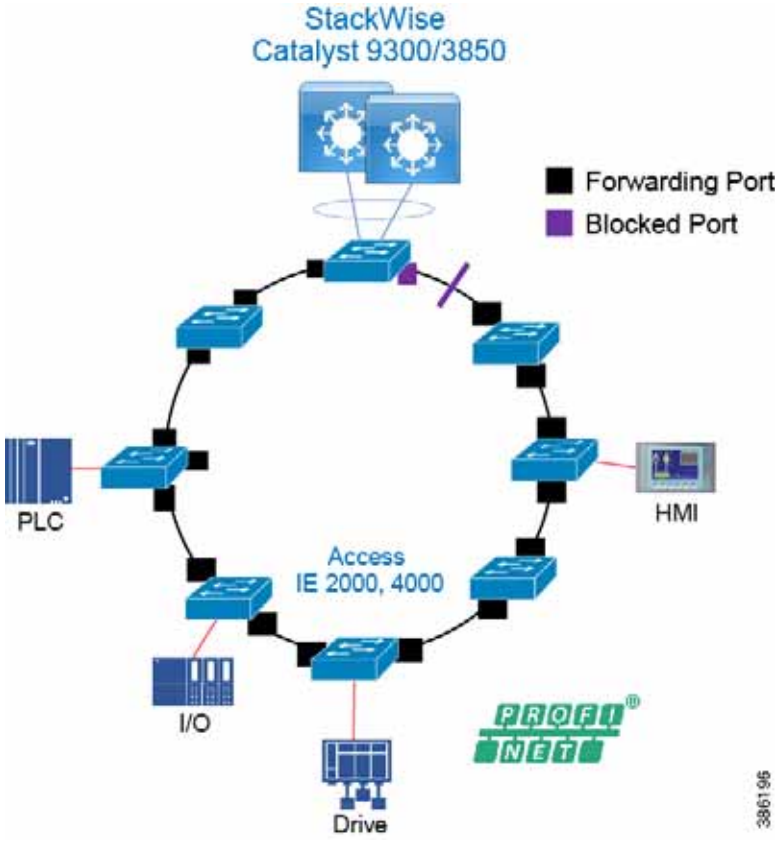
There are three port states used within MRP:

- Disconnected/Disabled—In this state, switch port will drop all received packets.
- Blocked—In this state, all received frames are dropped except control packets.

- Forwarding—Normal working state that forward all received packets on the port.

During normal operation, the network operates in the closed state. In this state, one MRM one ring port remains in a blocked port status and the other port is in the forwarding status. All MRCs will be in forwarding status as well. Loops are avoided because of the blocked port on the MRM.

Figure 27 MRP Normal Mode of Operations



Resiliency Summary and Comparison

Table 14 provides high-level guidance on resiliency protocols based on performance and interoperability. Note the maximum number of nodes is generally a recommendation, rather than an absolute limit.

Table 14 Resiliency Protocols Comparison

Protocol	Topology	Number of Nodes	Typical Convergence	Remark
RSTP/MSTP	Any	Max hops 255	50 ms - 6 seconds	Provides widest interoperability but poorest convergence and troubleshooting
MRP	Ring	50	200 - 500 ms	Siemens is big proponent. Interoperable with switches that support Standard IEC 62439-2. Common in PROFINET environment.
REP	Ring	50	50 - 250 ms	Cisco proprietary. Very easy setup and troubleshooting.
PRP	Any	Unlimited	0 ms	Duplicate LANs required.(expensive) Standard IEC 62439-3 Clause 4
HSR	Ring	50	0 ms	Requires all nodes in Ring support HSR. Standard IEC 62439-3 Clause 5

Note: RSTP and MSTP were not verified in the Industrial Automation CVD. Parallel Redundancy Protocol PRP is a lot more relevant for the utilities space and information on PRP can be found in the Utilities CVD.

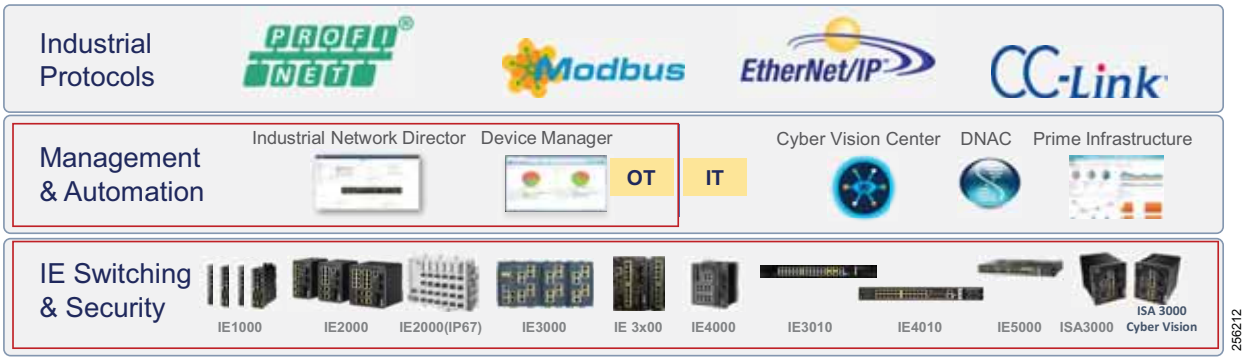
Cell/Area Zone Management

Ethernet networks are an integral part of modern automation and control environments and operations personnel are growing increasingly dependent on network monitoring to reduce unplanned downtime. Where possible the management network should have its own dedicated network within the mine. Practically it may not be possible to dedicate a separate physical infrastructure so a VLAN and or VRF should be configured to provide a segmented private network. Role based access control, secure use of network management traffic (SSH, SNMPv3) are best practices too.

OT control engineers are taking on more of a role for basic network management functions. The control engineers require visibility and access to the network when issues arise so network management must address the following key considerations.

Within the Cell/Area Zone, the tools provided to help assist with the management of the network must provide an OT view that is familiar to a control engineer. It should look and feel like a component or extension of the IACS system rather than an IT network management tool. The network should be easy to deploy, configure, and monitor. Network components should be easy to replace or install for the OT experienced controls engineer. Cisco Industrial Network Director (IND) is the tool to provide this requirement. Cisco DNA Center (DNA-C) is positioned as the tool to assist with network management at the operations layer where an IT-based team would provide network management functions in support of the industrial plant.

Figure 28 Network Management Support Model



Note: Cisco Prime and DNAC were not tested as part of the Industrial Automation CVD.

Cisco Industrial Network Director

The Cisco IND provides operations-centric network management for industrial Ethernet networks. The system supports industrial automation protocols such as CIP, PROFINET, OPC-UA, Modbus, BACnet, and so on to discover automation devices such as PLC, I/O, HMI, and drives and delivers an integrated topology map of automation and networking assets; this provides a common framework for operations and plant IT personnel to manage and maintain the industrial network.

The system uses the full capabilities of the Cisco IE product portfolio to make the network accessible to non-IT operations personnel. The simple user interface streamlines network monitoring and delivers rapid troubleshooting of common network problems found in industrial environments. For more information see: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

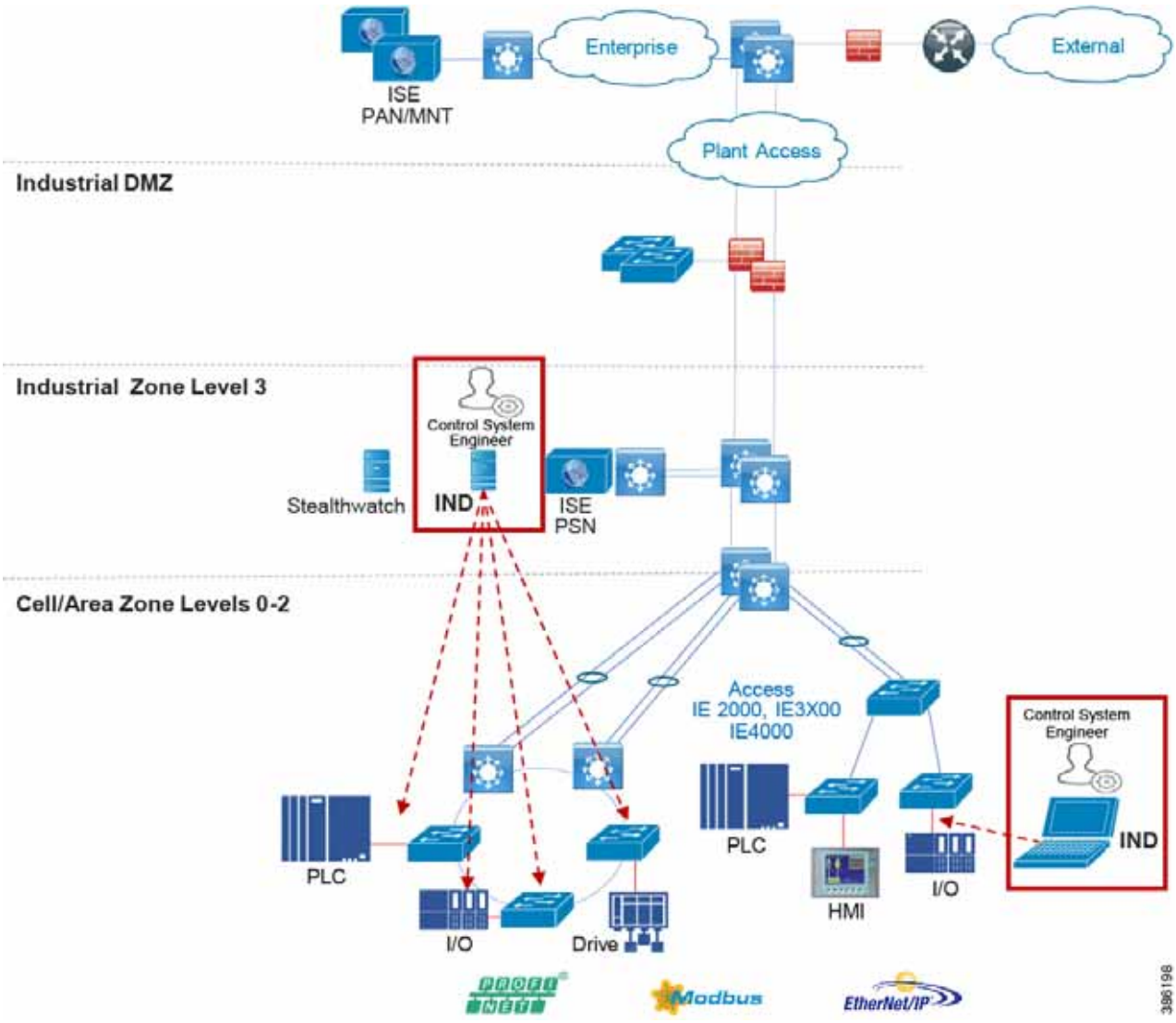
The IND Features include:

- Plug-and-play server for switch commissioning - The Cisco IND provides a plug-and-play server for the provisioning and replacement of industrial Ethernet devices. A controls engineer now has an easy way to replace faulty network equipment such as the network switch.
- Automated discovery of industrial and network assets - Cisco IND discovers the networking topology and automation devices with Common Industrial Protocol (CIP), PROFINET, Modbus, OPC-UA, BACnet, Siemens S7, and other industrial communication protocols. The user interface can provide visibility of connectivity between automation and networking assets on a dynamic topology map
- Troubleshooting - Cisco IND can visualize and provide alerts to networking events with contextualized industrial asset visibility.
- Role-based access control (RBAC) - Cisco IND is ideal for environments where different types of users need different levels of information and access.
- Rich application programming interfaces (APIs) for rapid integration with industrial applications - Cisco IND includes a comprehensive RESTful API allowing it to easily integrate with existing industrial asset management tools, automation applications, and control systems
- Supports IE 1000, IE2000, IE 3200, IE 3300, IE 3400, IE 4000, IE 4010, IE 5000

Cisco IND Deployment Options and Considerations

Cisco IND can be installed on a server in the industrial zone with tightly restricted access to other areas of the network. It is recommended to use only secure protocols such as HTTPS and SSH when possible to protect critical data. If required, Cisco IND is lightweight enough to be installed on a ruggedized laptop that resides within a zone on a plant floor, as long as it meets the system requirements. Figure 29 highlights the position in the architecture for Cisco IND. The example shows a server in the Industrial zone and a secure, ruggedized laptop in the Cell/Area Zone.

Figure 29 Cisco IND Deployment and Considerations



Cell Area Zone Security

Digital transformation initiatives in the plant are changing the dimension of traditional OT. Newer networking technologies and COTS hardware and software are replacing legacy products and newer business initiatives are forging a movement towards IT/OT convergence. Technology itself cannot address the entire security realm; people and process must play a

critical part in addressing the cybersecurity threat. This is key when addressing OT security. The IT teams need to have a thorough understanding of the business requirements and processes that apply within the industrial environment and assist with implementation. This is extremely relevant in the Cell/Area Zone where traditional IT skillsets are limited and the IT and OT teams need to move away from the traditional siloed approach to network management and work together. A 2015 Gartner study found security can be enhanced if IT security teams are shared, seconded, or combined with OT staff to plan a holistic security strategy.

Security in the Cell/Area Zone needs to be viewed as a component of an overall end-to-end security architecture across the entire mining on site operations. Any security capability needs to span the breadth of the mining operations and must encompass existing processes and strategy linked to an overall compliance effort while supporting safety, 24 hours a day, 7 days a week.

This section will provide an overview of:

- Network Hardening
- Site Reference architecture with a view on OT/IT Roles for supporting security across a mine
- Security System components
- Visibility and Segmentation design considerations
- OT Intent-based Security for Industrial Automation Use Cases

Network Hardening—A Component of System Integrity

System hardening, within the realms of cybersecurity, can be defined as reducing the attack surface or vulnerability of a system and making it more resilient to attack through hardening measures. Hardening activities include disabling unnecessary services and applications, providing least-privilege user access to systems, and adding additional security features such as anti-malware, anti-virus, and endpoint security. General system hardening practices apply to networks as well. Network hardening will deploy least privilege access control, disabling or removing unused services, logging, and enabling secure protocols. These hardening features and functions need to be configured across the three functional planes within a networking system. These three functional planes are the Management Plane, the Control Plane and the Data Plane.

- **Management Plane**-The management plane provides access to the networking devices and consists of functions that provide management of the networking system. The management plane is used to access, configure, and manage a device, as well as monitor its operations and the network on which it is deployed. This includes interactive management sessions that use SSH, as well as statistics gathering with SNMP or NetFlow. When you consider the security of a network device, it is critical that the management plane be protected. If a security incident undermines the functions of the management plane, it may be impossible for you to recover or stabilize the network. Where possible an out-of-band network for network management should be deployed. This keeps network management traffic separated from IACS traffic, which has the advantage of keeping the device reachability independent of any issues that may be occurring in the IACS network. If an out-of-band network is not possible, a logically separated network using a dedicated network management VLAN should be utilized.

- **Control Plane**-The control plane of a network device processes the traffic that is paramount to maintain the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, which includes the routing protocols and Layer 2 protocols such as REP. It is important that events in the management and data planes do not adversely affect the control plane. Should a data plane event such as a denial of service (DoS) attack impact the control plane, the entire network could become unstable. It should also be stated that control plane traffic needs to be understood and protected so that abnormalities do not affect the performance of the network devices' CPUs, thus making the networking device unstable and therefore creating/contributing to network-wide instability.

- **Data Plane**-The data plane forwards data throughout a networking system traversing the networking devices. This would be the IACS data traffic between controllers, I/O, HMI, and any other devices plugged into the network. The data plane contains the logical group of "customer" application traffic generated by hosts, clients, servers, and

applications that are sourced from and destined to other similar devices supported by the network. Within the context of security, and because the data plane represents the highest traffic rates, it is critical that the data plane be secured to prevent exception packets from punting to the CPU and impacting the control and management planes

The following sections provide best practices for network hardening.

Management Plane

- Dedicated out-of-band network should be deployed throughout the plant including the IDMZ.
- The AAA framework should be implemented, which is critical in order to secure interactive access to network devices and provides a highly configurable environment that can be tailored based on the needs of the network.
- ACLs should be enforced to prevent unauthorized direct communication to network devices.
- Configure secure networking protocols, such as SSH and SNMP v3, for access to the networking equipment.
- Network system logging should be enabled throughout the architecture.
- All network device configuration should be backed up after initial installation, setup, and following modifications.

Control Plane

Most routers and switches can protect the CPU from DoS-style attacks through functionality equivalent to Control Plane protection or policing.

Switches

- Within switched networks, it is important to protect the overall switched network from instability. Mechanisms are deployed in these types of networks to protect the integrity of the Layer 2 switched domains. For example, STP can be used within these switched domains to help maintain a loop free topology in a redundant Layer 2 infrastructure. Within Layer 2 networks, root devices exist that help provide information about the stability of the network. Guard mechanisms need to be configured so that these root devices are not changed. Bridge Protocol Data Units (BPDU) Guard and Root Guard are examples that should be configured to help protect the Layer 2 domain and prevent Spanning Tree instability.

Router/Routing Protection/Layer 3 Switches

- Neighbor Authentication - When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted device.
- Routing Peer Definition - The same dynamic peer discovery mechanisms that facilitate deployment and setup of routers can potentially be used to insert bogus routers into the routing infrastructure. Disabling such dynamic mechanisms by statically configuring a list of trusted neighbors with known IP addresses prevents this problem. This can be used in conjunction with other routing security features such as neighbor authentication and route filtering.
- Control Plane Policing or Protection - This option should be configured to help protect routing sessions by preventing the establishment of unauthorized sessions, thus reducing the chances for session reset attacks.

Data Plane

- Unused ports — Place any ports not being used into a shutdown state. For the purpose of a switch, add the switchport VLAN command with an unused VLAN (not VLAN 1) so that if a port is accidentally activated, it will not affect any deployed VLANs.

- Port security limits the number of MACs on a particular interface. This helps to prevent threats such as MAC attacks. Port security should be enabled on switch access ports.
- DHCP snooping – If servers or workstations in the architecture are using DHCP, then DHCP snooping and Dynamic ARP Inspection (DAI) should be considered.
- Traffic Storm Control – A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature can be used to prevent disruptions on Ethernet interfaces by a broadcast, multicast, or unknown unicast traffic storm.

VLAN Best Practices

- Disable all unused ports and put them in an unused VLAN. Any enabled open port provides an access medium into the network.
- Do not use VLAN 1 for anything. VLAN 1 is the default VLAN and is enabled on all ports by default; therefore, it is a security best practice to configure all the ports on all switches to be associated with VLANs other than VLAN 1.
- To assist with preventing VLAN hopping attacks, whereby an end station can spoof as a switch, configure all user-facing ports as non-trunking. Force tagging for the native VLAN on trunks and drop untagged frames to assist with preventing VLAN hopping.
- Use VTP transparent mode
- Explicitly configure trunking on infrastructure ports. For ports connecting switches, trunking is used to extend VLANs throughout the network. Explicitly configure only the VLANs required to be extended to other switches.

Note: DHCP snooping or Dynamic Advance Resolution Protocol (ARP) inspection utilizes IP Device Tracking. Certain industrial environments are susceptible to issues when IP device tracking is enabled. Follow the design best practices for IP device tracking as detailed later IPDT Considerations, page 79.

Cell Area Zone Security Framework

Cisco offers a comprehensive set of security tools to help secure industrial environments. These tools must be used in a basic security framework. This involves Visibility, segmentation, detection and then remediation.

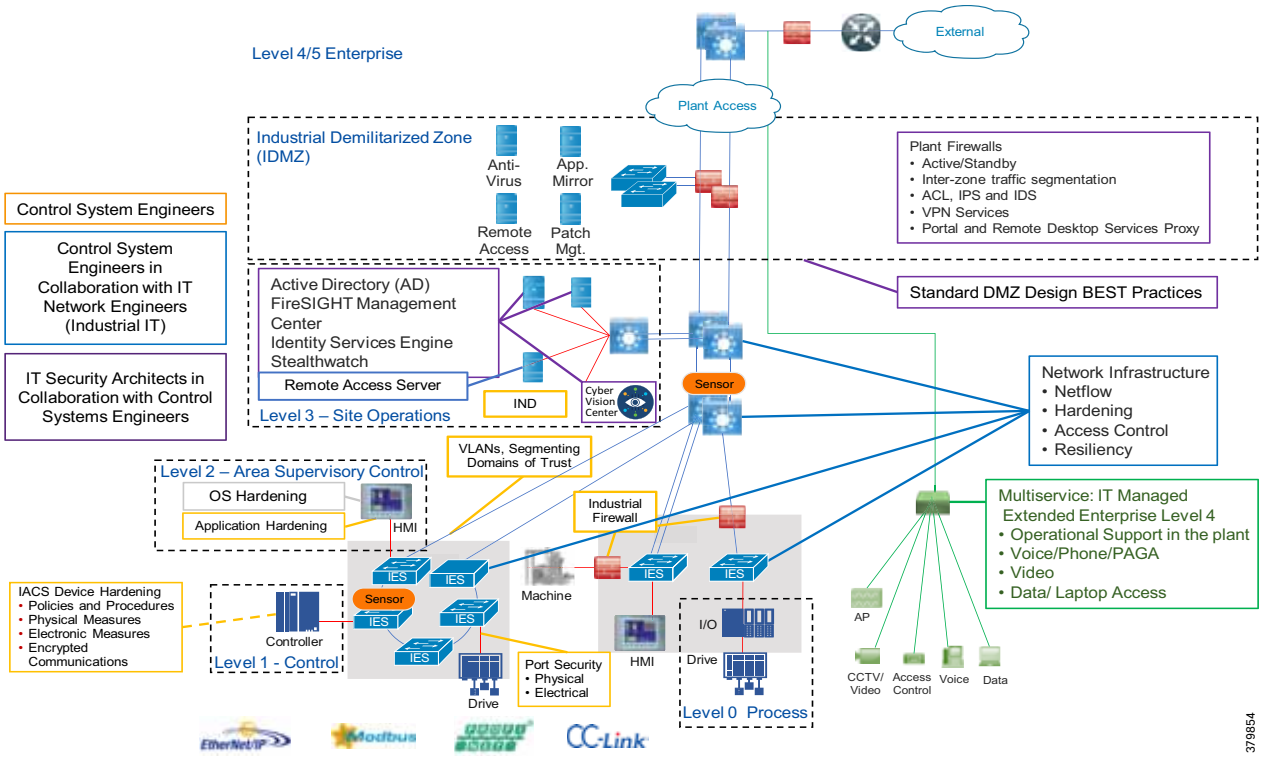
- Visibility - Gain visibility of all IACS devices present o a plant floor. Knowing what is present and active in a network will be vitally important to designing a policy which controls device communication. Understanding the vulnerabilities of the connected assets will also contribute to defining the security policy and architecture.
- Segmentation - Restrict Dataflow and communications of devices on the plant floor. Various techniques can be enabled to prevent the spread of any security incident and also ensure device communications is only between those defined in the security policy.
- Detection - Detecting incidents in a network malware spreading in a network—One behavior of the PLC blaster worm is to scan the network and discover other vulnerable devices. The key defense strategy is to discover that a scan is happening in the network and plan a remediation action plan.
- Remediate - Remediate any issues or incidents that are encountered. Build this into a security plan and continually assess update the security policy framework and procedures.

The design guide highlights the Design and recommendations.

Plantwide Security Reference Architecture

The following figure is a high level representation of the Site-wide view of security.

Figure 30 Industrial Automation Cell/Area Zone Network Security



The CPwE CVD defined personae for the security architecture defined applies potentially to mining too. The following provides details aligned with the figures above.

- Control System Engineers (highlighted in tan)–IACS asset hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network monitoring and change management, network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, and IACS application AAA.
- Control System Engineers in collaboration with IT Network (highlighted in blue)–Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), network monitoring and inspection, and wired and wireless LAN access policies.
- IT Security Architects in collaboration with Control Systems Engineers (highlighted in purple)–Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant firewalls, and IDMZ design best practices.

Standardization plays an important role in helping to provide an overall security strategy to align people process and technology. A security risk assessment is a key step and will help define which systems are critical control, non-critical control, and non-operational to assist with defining an overall security architecture while still meeting business and safety requirements. Risk assessment guidelines are provided in IEC 62443-3-2. Once the risk has been assessed, foundational security requirements as defined in IEC 62443-3-3 can provide guidance in securing the industrial control system. The DIG for the Industrial Automation program aligns with these foundational requirements:

- FR1 Identification and Authentication Control–Identify and authenticate all users (humans, software processes, and devices) before allowing them to access to the control system.
- FR2 Use Control–Enforce the assigned privileges of an authenticated user to perform the requested action on the IACS and monitor the use of these privileges.
- FR3 System Integrity–Ensure the integrity of the IACS to prevent unauthorized manipulation.

- FR4 Data Confidentiality-Ensure the confidentiality of information on the communications network and in storage. This may include methods such as segmentation, protecting against unauthorized access, and data encryption.
- FR5 Restricted Dataflow - Use segmentation and zones to provide isolation for each environment and conduits to limit the unnecessary flow of data between zones and architectural tiers.
- FR6 Timely Response to Events - Manage, monitor, log, and control the security of the infrastructure to identify, defend, and prevent any security threats or breaches including management audit, logging, and threat detection.
- FR7 Resources Availability - Ensure the availability of the control system against the degradation or denial of essential services.

System Components

Cisco Cyber Vision

Cisco Cyber Vision is a cybersecurity solution specifically designed for industrial organizations such as mining to ensure continuity, resilience, and safety of their industrial operations. It provides asset owners with full visibility into their IACS networks so they can ensure operational and process integrity, drive regulatory compliance, and enable easy deployment within the industrial network. Cisco Cyber Vision leverages Cisco industrial network equipment to monitor industrial operations and feeds Cisco IT security platforms with OT context to build a unified IT/OT cybersecurity architecture.

Cisco Cyber Vision provides three key value propositions:

- Visibility embedded in your Industrial Network—Know what to protect. Cisco Cyber Vision is embedded in your Cisco industrial network equipment so you can see everything that connects to it, enabling customers to segment their network and deploy IoT security at scale.
- Security insights for IACS and OT—Continuously monitor IACS cybersecurity integrity to help 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 SOC to the OT domain.

Primarily Cisco Cyber Vision is an asset inventory, network monitoring, and threat intelligence platform specifically designed to secure IACS. It is embedded into the Cisco 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 so they can work together on network segmentation, threat detection, and remediation to ensure continuity, resilience, and safety of their industrial operations.

Cisco Identity Services Engine

Cisco ISE is a security administration product that enables an OT-IT security administrative team to create and enforce access level security policies. One of the salient features of Cisco ISE is profiling services, detecting and classifying endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to pre-built or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Blackberry phones, and so on), desktop operating systems (for example, Windows 7, Mac OS X, Linux, and others), and numerous non-user systems such as printers, phones, cameras, and game consoles.

However, for IACS assets, the ISE built-in probes will not be able to get all the information from the IACS asset to create a granular profiling policy because IACS assets may not support some traditional IT protocols that ISE relies on to profile the device. To gain visibility of IACS assets, Cisco Cyber Vision interfaces with Cisco ISE using Cisco pxGrid, which is an open, scalable, and IETF standards-driven data sharing and threat control platform to communicate device information through attributes to ISE.

Using Cisco ISE, an IT security professional can create consistent security policies across the breadth of the entire network, making it the policy engine for users and assets that require access to the network. ISE shares user, device, and network details through pxGrid with partner platforms so that the other platforms can enhance their security policy. For example, Cisco Cyber Vision can also take in information from other platforms through pxGrid to enhance security visibility and context. Cisco Cyber Vision can communicate with pxGrid to share discovered device details for profiling context. Cisco ISE can also reduce risks and contain threats by dynamically controlling network access.

For more information about Cisco ISE see the Cisco ISE Overview:
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~stickynav=1

StealthWatch

Cisco StealthWatch improves threat defense with network visibility and security analytics. Cisco StealthWatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network, so they can quickly and effectively respond to threats. StealthWatch leverages NetFlow, IPFIX, and other types of flow data from existing infrastructure such as routers, switches, firewalls, proxy servers, endpoints, and other network infrastructure devices. The data is collected and analyzed to provide a complete picture of network activity.

With in-depth insight into everything going on across the network, you can quickly baseline your environment's normal behavior, regardless of your organization's size or type. This knowledge makes it easier to identify something suspicious.

Use cases for deploying in industrial plants include:

- Continuously monitor the extended network
- Detect threats in real-time
- Speed incident response and forensics
- Simplify network segmentation
- Meet regulatory compliance requirement
- Improve network performance and capacity planning

For more information see:
https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/at-a-glance-c45-736510.pdf

Visibility is the first step to securing the infrastructure: Deploying Cisco Cyber Vision and StealthWatch

Cisco Cyber Vision can really provide assistance to OT/IT teams with providing visibility into industrial assets connected to the industrial networks. Generally, there is a lack of confidence in having a complete understanding of what is connected to the Network. Providing asset discovery and threat awareness of assets on the industrial network is the first step in understanding risk awareness and helping to define security policies and a security framework across a mine. This provides an understanding of deploying Cisco Cyber Vision in the PCN mine networks.

Cisco StealthWatch can provide visibility into the flows within the network and with in-depth insight into everything going on across the network, you can quickly baseline your environment's normal behavior, regardless of your organization's size or type.

This section surveys the deployment guidelines for implementing Cisco Cyber Vision and Cisco Stealth Watch.

Cisco Cyber Vision

Cisco Cyber Vision has two primary components: Center and Sensor. The Sensor uses deep packet inspection (DPI) to filter the packets and extract metadata, which is sent to the Center for further analytics. Deep packet inspection is a sophisticated process of inspecting packets up to the application layer to discover any abnormal behavior occurring in the network. The Sensor sends only metadata information to the center, which prevents loading the network traffic.

Cisco Cyber Vision Center

Cisco Cyber Vision Center is an application that can be installed as a virtual machine or as a hardware appliance. The Center provides easy-to-follow visualization that allows an OT operator to gain visibility into the network infrastructure.

- Dynamic inventory – Cisco Cyber Vision Center generates a dynamic inventory of all the IACS devices on the plant floor. The Cisco Cyber Vision Sensor continuously listens to the events happening on the plant floor, thereby allowing the Cisco Cyber Vision Center to build and update the dynamic inventory of the devices in the plant floor. The OT operator does not need to perform any scans to get the list of current devices on the plant floor. Also, when a particular device goes offline, the Cisco Cyber Vision Center updates its list dynamically.
- Intuitive filters – Cisco Cyber Vision Center provides intuitive filters labeled as presets to help an OT operator to look examine data. For example, an operator may want to look at the current list of OT components or process control activities. The Center allows the operator to construct custom filters.
- Detailed IACS asset information – One of the significant advantages of the Cisco Cyber Vision solution is the ability to glean very detailed information about IACS assets.
- Dynamic maps – Cisco Cyber Vision Center provides very detailed maps that display the components and the communication flows between them.
- Baselining – Cisco Cyber Vision Center supports a feature called baselining, which allows an operator to select a set of components to monitor. After a baseline is defined, the operator can compare the changes that happened to this set of elements at different time instants.
- Vulnerability management – Cisco Cyber Vision Center highlights vulnerabilities that are present in IACS devices, which helps an operator to mitigate those vulnerabilities.
- Reports – Cisco Cyber Vision allows an operator to generate reports such as inventory, activity, vulnerability, and PLC reports.

Cisco Cyber Vision Sensor

In this guide, the Cisco IC3000 with Cisco 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, the management interface is used to transport the sensor information to the Cisco Cyber Vision Center; the four interfaces are used for data collection from SPAN networks.

Deployment Considerations

This section discusses the critical design considerations that must be taken into account while deploying Cisco Cyber Vision solutions in industrial automation environments. The Cisco Cyber Vision solution supports two deployment models: offline mode and online mode.

Cisco Cyber Vision Offline Mode

Cisco Cyber Vision offline mode is deployed 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. In these situations, the OT engineer can use offline mode, which involves capturing the data packets using a USB stick and then later

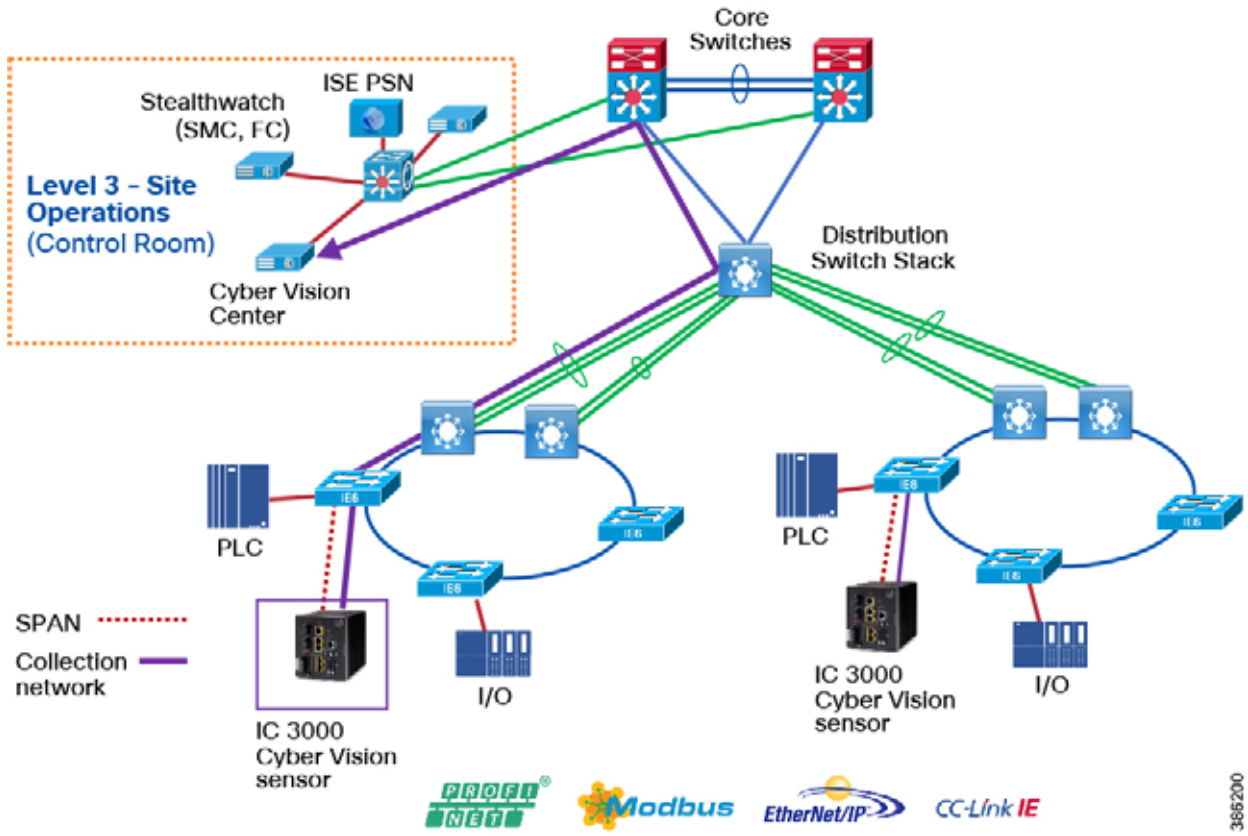
analyzing them by manually loading them in the Cisco Cyber Vision Center. This option is used by an OT engineer to perform a proof of concept. Generally this isn't scalable to provide full visibility of assets especially across the breadth of the mining operational domain.

Cisco Cyber Vision Online Mode

Cisco Cyber Vision online mode assumes that there is Layer 3 connectivity between the Cisco Cyber Vision Sensor and the Cyber Vision Center. The sensor will pass meta data to the Cyber Vision Center in real time as assets and vulnerabilities are discovered or detected. In this guide, we recommend customers use online mode for the following reasons:

- Online mode ensures that the OT and IT operations teams get a continuous visibility of traffic in real-time.
- There is no manual process of capturing the data and uploading the data as discussed in offline mode. The data is captured in real-time at the Cisco Cyber Vision Center.
- Offline mode depends on the available storage space of the USB disk and cannot be used as a solution for long term storage of the data.

Figure 31 Online Mode in Cell/Area Zone



As shown in Figure 31 Cisco IC3000 is deployed with Cisco Cyber Vision and has two distinct set of interfaces: collection interface and mirror interfaces. The collection is a Layer 3 interface that is used to transport the sensor metadata to the Cyber Vision Center. The mirror interfaces collect the SPAN traffic in the network.

Performance

The control system engineer deploying Cisco IC3000 must take into account its performance numbers. The critical performance metrics are:

- The number of flows supported for a single Cisco IC3000 is 15,000.
- The maximum number of packets per second is 12,000.

Capture Points

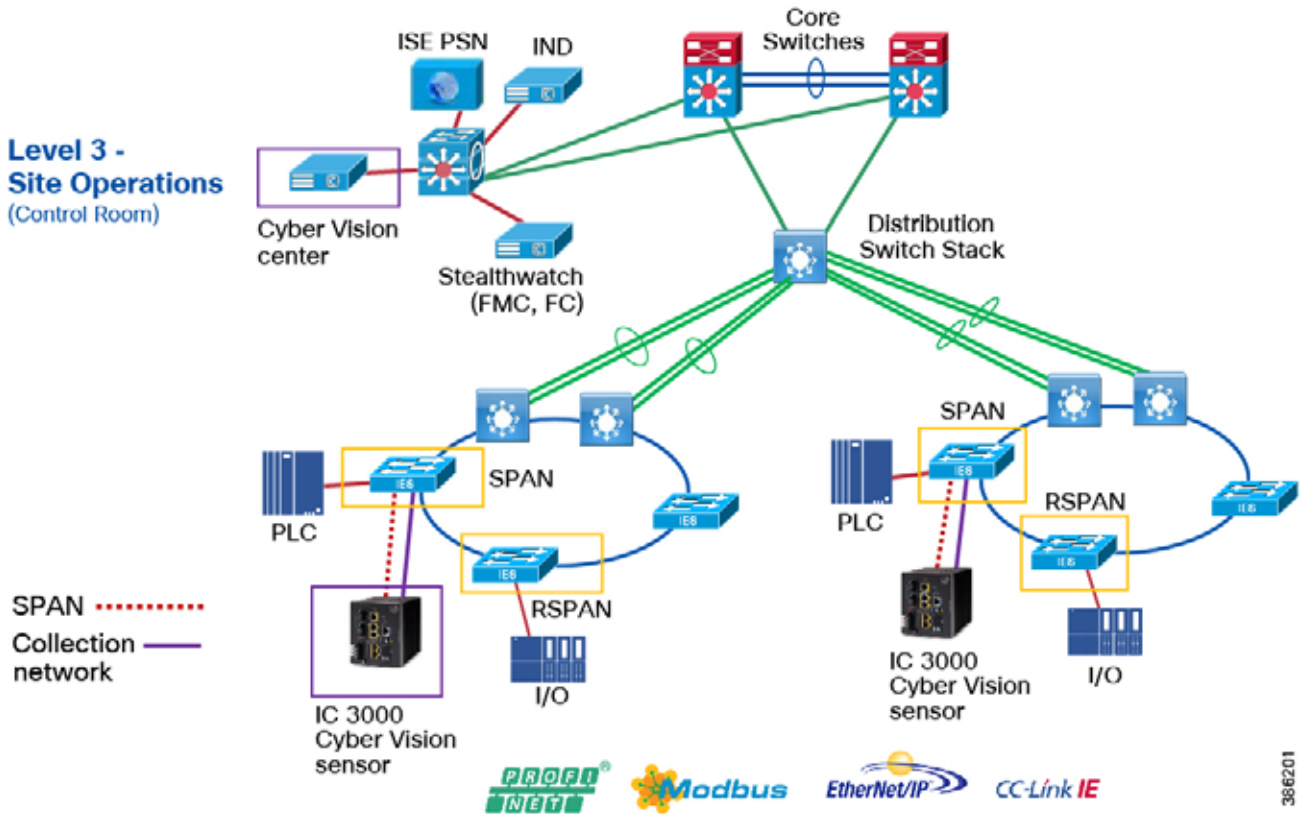
The effectiveness of the Cisco Cyber Vision solution depends on effectively capturing traffic, so deciding where to capture traffic is critical. For example, if there are many IACS devices attached to several switches in the network, and if you want to monitor the traffic from all those devices, then you have three choices:

- Enable RSPAN on all switches.
- Enable individual SPAN on each of the switches to be monitored and connect them to a specific span aggregation switch. Selectively RSPAN the span traffic from that switch to the Sensor and then you can selectively monitor the traffic
- RSPAN/SPAN enabled at selective points in the network.

Neither of these methods are ideal for discovering the assets within the mine process control networks. Enabling RSPAN on all switches should be carefully monitored as to not oversubscribe the network or network platform resources with RSPAN traffic and impact the critical process control traffic. A separate SPAN network traversing the breadth of the mine would be cost prohibitive and not practical.

Configuring RSPAN at selective and optimal points over a period of time, selectively turning on the RSPAN at different switches in the network to provide initial visibility of assets and vulnerabilities would help with the initial asset visibility and baseline assessment. The most critical traffic on the plant floor is communication from the PLC to other devices on the plant floor and most security attacks would probably exploit vulnerabilities in the PLC. This model could continuously monitor these critical assets post ongoing visibility assessments after discovery of all the essential assets.

Figure 32 Enable SPAN/RSPAN in the Cell/Area Zone

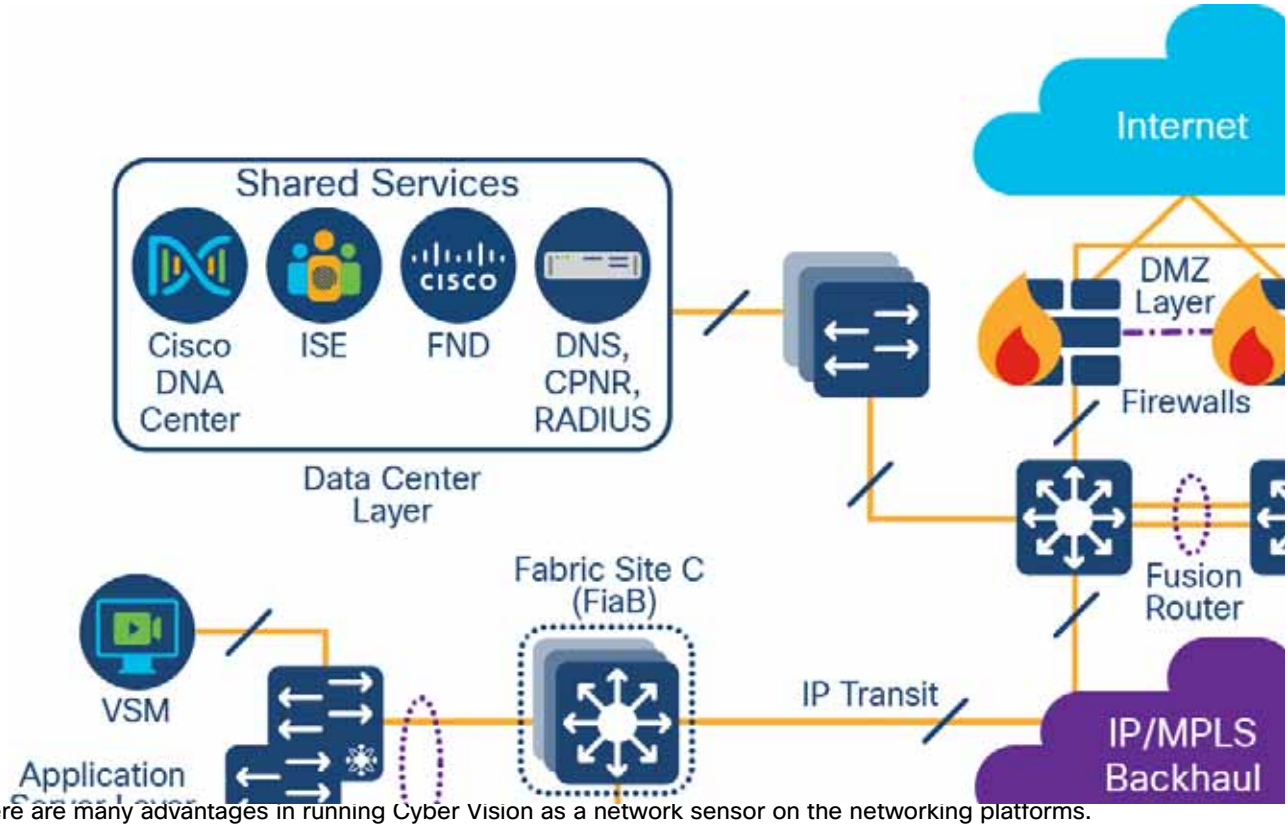


The design depicted in Figure 32 should be done carefully such that the RSPAN traffic should not affect the regular process control traffic. In the figure above, the IC3K Cyber Vision Sensor is attached to a switch. Now, to monitor traffic coming from an IO device or other assets on a remote switch then RSPAN can be enabled on the switch where asset is attached to it. This ensures IC3K Cyber Vision sensor is able to gain visibility of all the IACS devices in the Cell/Area Zone. As highlighted earlier this practice must be carefully planned as RSPAN can cause un-necessary increase in the traffic.

Use Cyber Vision Network Sensor in IE3400 switch

The ideal scenario is to embed the network sensor into the network infrastructure. Cisco IE3400 switches support a capability of running Cyber Vision Sensor as IOx application within the switch. The IOx application running in the Cisco IE3400 supports a feature known as ERSPAN. This feature passes the traffic that needs to be monitored directed towards the IOx application running in the IE3400 switch. The Cyber Vision Sensor application processes the data and sends the meta data to the Cyber Vision Center. The functionality of the network sensor is similar to hardware sensor except that instead of running in the IC3000 it runs directly in the IE 3400 switch. Deploying in The following diagram shows this architecture:

Figure 33 Cyber Vision Network Sensor in IE3400 switch



There are many advantages in running Cyber Vision as a network sensor on the networking platforms.

- There is no need to install any extra external hardware across the mine process control networks.
- Much simpler, faster & cheaper than sourcing/deploying/managing dedicated appliances and a separate SPAN network.
- There is no need to run RSPAN at a different switches in the Cell/Area Zone which can affect the network and impact control process traffic.
- Cyber Vision DPI engine on the sensor extracts only the information it needs to build inventories & threat detection, this meta data sent to the Cyber Vision Center represents only a minor percentage of network traffic conserving bandwidth and not impacting network performance.

Note Cyber Vision network sensor on the IE3400 has not yet been validated. This is an impending feature to be released in the near future.

Cisco NetFlow and StealthWatch

Cisco NetFlow

The Cisco IE 3400, Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, and Cisco Catalyst 9300 support full Flexible NetFlow. NetFlow is an embedded instrumentation within Cisco software to characterize network operation. It provides visibility into the data flows through a switch or router. Enabling NetFlow provides a trace of every data conversation in the network without the need for any SPAN ports. Cisco StealthWatch can use Cisco NetFlow for network flow analysis contributing to establishing a baseline of normality in the network and security analysis such as malware detection and anomaly detection.

Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets.

Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes. IP packet attributes used by NetFlow:

- IP source address
- IP destination address
- Source port
- Destination port
- Layer 3 protocol type
- Class of Service
- Router or switch interface

All packets with the same source and destination IP address, source and destination ports, protocol interface, and class of service are grouped into a flow and then packets and bytes are tallied and stored in the NetFlow cache. The cache can then be exported to a system such as Cisco StealthWatch where deeper analysis of the networking data can be used to identify threats or malware.

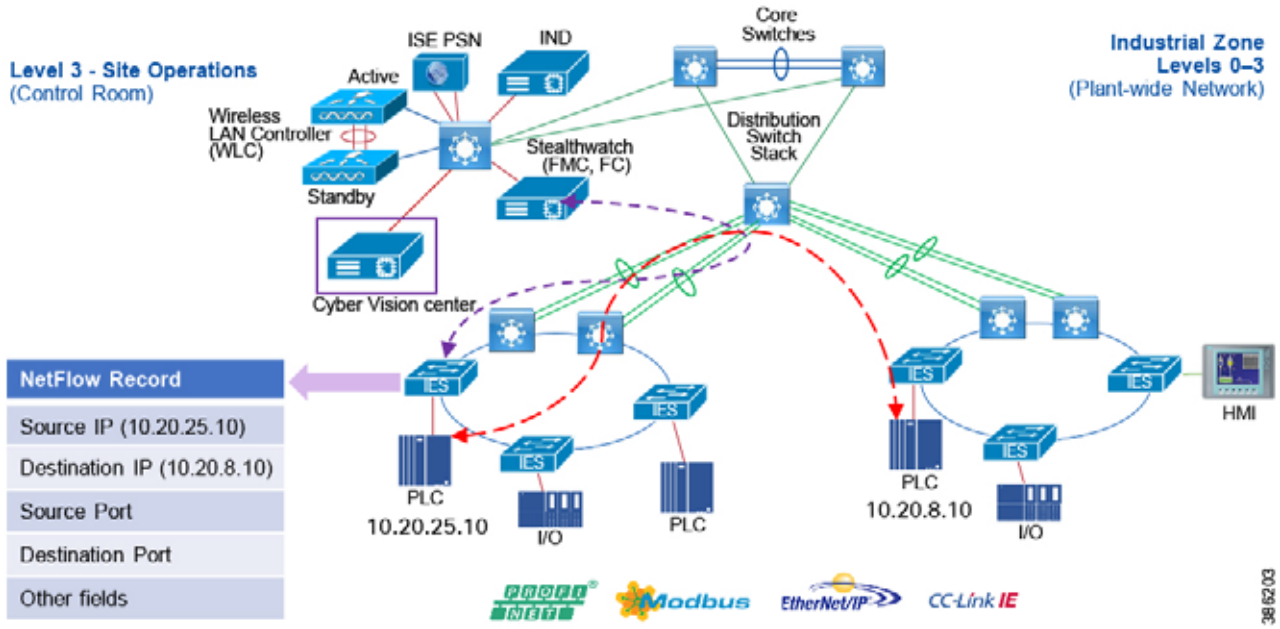
NetFlow Data Collection

A flow is a unidirectional connection between a source and a destination. To describe a full exchange between two devices, two independent unidirectional flows are needed. For example, when data is flowing between client and server, then there are two flows occurring: from client to server and from server to client. NetFlow is a protocol that creates flow records for the packets flowing through the switches and the routers in a network between the end devices and exports the flow records to a flow collector. The data collected by the flow collector is used for different applications to provide further analysis. Initially, NetFlow was used for providing traffic statistics in a network, but later it started gaining traction as a network security tool. In the Industrial Automation Network Security CVD, NetFlow is primarily used for providing security analysis, such as malware detection, network anomalies, and so on. There are many advantages in deploying NetFlow:

- NetFlow can be used for both ingress and egress packets.
- Each networking device in a network can be independently enabled with NetFlow.
- NetFlow does not see a separate management network to collect the traffic.

Note: Within the mining reference architecture the export of the data would need to flow to the network operations and security VRF, from a management VRF. This has not been validated as part of this design and platform capabilities and understanding of the management interfaces in a VRF should be considered.

Figure 34 NetFlow Data Collection



With the latest releases of NetFlow, the switch or router can gather additional information such as ToS, source MAC address, destination MAC address, interface input, interface output, and so on. For Cisco Cyber Vision and ISE integration, collecting the MAC address of the device is very critical.

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the StealthWatch Flow Collector. A flow is ready for export when it is inactive for a certain time (for example, no new packets are received for the flow) or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download and the standard CIP/IO connections). There are timers to determine whether a flow is inactive or a flow is long lived.

After the flow time out the NetFlow record information is sent to the flow collector and deleted on the switch. Since the NetFlow implementation is done mainly to detect security-based incidents rather than traffic analysis, The recommended timeout for the Cisco IE 4000, Cisco IE 4010, Cisco IE 5000, and Cisco Catalyst 9300 switches is 60 seconds for the active timeout and 30 seconds for the inactive timeout. For the Cisco IE 3400, the active is 1800 seconds, the inactive is 60 seconds, and the export timeout is 30 seconds.

The next consideration is on enabling NetFlow in the network. This guide recommends using NetFlow for security, therefore the recommendation is to enable NetFlow monitoring on all the interfaces in the Industrial Automation network.

StealthWatch Deployment Considerations

The main components of the StealthWatch system are:

- Flow Collectors
- StealthWatch Management Console

Note: The respective systems reside on different virtual or hardware appliances.

The Flow Collector collects the NetFlow data from the networking devices, analyzes the data gathered, creates a profile of normal network activity, and generates an alert for any behavior that falls outside of the normal profile. Based on the network flow traffic, there could be one or multiple Flow Collectors in a network. The StealthWatch Management Console (SMC) provides a single interface for the IT security architect to get a contextual view of the entire network traffic.

The SMC has a Java-based thick client and a web interface for viewing data and configurations. The SMC enables the following:

- Centralized management, configuration, and reporting for up to 25 Flow Collectors
- Graphical Charts for visualizing traffic
- Drill down analysis for troubleshooting
- Consolidated and customizable reports:
  - Trend analysis
  - Performance monitoring
  - Immediate notification of security breaches

Some important considerations when deploying a Steathwatch system include:

StealthWatch is available as both hardware (physical appliances) and virtual appliances. To install hardware and software appliances, refer to the StealthWatch guide:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

The resources allocation for the StealthWatch Flow Collector are dependent on the number of flows per second expected on the network and the number of exporters (networking devices that are enabled with NetFlow) and the number of hosts attached to the each networking device. The scalability requirements for the Flow Collector are available at:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

The data storage requirements must be taken into consideration, which are again dependent on the number of flows in the network. The sizing table for data storage is available at:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

A specific set of ports needs to be open for the StealthWatch solution in both the inbound and outbound directions. For the complete list of ports that are recommended to be open, refer to:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

Restricted Data Flow using Segmentation and Zoning

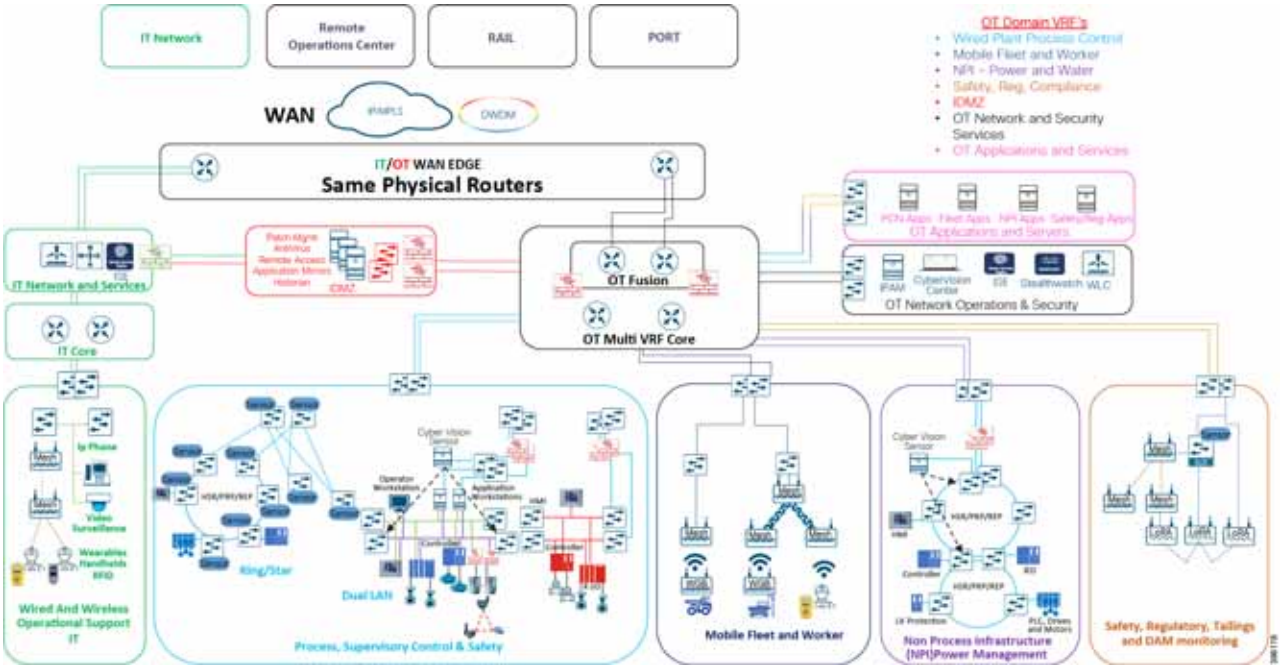
Segmentation is a key component to creating zones of trust to help protect IACS networks and processes. IEC 62443 details restricted data flow recommendations to segment the control system into zones and conduits to limit the unnecessary flow of data between process networks or services. Segmentation can be physical or logical. Ideally physical segmentation of operating domains within the mine will help contribute to a better security posture, however in the majority of instances this is not practical or economically feasible. Therefore logical segmentation techniques over a shared infrastructure are the focus of this document based on risk and the policy framework typical of a mine environment.

Traffic Flows – Inter VRF and Intra VRF

Traffic flows as described in the Cell/Area Zone Traffic Patterns and Considerations highlight inter zone and intra zone traffic. Real-time control predominantly within the cell and non-real time communications northbound, typically informational in nature and would flow between workstation or server in Level 3 operations and devices in Levels 0-2.

The design primarily distinguishes between inter-VRF traffic and intra-VRF traffic. The design described here for the cell area zone fits into this model and is described in Mining Solution Overview and Use Cases. As a reminder the high level architecture figure highlights the different operational domains and shared service domain across the mine site. These domains are separated using VRFs as the primary mechanism for segmentation. Any traffic traversing between a VRF domain will pass to the fusion routers and if deployed through firewalls providing IDS functionality. An example would be between the Shared OT network Operations and Security VRF and the Process control network, another may be between the OT applications VRF and the Process control network within levels 3 and levels 0-2 (PCN/control).

Figure 35 Mine Site Architecture - Logical Domains



Note the figure depicts different domains from a logical perspective rather than a physical perspective. The same physical distribution and access switches may connect networking and equipment from multiple domains. In smaller mines OT/IT services may be forced to use the same physical network infrastructure. The use of this segmentation architecture fully supports this requirement.

Traffic deemed part of the same domain such as all process control network and supervisory control will remain within the VRF and could utilize VLANs, ACLs, OT firewalls and TrustSec to provide segmentation and restricted data flows. Intra VRF/domain traffic will be the primary focus of the design for segmentation in the cell area zone and is the focus of this document. The VRF design is outside the scope of validation at this time and is shown as the model that this architecture needs to fit into.

Cell Area Zone Segmentation

IT security architects in conjunction with a control system engineer should design an access policy that specifies the East-West and North-South communication flows that must be allowed in an IACS network. In an IACS network, having an open policy that allows every IACS asset to communicate with every IACS asset is convenient, but that approach increases the risk of cyber threat propagation. On the other hand, implementing a restrictive policy that does not allow any inter Cell/Area Zone communication is also counterproductive because certain IACS assets need to access other IACS assets that exist in different Cell/Area Zones. Since the exact requirements of a particular scenario are based on the current IACS application requirements, specifying a policy that would work for all the deployments is not possible. Hence in this guide, an access policy example is shown that can be customized for use in different environments. The following assumptions about the access policy for an IACS network are detailed below.

- All the traffic within the Cell/Area Zone is implicitly permitted because it is assumed that a Cell/Area Zone is formed because a group of IACS assets need to communicate with each other, so no enforcement is applied to any IES in the Cell/Area Zone.
- All the traffic between any two different Cell/Area Zones will be enforced. As an example, would be interlocking controller communication across a cell zone boundary.

Historically, Access Control Lists (ACLs) and dynamic ACLs (dACLs) have been used to restrict data flows as well as OT firewalls in networks. The primary disadvantage with ACLs and dACLs is that they are associated or bound to an IP address or range of IP addresses. This can require changing ACLs whenever an IP address changes or new asset with a new IP address is added to the network. Managing this mechanism network-wide potentially results in large access control lists that are prone to misconfiguration and difficult to maintain and manage. Large ACLs may impact the switching performance of the distribution switch.

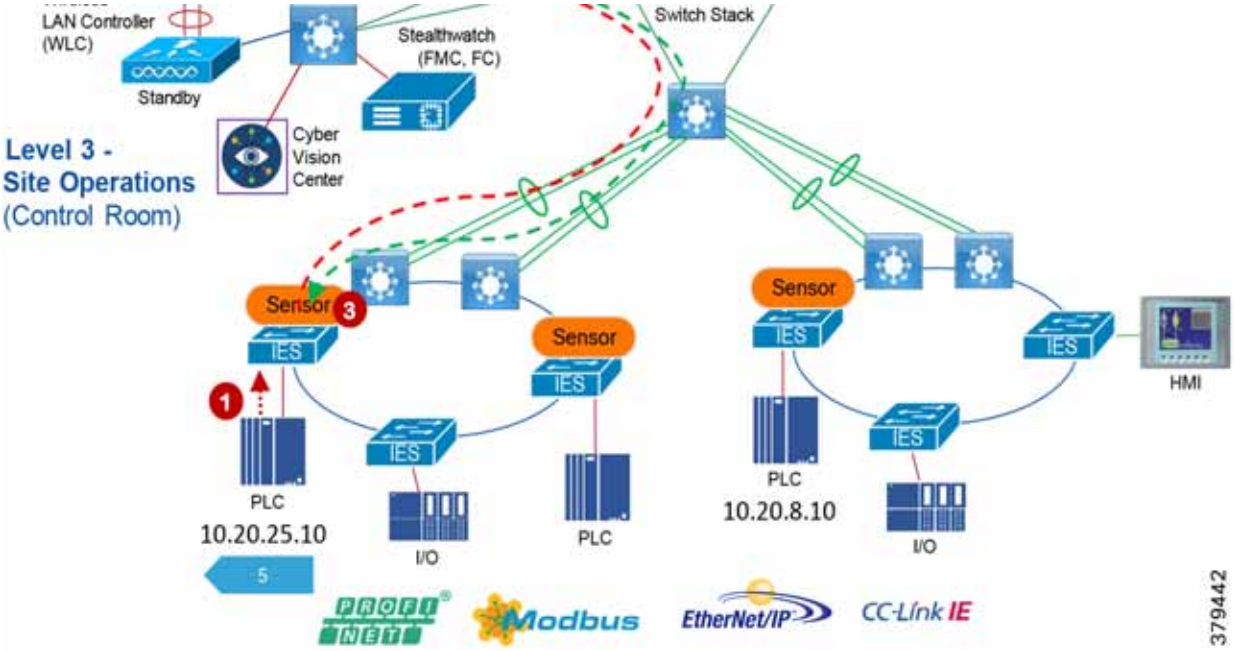
Cisco TrustSec with SGT has advantages over ACL or dACL that make them more scalable and easier to manage. Users or devices are based on context such as a user role, device type or location and this is expressed within a security Group. SGTs are applied to user or device on access to the network and then network devices such as routers switches and firewalls use these tags as part of SGACLs to administer the policy and filtering decisions. This SGT is not bound to a specific IP and therefore makes it easier to manage and maintain throughout an infrastructure. This design guide highlights the design considerations and validation of Trustsec technology within the Process control layer levels 0-2 based on the policy definition and traffic flows described earlier in this section.

Cell/Area Zone Segmentation using TrustSec Technology Overview

Cisco TrustSec technology assigns SGTs to all data flows from IACS assets, networking devices, and users when they attach to a network. By using these tags, an IT security architect can define an access policy and enforce that policy through the network.

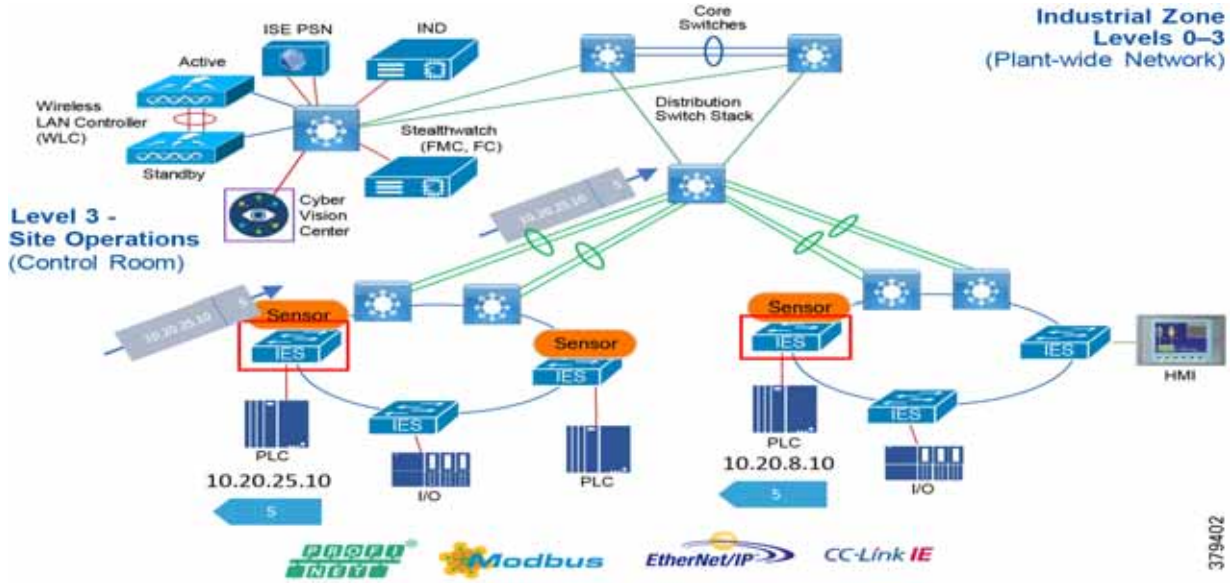
Cisco TrustSec is defined in three phases: classification, propagation, and enforcement. When the users and IACS assets connect to a network, the network assigns each entry a specific SGT based on the devices classification using method of authentication and authorization.

Figure 36 Cisco TrustSec Device Classification



The next phase of TrustSec is propagation, in which the SGT tag associated with the device is inserted into the ethernet frame of every packet generated from the device and propagated through the network. An example, When an Ethernet frame is generated by the Industrial Asset, the switch inserts the SGT value of (5) along with the IP address and sends it to the next switch. The next switch, if configured with SGT in-line tagging, propagates the same frame to the next switch and this information travels in hop-by-hop fashion to the destination.

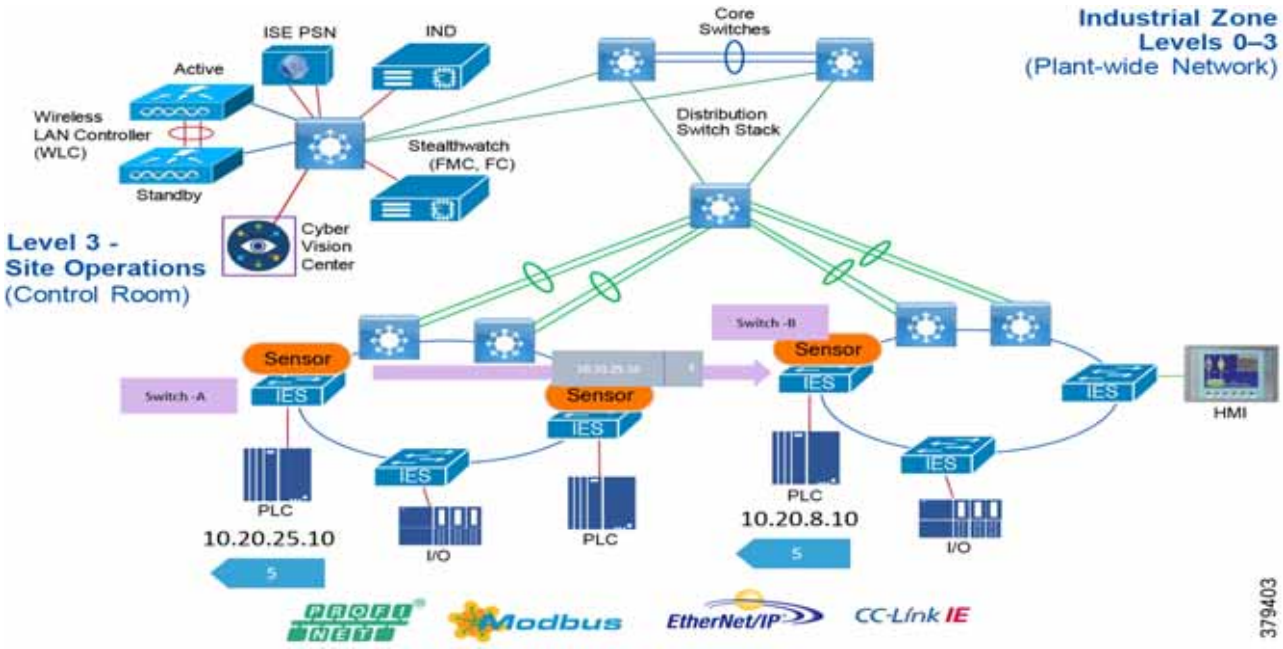
Figure 37 Cisco TrustSec SGT Propagation



In certain network topologies such as mixed switching environments or when looking to upgrade older infrastructure with newer networking, switches in the path from the source to the destination may not support in-line tagging. When that scenario happens, the non-SGT capable switch would ignore the SGT in the frame and would send a normal Ethernet frame on the out-going interface. For in-line tagging feature to work, all the switches in the path must support this feature. Cisco TrustSec also supports a different mechanism to transport SGT frames over a path when a non-SGT capable IES (for example, Cisco IE 2000) is present by using SGT Exchange Protocol (SXP).

The following diagram shows how an SGT is transported over an SXP tunnel between Switch A and Switch B. The Switch B in this diagram derives the source tag from the device attached to itself and the destination tag through an SXP tunnel.

Figure 38 Cisco TrustSec SGT Propagation Using SXP Tunnel



Finally the enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router, or switch. The enforcement device takes the source SGT and compares it to the destination SGT to determine if the traffic should be allowed or denied. The advantage of Cisco TrustSec is that any switch, router, or firewall between the source and the destination can impose the policy, but the key requirement is that the enforcement point must be able to map the destination IP address to the tag value. Therefore the SGACL is at the egress where the destination IP to SGT is known, or if the enforcement point is centralized for example using SXP (provides the networking device with an IP to SGT mapping) to provide this awareness.

The IT architect must consider the following when designing policy enforcement:

- IE Switch platform support for Trustsec Features
- Group Tag definition for the policy matrix

IE switch platform support for Trustsec – legacy

Cisco industrial switches can authenticate the end devices and support the application of a SGT tag. However, certain Industrial Ethernet Switches have two constraints: 1) Lack of inline tagging support, and 2)Lack of policy enforcement support. With these two constraints in mind we move policy enforcement to a different point in the network which is the distribution switch when there are legacy IE platforms in the Cell/Area Zone. In Brownfield deployments our design assumes that the distribution switch stack is a pair of Catalyst 9300 switches and these switches do support policy enforcement. The second constraint is lack of support for inline tagging. And this constraint is addressed by implementing SXP Tunnel from ISE to the distribution switch. When an SGT is assigned to the IACS device after MAB authentication/authorization ISE learns this information in its database. When we configure SXP Tunnel between ISE and the distribution switch then ISE transports this SGT information to the distribution switch using the SXP Tunnel for the distribution layer switch to enforce.

Group Tag definition for the policy matrix

The IE3400 explicitly does not have these limitations and policy enforcement could be deployed at the access layer with IE3400 switches. Special considerations need to be given to the scalability of the number of group and tag definitions and policy requirements for a large number of assets and asset classes across a mine. The IE 4000 and IE 5000 can support policy enforcement and inline tagging at the access layer with the same considerations for group definition and policy enforcement. For example there could be 100s of production zone types such as underground FAN controllers,

conveyor controllers, underground refueling controllers, rock crushers, dewatering plant controllers; the SGT table space will be 100s of entries in the X-and Y-axis of the site policy matrix which could impact the complexity and scalability of the deployment. Leading practice if for the mine-site security model design will need to flow from a formal review of the mine systems process communications and required levels of visibility/control of the assets connected to the mine network

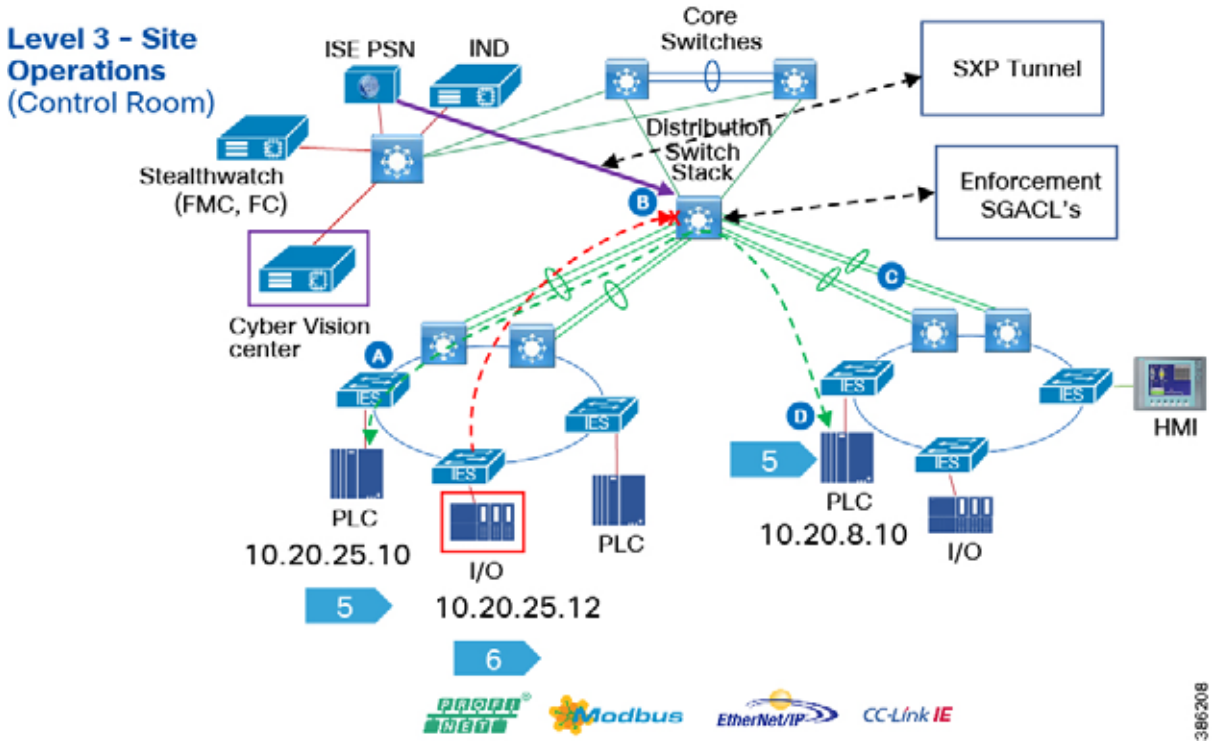
Note: the IE4000/5000 support one SGT per port at the ingress access port if deployed as an enforcement policy point.

Validated Model

The model highlighted as part of this validated design from Industrial Automation keeps the group definition and policy management simple based on specific device types and assumes all traffic within a zone is permitted. It supports brownfield deployments too where legacy IE2000 switches are deployed. The inter cell access is enforced at the distribution layer switches.

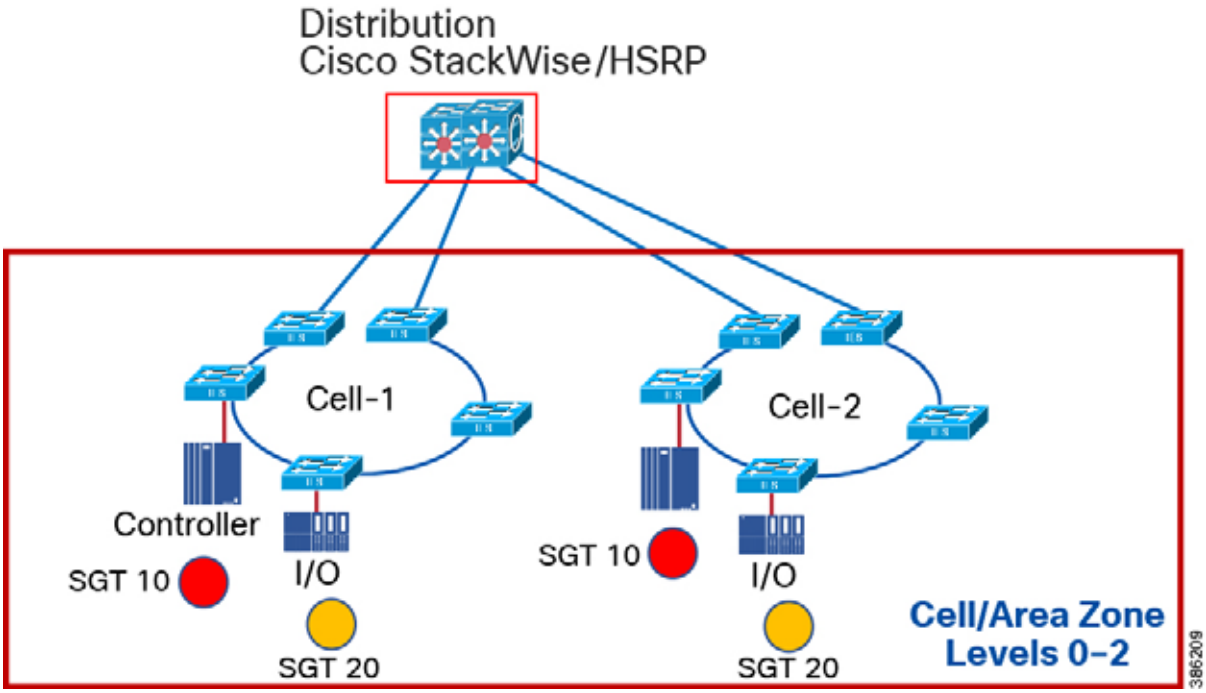
The following diagram shows the policy enforcement at the distribution switch.

Figure 39 Policy enforcement at the Distribution Switch



You will note that Layer 3 is enabled between the access layer and the distribution switch. In the centralized group tag model the Controller group Tag (10) and the I/O group Tag (20) are going to be used across multiple cell area zones. This is highlighted in the figure below. When using layer 2 in the rings intra cell traffic may flow through the distribution layer switches in the rings.

Figure 40 Layer 2 rings SGT issue with Distribution enforcement



If policy dictates that I/O cannot communicate with devices outside of its cell then the policy at the distribution will restrict this. However in a layer 2 ring if legitimate intra cell communication between the Controller and I/O flows through the distribution switches then this traffic will not be permitted as the policy enforcement will restrict this.

In the validated design we connect two of the switches in the Cell/Area Zone to the distribution switch using the L3 ether channel link and we apply policy enforcement at the distribution switch. The policy enforcement applied at the distribution switch not only blocks the inter-cell traffic but allows intra-cell traffic. This happens because the distribution switch is not part of the Layer 2 access, For ring-based topologies, we recommend that customers have Layer 3 network access from two of the switches in the Cell/Area Zone to the distribution switch. The previous figure “Policy Enforcement at the Distribution Switch” highlights this.

Again we do highlight that this is only for this policy enforcement and group tagging model. If policy enforcement is deployed at the access level switches then layer 2 to the distribution can still be deployed with the appropriately designed group tagging model. Though as mentioned earlier this could be challenging due to the number of tags required. For 100’s of production zone types and controllers the SGT table space will be 100s in the X- and Y-axis of a policy matrix which could impact the complexity of the deployment. Again the security model design will need to flow from a formal review of the mine systems process communications and visibility into the assets connected.

TrustSec Network Policy Enforcement Example for Brownfield deployments

The IT security architect must next decide where in the design the access policy should be enforced. For example, consider the case where the policy is enforced on an IES located in the Cell/Area Zone. As stated in the previous section, the basic assumption is that every IACS asset in the Cell/Area Zone must be able to access every other IACS asset. The second assumption is that policies are enforced on East-West communication going across the Cell/Area Zones. For example, there are two Cell/Area Zones, Cell/Area Zone-1 and Cell/Area Zone-2, and each Cell/Area Zone contains a PLC and an I/O device. From a Cell/Area Zone-1 intra-zone policy perspective, every PLC and I/O in Cell/Area Zone-1 must be able to access one another. The inter-Cell/Area Zone security access policy is to block the communication between I/O in Cell/Area Zone-1 to the PLC in Cell/Area Zone-2. This security access policy is shown in the table below.

Table 15 Network Policy Matrix Example

	PLC-Cell/Area-1	I/O-Cell/Area-1	PLC-Cell/Area-2	I/O-Cell/Area-2
PLC-Cell/Area-1	Yes	Yes	No	No
I/O-Cell/Area-1	Yes	Yes	No	No
PLC-Cell/Area-2	No	No	Yes	Yes
I/O-Cell/Area-2	No	No	Yes	Yes

When designing a security policy using TrustSec, associate each IACS asset with a tag. In the example of a PLC with tag 10 and an I/O device with tag 20, two policy tables are needed: 1) Intra_Cell/Area Zone and 2) Inter_Cell/Area Zone.

Table 16 Intra_Cell/Area Zone Access Policy Enforcement Example

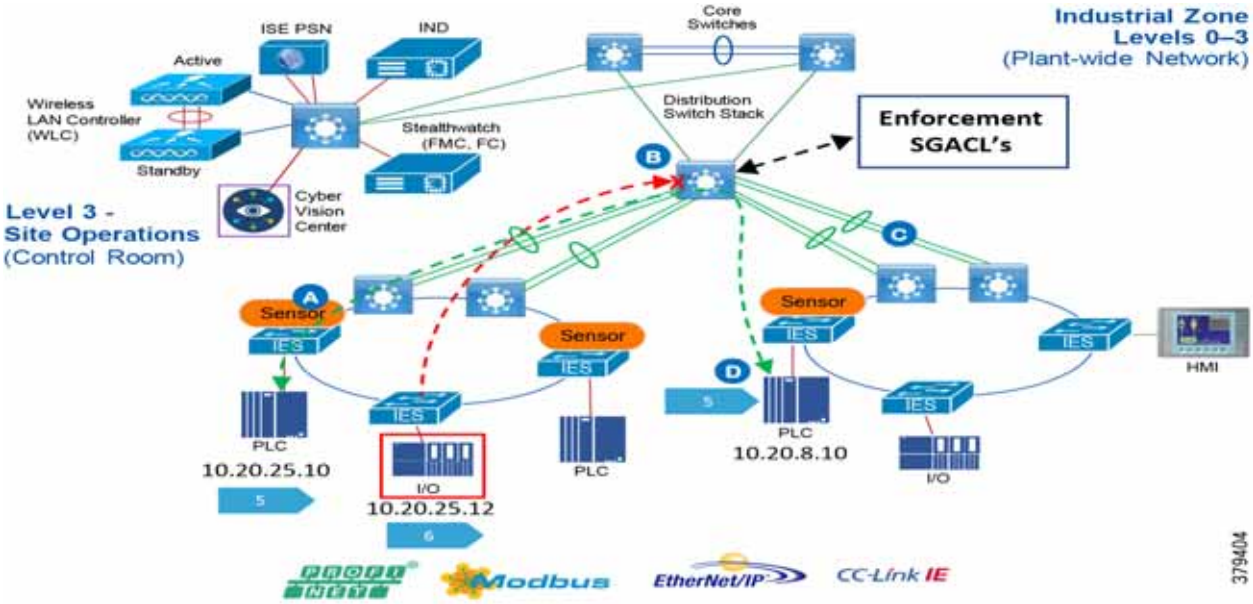
	10	20
10	Yes	Yes
20	Yes	Yes

Table 17 Inter_Cell/Area Zone Access Policy Enforcement

	10	20
10	Yes	No
20	No	No

As seen above, the Cell/Area Zone IES needs to have two tables implemented and that is not possible with the current design. The current TrustSec policy enforcement supports only a single matrix. To ensure both objectives are achieved, implement the security access policy on the distribution switch and do not have any enforcement on the Cell/Area Zone IES. By doing so, the tables policy requirements have been met because when no policy is imposed on the Cell/Area Zone IES, then all the IACS assets within the Cell/Area Zone IES can communicate Figure 41 shows the inter-Cell/Area Zone security access policy enforcement point at the distribution.

Figure 41 Access Policy Enforcement Example



Scalable Group Tag Exchange Protocol Considerations

Scalable Group Tag Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one

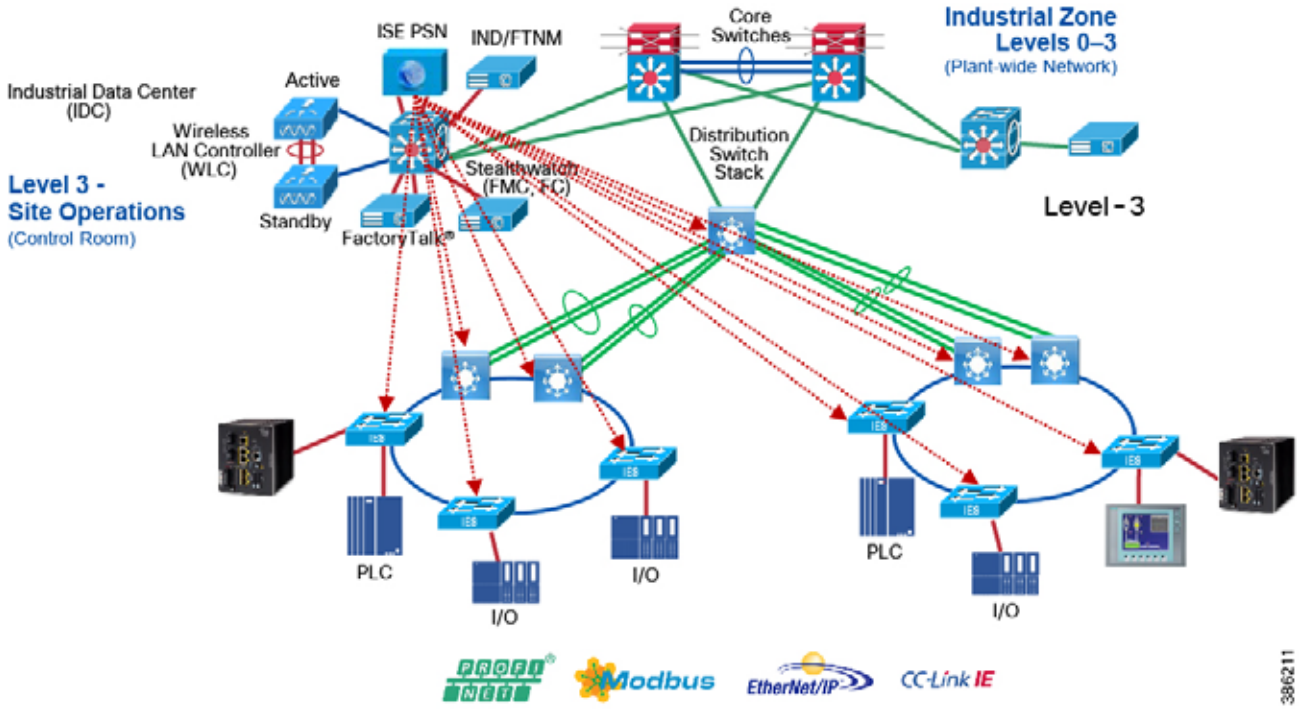
SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up an SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them acts as both speaker and listener. Connections can be initiated by either peer, but mapping information is always propagated from a speaker to a listener.

As shown in the previous section, the enforcement is moved to the distribution switch, so the distribution switch needs to derive the destination IP address to SGT. This is because the Ethernet frame has only the source SGT information and to enforce the policy the distribution switch needs to learn the SGT binding associated with the destination IP address.

In the current design example, SXP tunnels are established from the access layer IES to the Cisco ISE and the distribution switch also has an SXP tunnel to the Cisco ISE. This way the IP-SGT binding information is sent to the Cisco ISE and the distribution switch learns the IP-SGT binding information from the Cisco ISE. Figure 42 depicts the design.

Figure 42 SXP Design in Industrial Automation Network Security CVD



Policy Definition and Enforcement Summary

The Design for policy definition and enforcement previously described in this section is a well defined model based on the assumptions made allowing all traffic within a cell area zone to communicate and provide policy for any inter cell communication. The model is scalable and provides a simple Security Group model. One point to highlight is that a thorough understanding of the assets connected, their vulnerabilities and traffic patterns both inter and intra cell are needed in order to define a policy framework. Northbound flows should be considered between the cells and the OT application layer. There are other models that are mentioned within the section that elude to policy enforcement on the IE switches which would require different policy matrices and different Security Group definition to support the model. This though was not validated as part of the Industrial Automation CVD.

Platforms Validated as part of the Industrial Automation CVD for TrustSec and their roles:

- Distribution 9300 Policy Enforcement
- Access Device IE 3400 and IE4000

Cisco ISE Deployment Considerations

Deploying Cisco ISE in a large network requires an IT security architect to consider several factors such as scalability and high-availability. This design guide covers many factors related to deploying a large-scale Cisco ISE deployment. We encourage the reader to read the CPwE DIG to develop a good understanding of large-scale solution deployments.

In the distributed installation, the Cisco ISE system is divided into three discrete nodes (personas)-Administration, Policy Service, and Monitoring-which are described as follows:

- The Policy Administration Node (PAN) allows the Enterprise IT team to perform all administrative operations on the distributed Cisco ISE system. The PAN (located in the Enterprise Zone) handles all system configurations that are related to functionality such as authentication and authorization policies. A distributed Cisco ISE deployment can have one or a maximum of two nodes with the Administration persona that can take on the primary or secondary role for high availability.
- The Policy Service Node (PSN) provides client authentication, authorization, provisioning, profiling, and posturing services. The PSN (located within the Industrial and the Enterprise Zone) evaluates the policies and provides network access to devices based on the result of the policy evaluation. At least one node in a distributed setup should assume the Policy Service persona and usually more than one PSN exists in a large distributed deployment.
- The Monitoring Node (MnT) functions as the log collector and stores log messages and statistics from all the PAN and PSN devices in a network. The MnT (located in the Enterprise Zone) aggregates and correlates the data in meaningful reports for the IT and OT personnel. A distributed system can have at least one or a maximum of two nodes with the Monitoring persona that can take on primary or secondary roles for high availability.

For optimal performance and resiliency, this CRD provides these recommendations for the Industrial Automation Identity and Mobility Services architecture:

- Administration and Policy Service personas should be configured on different Cisco ISE nodes.
- Monitoring and Policy Service personas should not be enabled on the same Cisco ISE node. The Monitoring node should be dedicated solely to monitoring for optimum performance.
- A PSN should be placed in the Industrial Zone (Levels 0–3) to provide services for clients in the Industrial Zone. If the Enterprise and Industrial Zones become isolated, any existing clients will still be able to securely access the network. For best practices, see Previous and Related Documentation for links to the Industrial Automation IDMZ CVD DIG.

Based on the recommendations above, a typical distributed Cisco ISE deployment in the Industrial Automation architecture consists of the following nodes (hardware appliances or VMs).

- One Primary Administration/Secondary Monitoring node
- One Secondary Administration/Primary Monitoring node
- One or several PSN in the Enterprise Zone
- One or several PSN in the Industrial Zone

Note: The number of PSN in the Enterprise and Industrial Zones may depend on the company size, the number of active clients, redundancy requirements, and geographical distribution (for example, one PSN per each plant).

IPDT Considerations

IP Device Tracking (IPDT) is a feature that allows an IES or any other switch or router to keep track of connected hosts attached to it. The IPDT feature must be enabled for several security features such as dot1x,MAB, Web-Auth, auth-proxy, and so on. The IPDT feature keeps mappings between IP addresses and MAC addresses. To do the tracking, the IES sends an ARP probe with default interval of 30 seconds. The probes are implemented as per RFC5227 where the source IP address is set to 0.0.0.0. If the IPDT feature is enabled with a default source IP address of 0.0.0.0, then there could be conflict between the IES and an IACS asset that is also doing device tracking (the duplicate IP address 0.0.0.0) problem is explained in:

https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problem-solution-product-00.html

OT Intent-based Security for Industrial Automation Use Cases

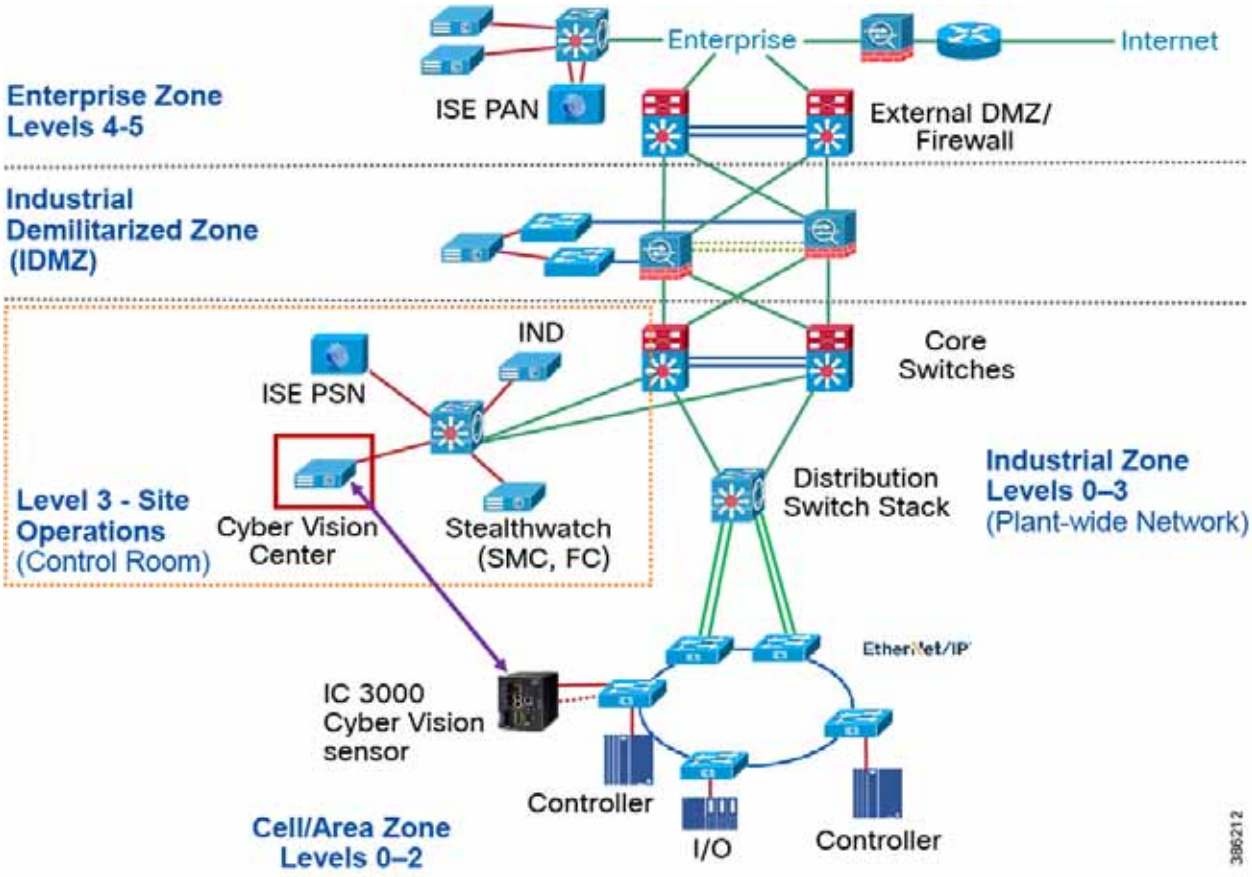
The previous section outlined the considerations for the design and implementation of Visibility and Segmentation within the Cell area zone for Security. This section provides example use cases that highlight how different component such as IES, ISE Cisco Cyber Vision and StealthWatch integrate to provide the core security capabilities for Visibility, Segmentation and Detection. The following use cases can apply to the mine.

- Visibility and Identification of network devices and IACS assets in the Cell/Area Zone
- Group policy assignment of IACS assets in Industrial Zone
- Malware detection with NetFlow in the Cell/Area Zone and Level-3 Site Operations zones
- OT-managed remote user (employee or partner) access to the plant infrastructure
- Detection of operational events (enabled by Cisco Cyber Vision)

Visibility and Identification of IACS Assets in the Cell/Area Zone

The purpose of this use case is to show how an OT control system engineer and IT security architect can work together to gain visibility of the network devices and IACS assets in the Cell/Area Zone. The visibility must be granular enough that the IT security architect can know the type of the IACS asset-Controller, I/O, drive, HMI, and others. To segment traffic flows going across in East-West or North-South direction it is important that the IT security architect gain visibility of the current network topology in the plant-wide network. In this guide, there are two methods to gain visibility to IACS assets using Cisco Cyber Vision, and Cisco Industrial Network Director (IND).

Figure 43 Visibility and Identification in the Cell/Area Zone



This section describes both use cases:

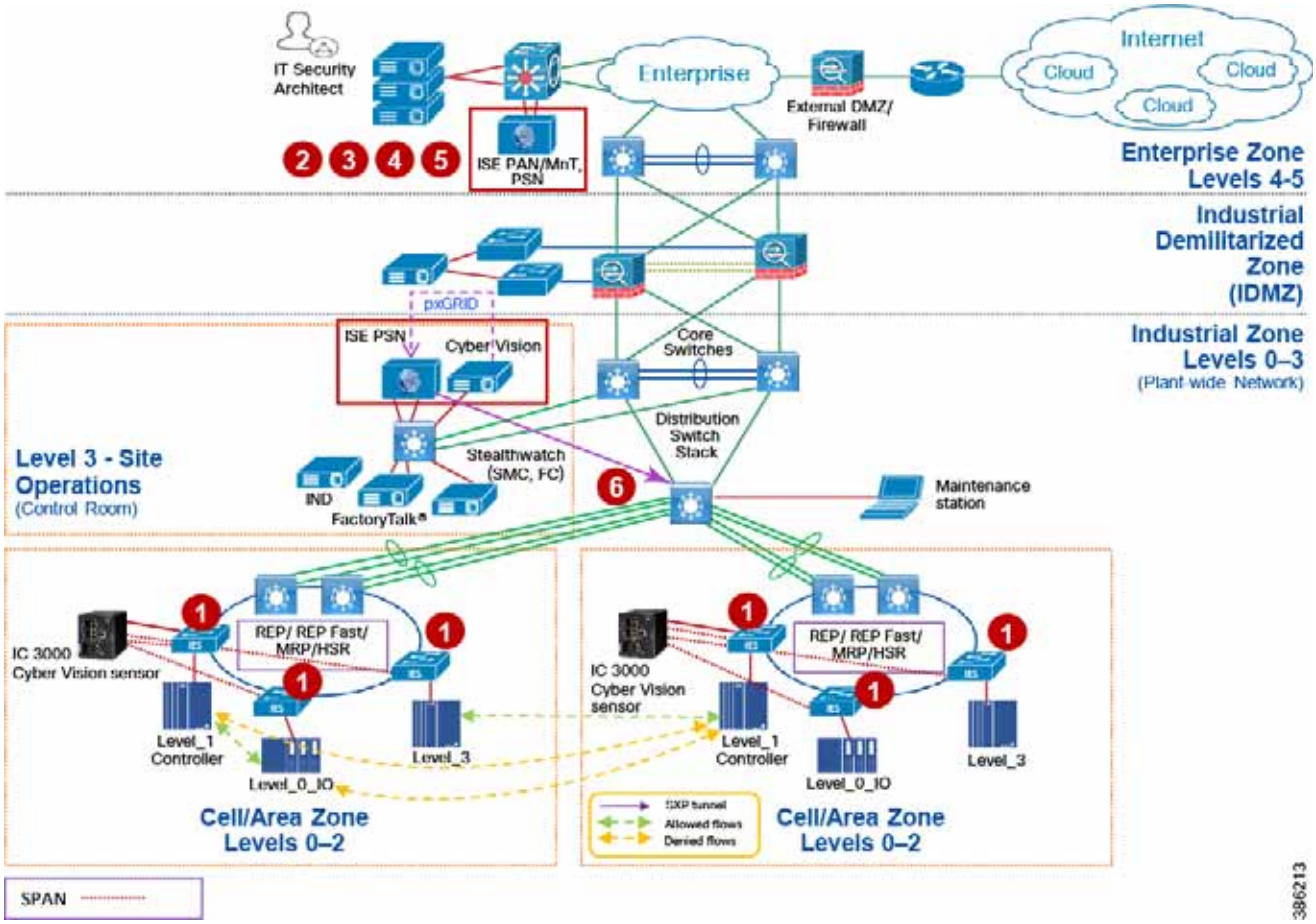
1. An OT control system engineer decides which IACS assets to monitor, choses Cyber Vision Deployment option, and configures passive monitoring (SPAN) on the ports. Refer to the implementation guide.
2. Cisco Cyber Vision Center dynamically learns the IACS vendor-name, model-name, serial-number, ip-address, mac-address, firmware version, device-name, and other pertinent information.

The CyberVision Center can now run a vulnerability assessment against the asset to provide the IT security and OT controls engineer information to help aid security policy and segmentation.

Cell/Area Zone Segmentation of IACS Assets using Cisco Cyber Vision

This use case describes in detail how to achieve segmentation of different traffic flows in a Cell/Area Zone using Cisco ISE and Cyber Vision.

Figure 44 Cell/Area Zone Segmentation of IACS Assets using Cisco Cyber Vision



The Asset information gained from CyberVision in the previous use case, can now provide attributes and context to Cisco ISE via pxGRID:

1. The IT security architect must configure port-based authentication on all the IES. Refer to the implementation guide.
2. The IT security architect must configure TrustSec SGTs for different IACS assets—Level_1_Controller, Level_0_IO, and Level_3 in ISE. Refer to the Industrial Automation implementation guide.
3. The IT security architect must configure Authentication and Authorization policy in ISE. Refer to the Industrial Automation implementation guide.
4. The IT security architect must configure SXP tunnels from IES and the distribution switch to ISE. Refer to the Industrial Automation implementation guide.
5. The IT security architect must configure the TrustSec Policy Matrix on ISE. Refer to the Industrial Automation implementation guide.

6. The IT security architect must configure the enforcement on the Cisco Catalyst 9300, or Cisco IE 5000 distribution switch. Refer to the Industrial Automation Implementation Guide.

Flow-Based Anomaly Detection

This use case describes how an IT security architect can use StealthWatch along with NetFlow enabled on IES and Cisco Catalyst 9300, and Cisco Catalyst 9500 acting as distribution switches to monitor the network flows in the plant-wide network. In addition, this use case also shows the integration between the Cisco Cyber Vision and StealthWatch. The integration between the Cisco Cyber Vision and StealthWatch helps an IT security architect to understand the context of OT flows happening in the Cell/Area Zone. The integration between Cisco Cyber Vision and StealthWatch happens by implementing the following steps.

To detect traffic flows occurring across the mining operations, it is important that NetFlow is enabled on all the networking devices to capture the traffic flows that are sent to the StealthWatch FlowCollector. SMC retrieves the flow data from the FlowCollector and runs pre-built algorithms to display the network flows and also detect and warn if there is any malicious or abnormal behavior occurring in the network. In this guide, three flows are shown to demonstrate the capability of StealthWatch using NetFlow:

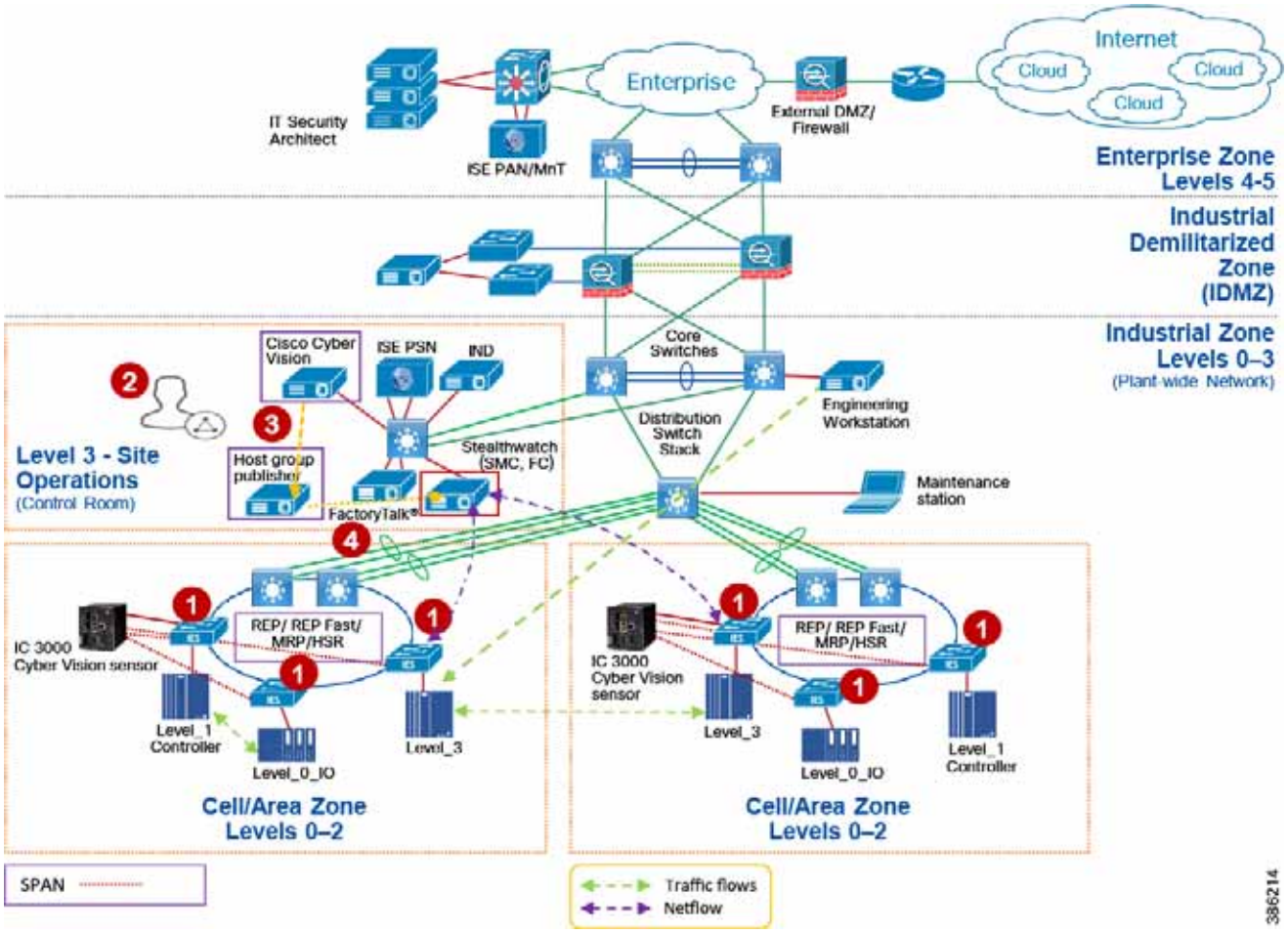
- Traffic between IACS assets in a Cell/Area Zone (Intra-Cell/Area Zone).
- Traffic between Level_3 IACS assets across the Cell/Area Zone (East-West or Inter-Cell/Area Zone traffic).
- Traffic between the EWS and a Level_3 IACS asset (North-South) traffic.

The following steps must be performed by the IT security architect to detect the above-mentioned flows:

1. IT security architect must enable NetFlow on all the IES and the Cisco Catalyst 9300 switches. Refer to the Implementation Guide.
2. The IT Security Architect deploys the Cisco Cyber Vision python scripts in a server.
3. The IT Security Architect using the python script connects to the Cisco Cyber Vision Center and download the host group information.
4. The IT Security Architect using the python script connects to the StealthWatch management Console (SMC) and publishes the host group information.

StealthWatch can now display context of the assets that are communicating rather than just the IP address.

Figure 45 Flow-based Anomaly Detection



Detection of Malware in Cell/Area Zone and Level-3 Operations

This section discusses how StealthWatch detects malicious traffic traversing a plant network. When malware is spreading in the network, it becomes very difficult to pinpoint where the malware propagation is occurring. An IT security architect needs to identify the source and then develop a remediation plan to address the problem. StealthWatch has many inbuilt machine learning algorithms that can assist an IT security professional in detecting possible malware propagation in the network. It can detect abnormal behavior and provide the IP address of the device that is causing the propagation. This information greatly simplifies the detection process.

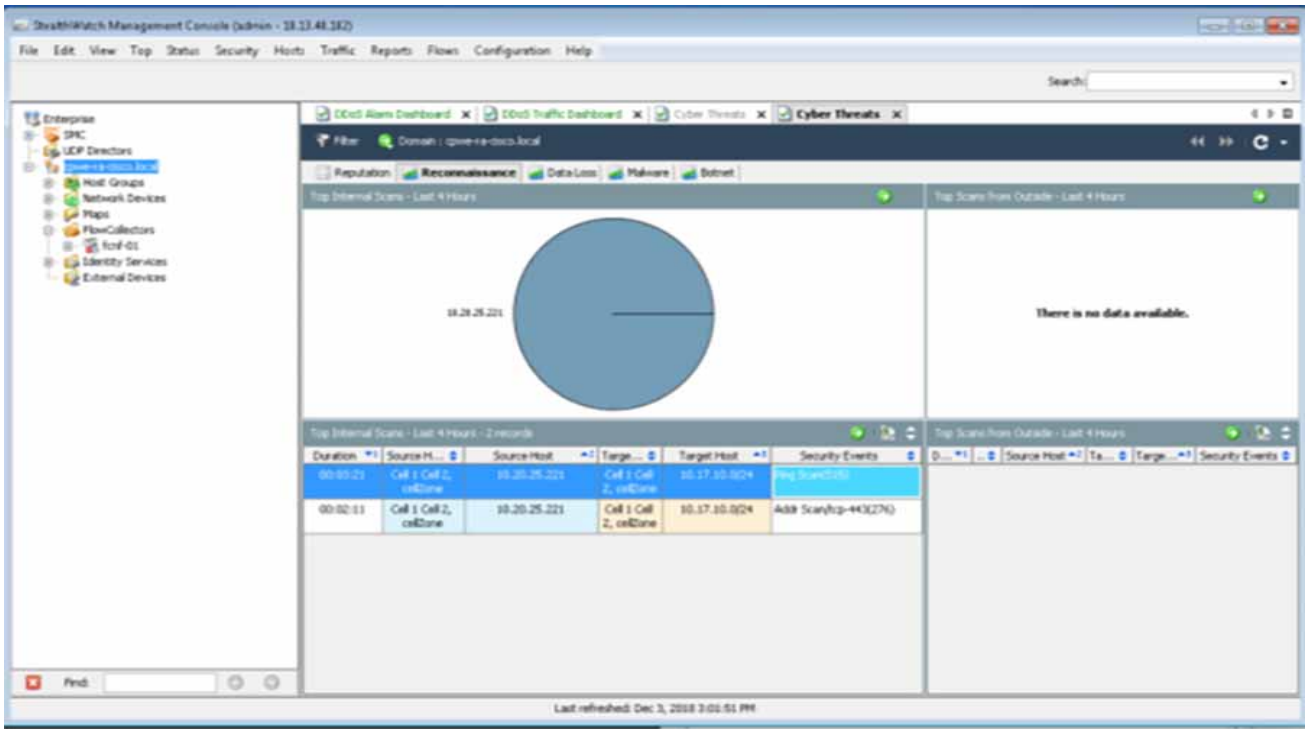
Without StealthWatch, IT security architect may have to follow a number of potentially time-consuming steps to investigate the malicious activity, such as shutting down parts of the network and going through logs of many devices. These steps not only take time to isolate, but also increase the risk of other vulnerable devices becoming infected. When active malware is detected, quickly enacting a remediation plan is essential in building a defense against malware.

Often the malware behavior is to immediately scan the network to identify any other vulnerable devices in the plant-wide network. In this CRD, two traffic flows related to malware are discussed:

- An infected laptop attached to an IES
- An infected laptop attached to a Layer-3 site operations center.

In both the cases, the infected laptop attempts to scan the entire IP address range to identify the next possible targets and attempt to infect them. StealthWatch would immediately detect a possible infiltration by generating an alarm under High Concern Index. Any alarm that comes under High Concern Index must be immediately taken into consideration and as more malicious behavior is detected with alarms, a host High Concern Index increments to signify the increasing threat. Figure 46 shows how an alarm is displayed in the SMC. In Figure 46, the host 10.20.25.221 is attempting to do a scan for the 10.17.10.0/24 network.

Figure 46 Detection of Malware in Cell/Area Zone and Level-3 Operations



For more information about alarms see:

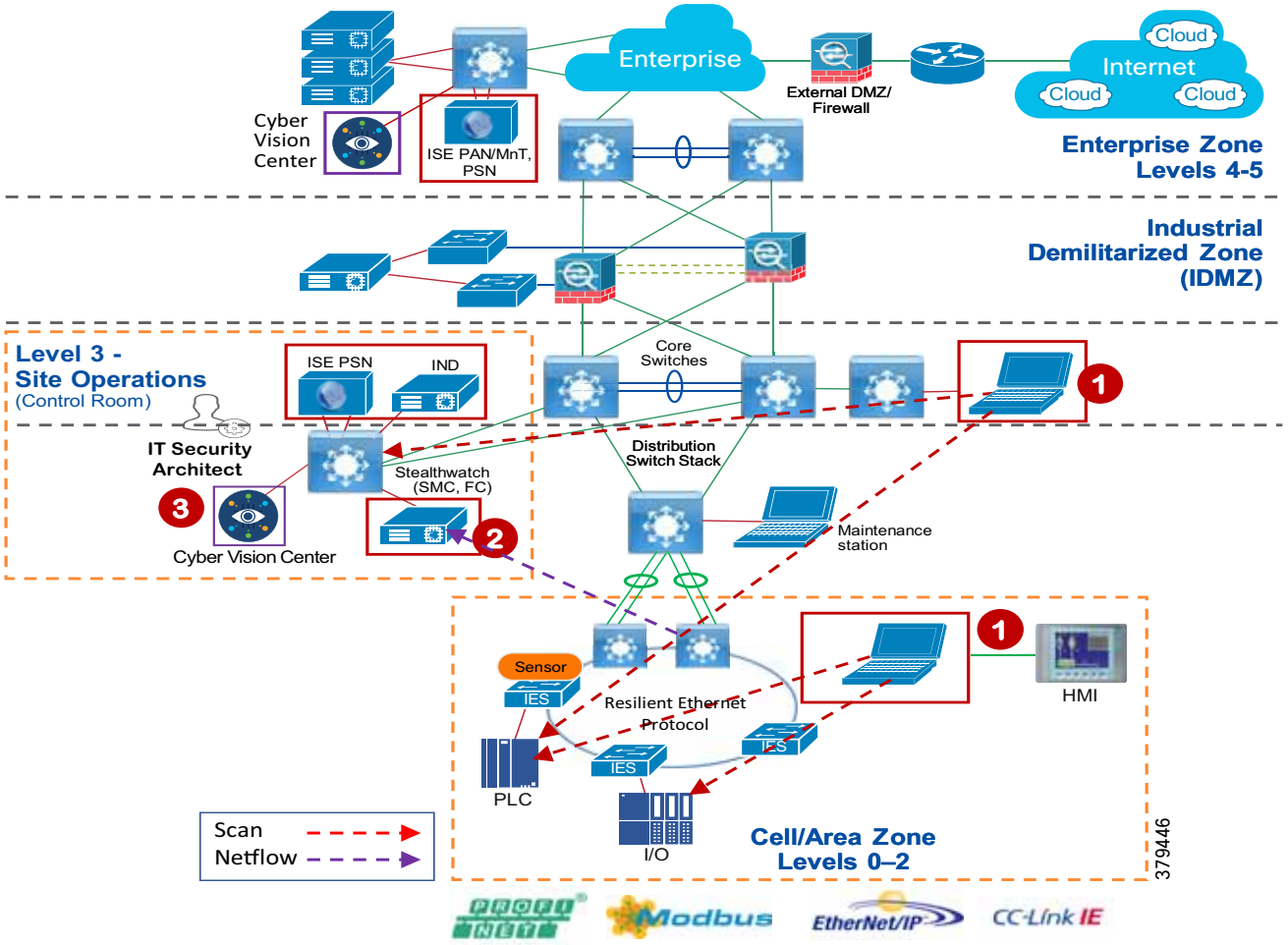
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf

Figure 47 shows the scenario where an infected laptop is connected to Cell/Area Zone or Level_3 Site Operations zone and is being detected by StealthWatch. The steps involved are:

1. The IES in the Cell/Area Zone or the distribution switch in Level_3 Site Operations is enabled with NetFlow. Refer to the implementation guide.
2. The SMC reports an alarm indicating that there is a malicious activity occurring in the network.

An IT security architect responds to the alarm by planning the next stage of remediation that can involve doing further investigation, restricting the access of the IACS asset, and so on.

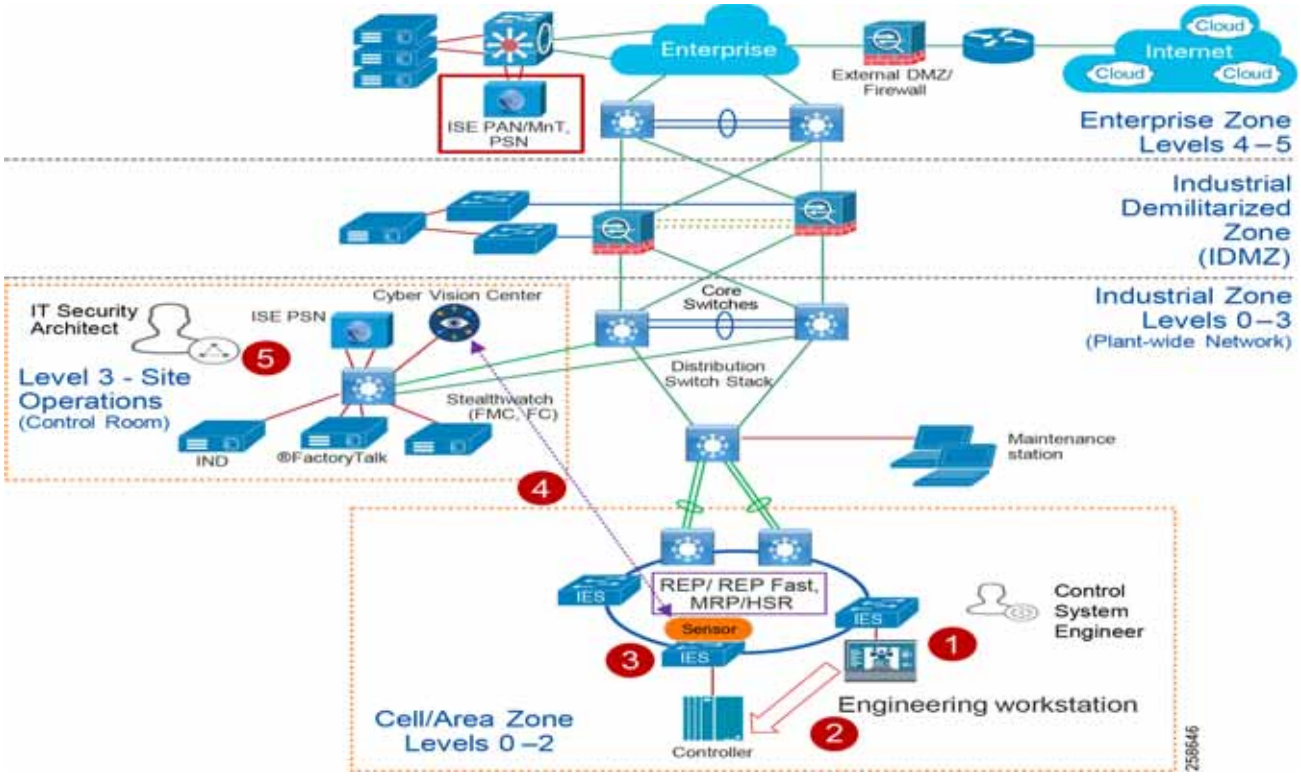
Figure 47 Detection of malware in Cell/Area Zone



Detection of Operational Events—Enabled by Cisco Cyber Vision

The purpose of this use case is to show how Cisco Cyber Vision solution can detect operational events in the Cell/Area Zone. Operational events can include a program download from the engineering workstation to a PLC, start CPU, Stop CPU, and so on. When such events occur in the Cell/Area Zone, the Cisco Cyber Vision Sensor, which is passively monitoring these events, detects them and sends metadata about those events to the Cisco Cyber Vision Center. The Cisco Cyber Vision Center displays those events on its dashboard with all pertinent information such as graphical description of the flow, the IP address of the workstation, and the controller information.

Figure 48 Detection of Operational Events – Enabled by Cisco Cyber Vision



The sequence of events is:

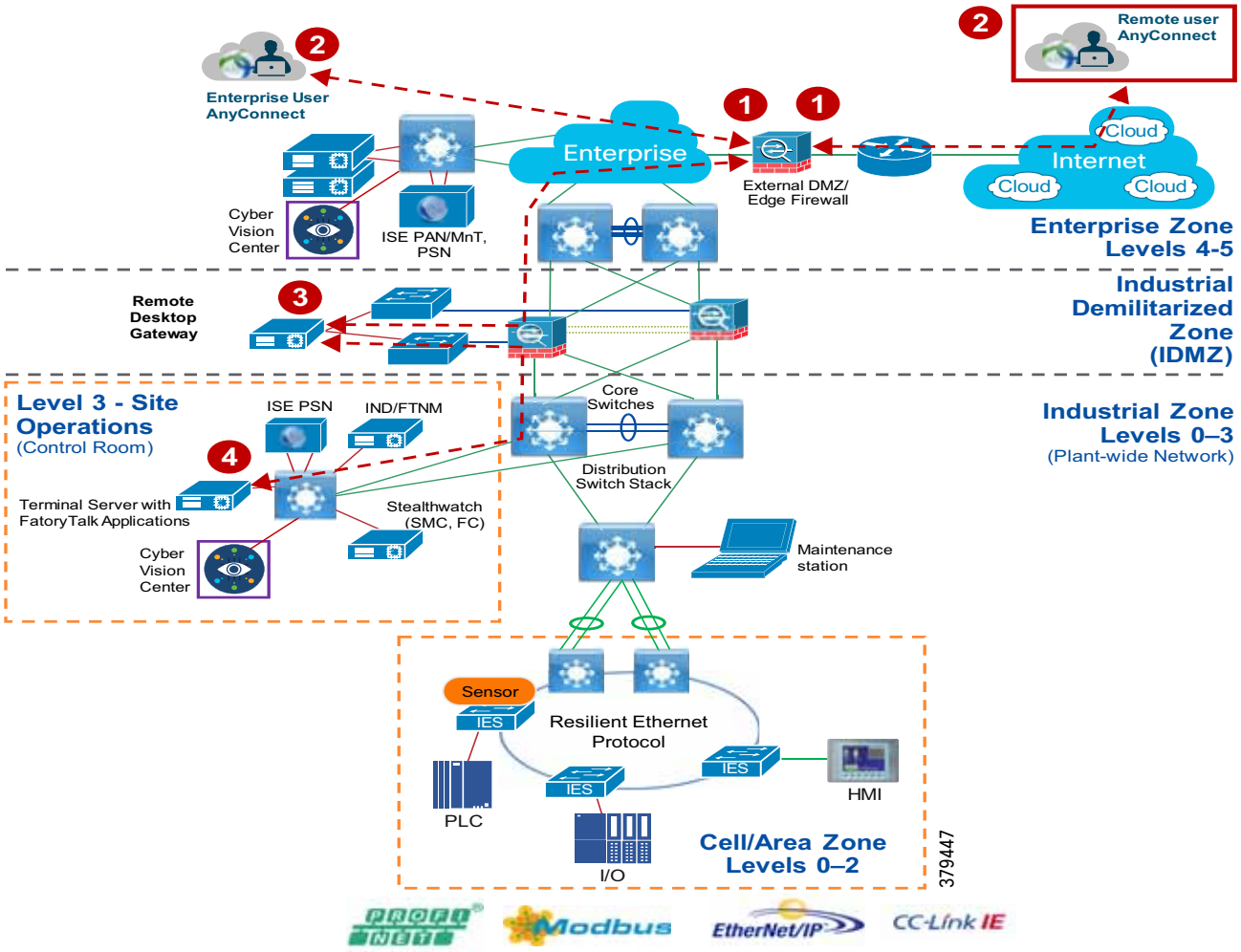
1. The control system engineer modifies or builds a new application on the engineering workstation.
2. The control system engineer pushes the program to the controller.
3. The Cisco Cyber Vision Sensor deployed in the Cell/Area Zone detects the event.
4. The Cisco Cyber Vision Sensor sends that event to the Cisco Cyber Vision Center.
5. The IT security architect reviews the alert and determines the legitimacy of the event

OT Managed Remote Access to Plant Floor

This use case describes how a remote user employee or partner can access a networking device or an IACS asset from either the internet or the Enterprise zone. The *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* (for best practices, see Previous and Related Documentation for links to the Industrial Automation IDMZ CVD) provides design considerations and implementation details for providing remote access. The high-level steps for the remote access solution in that CVD as described in Figure 48 are:

1. A remote VPN gateway (ASA firewall) is enabled with a VPN group that authenticates a remote user and authorizes a service, which in this case is to access a remote desktop gateway in the IDMZ.
2. The remote user, either an employee or partner, uses a remote access VPN client (Cisco AnyConnect) to connect to the remote VPN gateway and establishes a VPN session.
3. From the remote VPN gateway a connection is established to the remote desktop gateway in the IDMZ.
4. From the remote desktop gateway, a connection is established to the Terminal Server with FactoryTalk applications in the Level_3 – Site Operations.

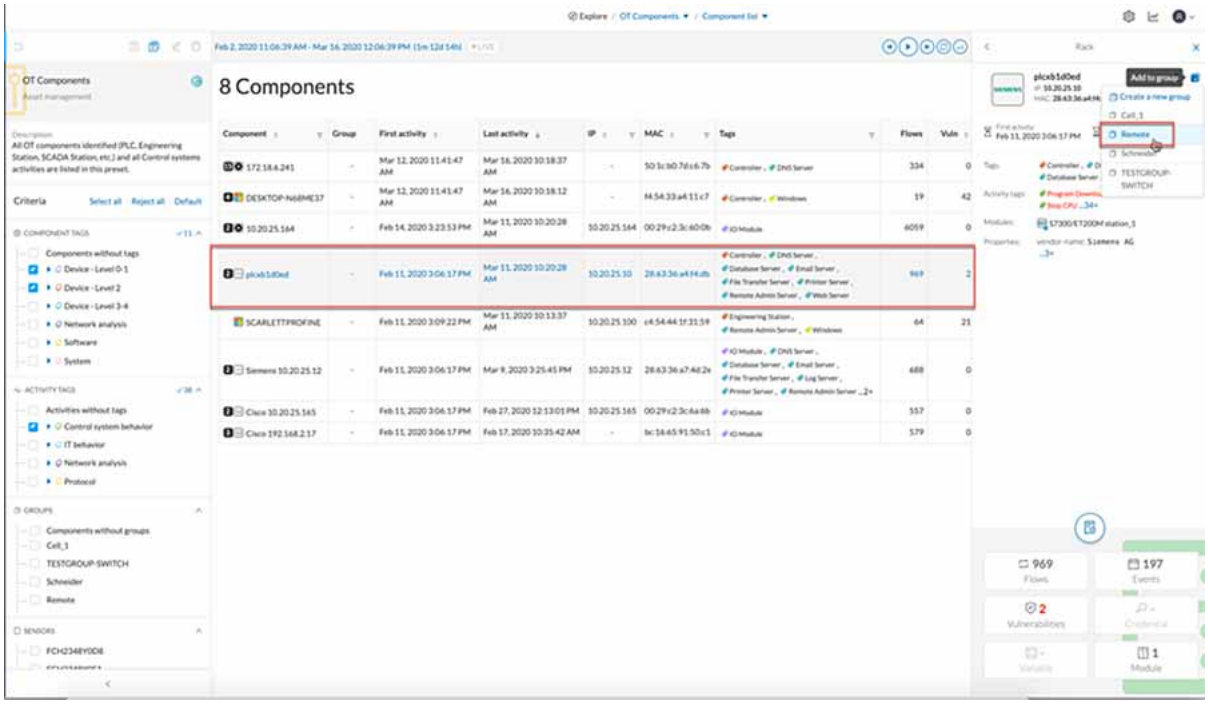
Figure 49 Remote User Access in Industrial Automation Network



This use case builds on the previous Securely Traversing IACS Data Across the Industrial Demilitarized Zone CVD and expands the remote user use case by providing the means for an OT control system engineer to influence the remote access. In the previous CVD, when a remote user needs access an OT control system engineer opens a request to IT security architect to enable remote access for IACS assets. The remote user than accesses the desired IACS asset. However, when the remote user no longer needs access to the IACS asset, then the OT control system engineer must open another case for removing access. This process works, but when access is not removed in a timely manner, the risk of a security breach increases.

The ISE and Cisco Cyber Vision integration via pxGrid provides a way for an OT control system engineer to govern device access by modifying the assetTag of the IACS asset. When an OT control system engineer changes the group of the IACS asset, ISE updates the profile for the asset and the SGT (and communication restrictions) updates. When the IACS asset is put back in the original group, the remote access to the asset is revoked through the same profiling update. The Figure below shows the group information of an asset.

Figure 50 Modifying the Group information of an IACS asset



In this Industrial Automation CVD, the remote access use case is demonstrated by creating a separate group called Remote. A device that needs remote access needs to be moved to this group and when such an action is performed the following events are triggered:

1. The Cisco Cyber Vision sends a new device attribute “Remote” to ISE, which is linked to the “assetGroup” field in ISE. Refer to the implementation guide.
2. ISE classifies this device as Remote Access and issues a Change of Authorization for the IACS asset. This triggers a new authentication and authorization, which results in a new SGT assignment. Refer to the implementation guide.
3. The Cisco Catalyst 9300 distribution switch downloads the new SGACL from the ISE to allow access to the IACS device. Refer to the implementation guide.
4. Once the access to the IACS asset is no longer needed, the OT control system engineer moves the IACS asset back to the original group.
5. Cisco Cyber Vision communicates the new group information to ISE, which triggers another reauthentication and reauthorization, placing the IACS asset back in its original profile of “Level_1_Controller”. Refer to the implementation guide.
6. The Cisco Catalyst 9300 distribution switch has an existing policy that denies communication from Remote_Access to Level_1_Controller, so the remote communication is blocked.

Note: When a new SGT is assigned to an IACS asset there will be a temporary loss of connectivity for few seconds before applications can communicate with the IACS asset. The controller will not be part of the IACS network while in the remote access group.

Previous and Related Documentation

This design and implementation guide is an evolution of a significant set of industrial solutions issued by Cisco. In many ways, this document amalgamates many of the concepts, technologies, and requirements that are shared in industrial solutions. The vertical relevance will be maintained, but shared technical aspects are essentially collected and referred to by this document.

- The existing documentation for manufacturing and oil and gas can be found on the Cisco Design Zone for Industry Solutions page:

  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html

- The Cisco Catalyst 9300 is positioned as the distribution switches where there is a controlled IT environment.
  - Cisco Catalyst 9000 switching product page:

    https://www.cisco.com/c/en/us/products/switches/catalyst-9000.html

- Cisco Catalyst 9300 StackWise–480 configuration:
  - For Cisco Catalyst 9300

    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/stck_mgr_ha/b_165_stck_mgr_ha_9300_cg/managing_switch_stacks.html

- Industrial Ethernet switching product page:

  https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html

- Cisco IE 3x00 Series Switch

  https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/16_10/release_note/b_1610_releasenote.html

- Cisco IE 4000, Cisco IE 4010, and Cisco IE 5000:
  - Switch Software

    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html

  - Switch Software Smartports configuration

    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacro.html

- Cisco Industrial Network Director:

  http://www.cisco.com/go/ind

  - Network Management for Operational Technology in Connected Factory Architectures

    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD/IND_Connected_Factory_CRD.html

- IEC Standards: IEC 61588 Precision clock synchronization protocol for networked measurement and control systems

  http://s1.nonlinear.ir/epublish/standard/iec/onybyone/61588.pdf

Table 18 Previous Manufacturing Industry Documentation

Solution	Description
Connected Factory—CPwE https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html	Solution to assist manufacturers seeking to integrate or upgrade their Industrial Automation and Control System (IACS) networks to standard Ethernet and IP networking technologies.
Connected Factory—PROFINET https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-factory/connected-factory-profinet.html	Solution for PROFINET-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.
Connected Factory—CC-Link IE https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/MELCO/CC-Link_Connected_Factory.html	Solution for CC-Link IE-based industrial environments to integrate Cisco Industrial Ethernet switches into the automation network.
Connected Machine https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-machines.html	Enable rapid and repeatable machine connectivity, providing business improvements such as overall equipment effectiveness (OEE) and machine monitoring.
Connected Factory—Network Management for Operational Technology https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD.html	Discusses the use of Cisco's Industrial Network Director application for monitoring industrial network assets and discovering automation devices within the context of the Connected Factory solution.