






Enabling Industry 4.0 with Next-Generation Infrastructure

Solution Guide

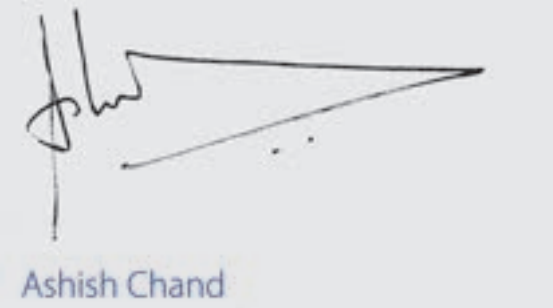
BELDEN
SENDING ALL THE RIGHT SIGNALS

Transforming Your Network from Providing Outputs to Providing Outcomes!

Automation networks are rapidly evolving to deliver business outcomes in safety, innovation, quality, delivery and productivity more directly than ever before. At the same time, disruptive technologies like distributed control, edge data processing and cloud analytics are fundamentally changing the network architecture of automation control systems, enabling those outcomes but also driving the need for unified industrial communications. This transition, propelled by the adoption and standardization of real-time Ethernet, is accelerating the transformation to Industry 4.0.

The expertise to design and deploy high-quality hardware and software working together in networks designed for specific use cases while ensuring high availability, reliability and security is rarely available in one place. Belden's portfolio of network products which draw on knowledge of disparate applications accumulated over more than a hundred years, our global service and support capabilities, and our proven track record of successful installation make us the provider of choice for customized, future-ready networks.

We have all the expertise you need to transform your network in one place. If you are not already talking to us about your networking requirements, you probably should be!



Ashish Chand
Executive Vice President,
Industrial Automation

Overview

Smart industries of today are optimizing logistics, customer service, and management using and integrating computation, networking and other IoT technologies. Such integration produces networks that are interconnected and complex. With Industrial Automation blurring the lines between IT and OT, new and pressing challenges have arisen: misconfigurations across different layers, risks of operational disruptions and the ever-larger-looming threat of cyber-attacks.

All of these challenges can be confidently met with the help of a trusted signal transmission partner. Whether for smart buildings, wireless, IoT or Big Data, Belden's range of robust solutions that meet the most rigorous compliance standards can make communication reliable, capable and secure across all network layers from field to WAN.

With a proud legacy of innovation, product quality and customer service that spans more than a century, Belden brings leading-edge solutions for infrastructure that guarantee uninterrupted, secure transmission of data and information.

In this solution guide we showcase some of the trends in technology that are powering digital transformation across industry and how Belden solutions offer everything that's needed for a seamless transition to industry 4.0.

Belden is a global leader in signal transmission and security solutions to support mission-critical applications of enterprise and industrial customers. Every customer of Belden can rely on our products to operate and perform even in the harshest, most demanding environments and can count on Belden's uncompromisingly responsive service and support.

The Building Blocks Of Industry 4.0

The Internet of Things (IoT) is the embedding of technology in everyday objects that allows them to connect over the Internet and exchange data with other devices and systems. IoT's enablement of real-time communication between heretofore passive, isolated devices is dramatically changing the way people live and work and making lives simpler and safer. Industrial applications of IoT promise the Industrial Internet of Things (IIoT) that will allow industries to equip themselves with network-connected machines that range from sensors for predictive and preventive maintenance to industrial robots that accelerate the speed of production lines. Employing machine-to-machine (M2M) communication, machine learning and other Big Data techniques, IIoT is already allowing industrial enterprises to make quantum-jump improvements in the efficiency and reliability of their operations. IIoT is a key element of Digital Transformation and is set to play a central role in the next revolution of the industrial ecosystem referred to as Industry 4.0.

Industry 4.0 can be understood as the convergence of several emergent trends in manufacturing, logistics and computing. At its heart is the fact that physical devices, machines, and processes can be controlled and operated better than ever before by "nervous systems" constructed by combing IIoT with cloud computing, machine learning and artificial intelligence.

Digital Transformation is increasingly being adopted in all verticals, right from education to manufacturing. More and more businesses recognize the need to quicken their pace of change and adopt game-changing technologies and platforms like IIoT, Edge Computing, Smart Factories, Smart Grids and Industry 4.0. Every layer of network infrastructure must be equipped for seamless communication.

Essential to success are reliable communication and signal transmission between devices. Today the industrial ecosystem is moving away from fieldbus networks based on proprietary technologies and communication protocols to universal standards like Ethernet, 802.11 WiFi, IP, TCP and UDP. Standards-based, secure networks are the foundations for successful transitions to IIoT. Wireless networking is also becoming a popular method connecting corporate and industrial systems because of the ease of employment and relatively low cost.

Today the industrial ecosystem is moving away from fieldbus networks based on proprietary technologies and communication protocols to universal standards like Ethernet, 802.11 WiFi, IP, TCP and UDP. Standards-based, secure networks are the foundations for successful transitions to IIoT.

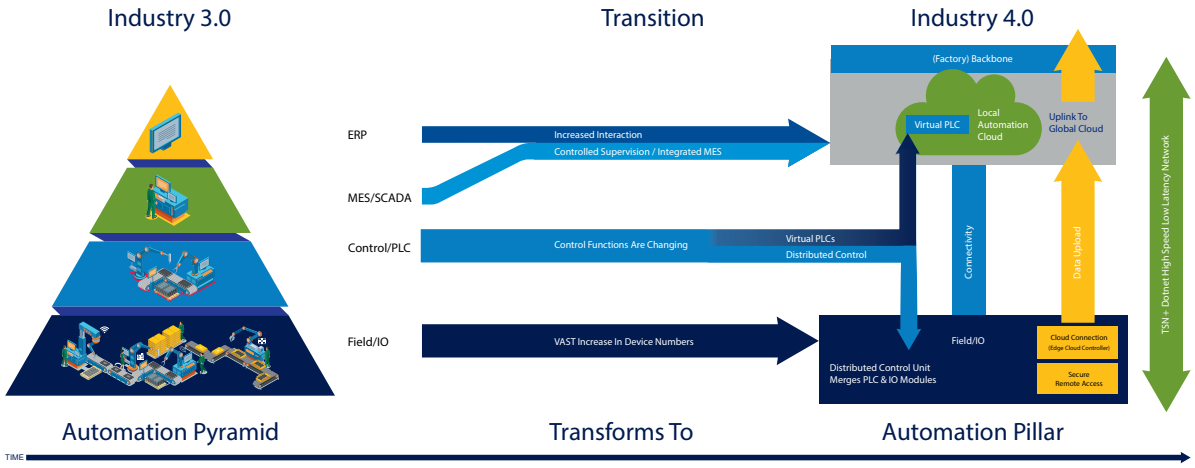


Figure 1: Industrial Automation Transformation

Industrial Automation Conceptual Architecture

In manufacturing Digital Transformation means automating factories and inbound and outbound supply chains. For industries like oil and gas, automation will be needed along the value chain from extraction through refinement to distribution. Irrespective of the industry and the diversity and scale of the businesses acting in it, the constants in their network infrastructures will continue to be cabling, connectivity, networking, security and industrial protocols. These core components are what the Belden Industrial Automation Solution Guide is about.

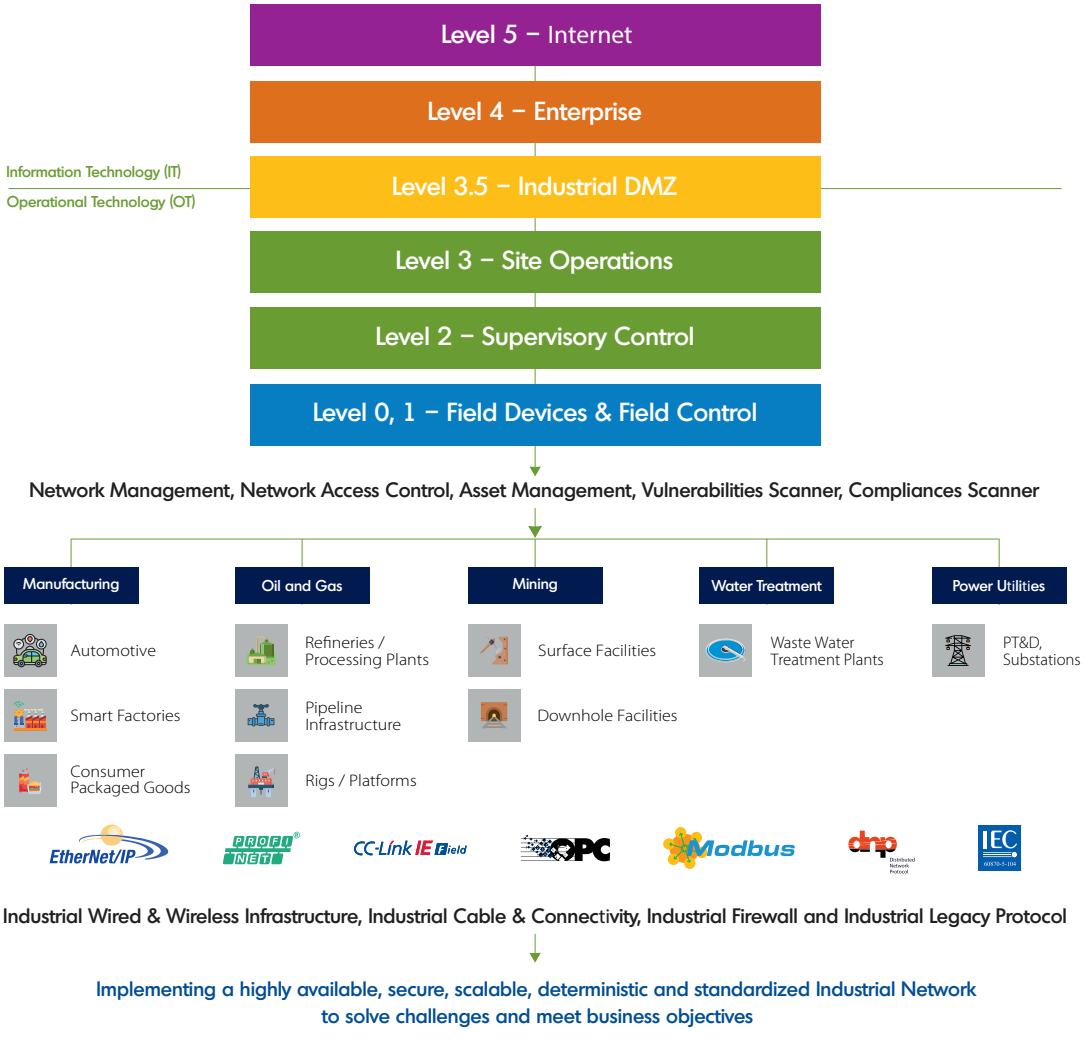


Figure 2: Conceptual Architecture - Overview

Creation of a Single Network for Greater Outcomes

Industry 4.0 promises unprecedented levels of flexibility that translate into agile production which in turn enables manufacturers to respond quickly to seasonal or shifting customer demand. It increases uptime and reduces overheads, maintenance costs and resource consumption leading to improvements in customer confidence and resultant business. These are just examples of industry-changing developments expected in the Fourth Industrial Revolution.

However, realizing these opportunities depends on businesses' capabilities to acquire, communicate and analyze data - data and the information manufactured from it are the currencies by which all of these improvements can be obtained. But in most factories today data is stored in silos, isolated and inaccessible and difficult to transform into actionable insights.

Breaking down the barriers between the silos requires successful IT/OT convergence. Traditionally, office Information Technology (IT) networks and plant floor Operational Technology (OT) networks have been wholly separate and the personnel supporting them often had little interaction. As Industrial Ethernet replaces fieldbus on the plant floor networks are merging, requiring specialists to find new ways of collaborating but also creating valuable opportunities to combine resources in pursuit of shared goals and business success.

With Ethernet now commonly running on both the IT and OT sides, the costs and shortcomings of isolated networks are becoming ever harder to justify – hence the onset of the convergence of IT and OT, in concept the creation of unified business networks, strategically protected and allowing data to flow only as the business permits. Selective shared access implemented through device connectivity and strong, dynamic systems of permissions protect information and resources from unauthorized access.

Converged networks open up possibilities for selectively sharing data. Hence the emergence of what has come to be known as the convergence of IT and OT – the creation of a single network.

Creation of a Single Network for Greater Outcomes

TSN is a suite of protocols geared to achieving deterministic data transfer at the network level. TSN enables IT-OT convergence as it allows information flows across IT and OT processes over a common infrastructure without compromising on real-time characteristics or performance guarantees.

Time Sensitive Networking (TSN) is a set of IEEE Ethernet standards that are foundational for meeting the demands of Industry 4.0. With TSN all data in the factory - from the sensors to the Cloud, the front office and everywhere in between - can coexist and communicate. TSN is the first step to breaking down data silos that hinder industrial communications and enabling extensive access to data-based decision support. TSN serves as the springboard for industrial organizations seeking to achieve the promise of Industry 4.0 by enabling:

- Creation of a common language
- Collaboration between IT and OT specialists
- High reliability over standard Ethernet
- Scalability and agility
- Better utilization of factory assets to maximize efficiency

TSN standards are crucial in ushering in the next-generation of technology that will revolutionize manufacturing operations in a cost effective manner.

Time-Sensitive Networking (TSN) adds a level of determinism to Ethernet-based data transmissions that was previously not possible with conventional Ethernet technology.

In the future Ethernet networks will provide:

- Calculable, guaranteed end-to-end latencies
- Low latency fluctuations - jitter
- Extremely low packet loss

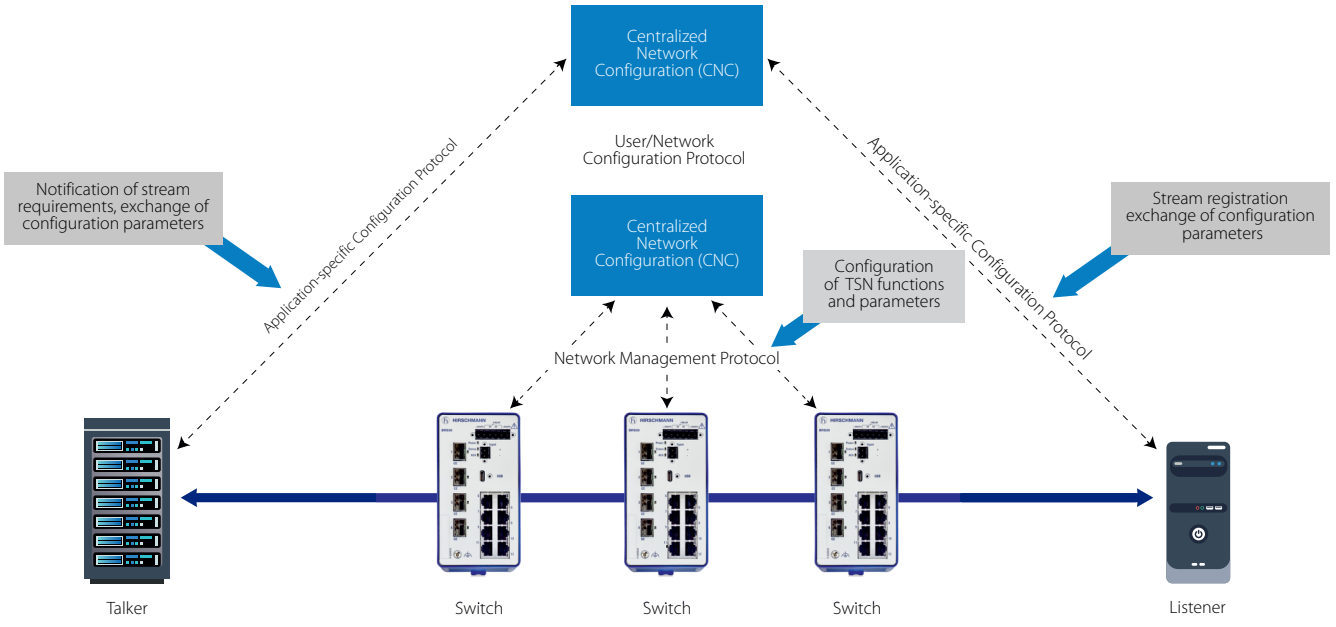


Figure 3: TSN Configuration Approach

The Belden Industrial Automation Reference Architecture (Figures 4a and 4b) recognizes and responds to the need for Time Sensitive Networking across the separate layers of infrastructure that businesses need to participate in the Fourth Industrial Revolution.

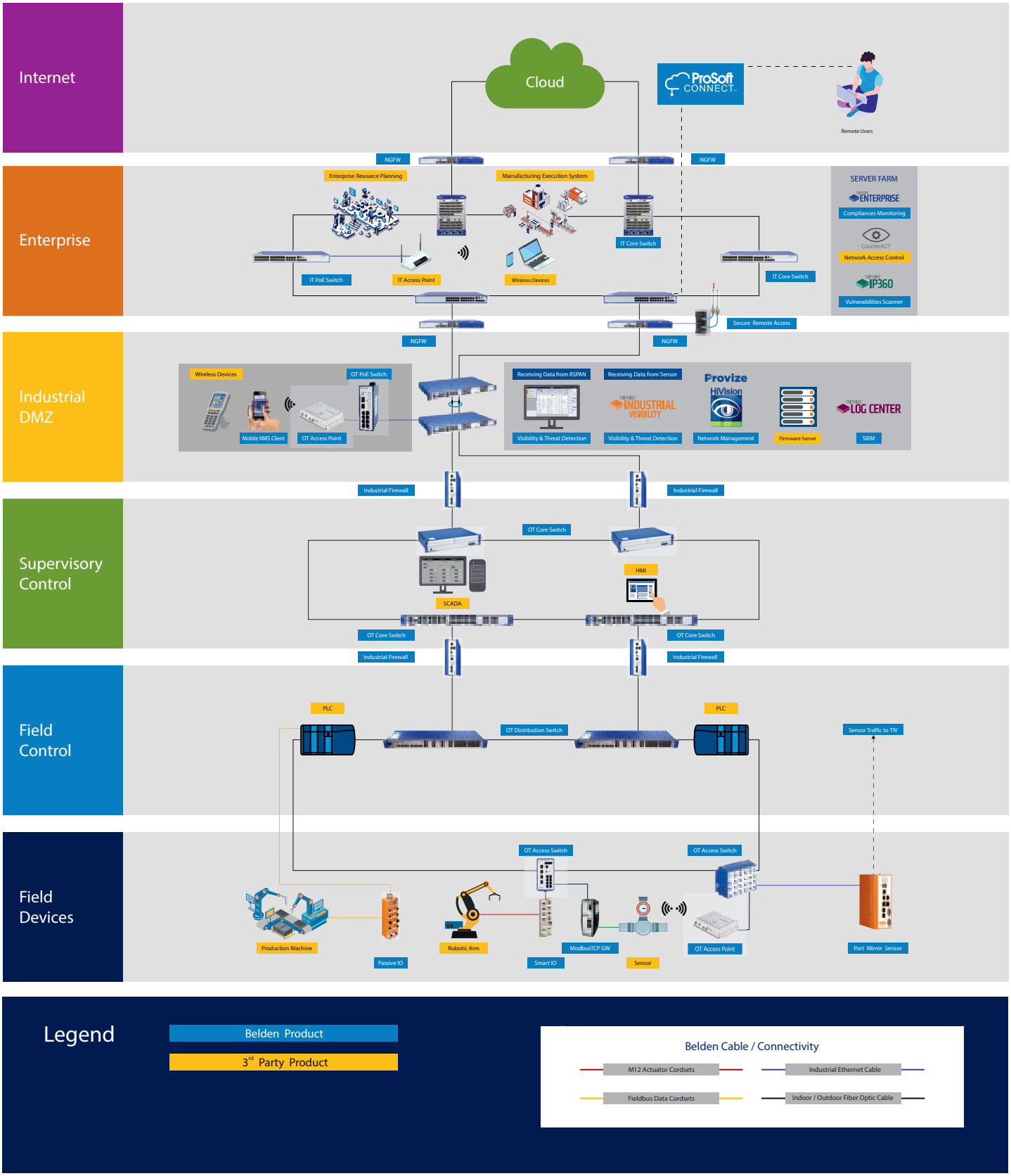


Figure 4a: Belden Industrial Automation Reference Architecture - Factory Automation

The Reference Architecture Designs include all key components from cables, connectors and wired and wireless network devices, through cyber security and protocol technologies, to Industrial Automation and Control System (IACS) plant environments and all other assets essential to production environments. It specifies a Belden validated reference architecture that informs and guides network design by end users, technology partners and system integrators.

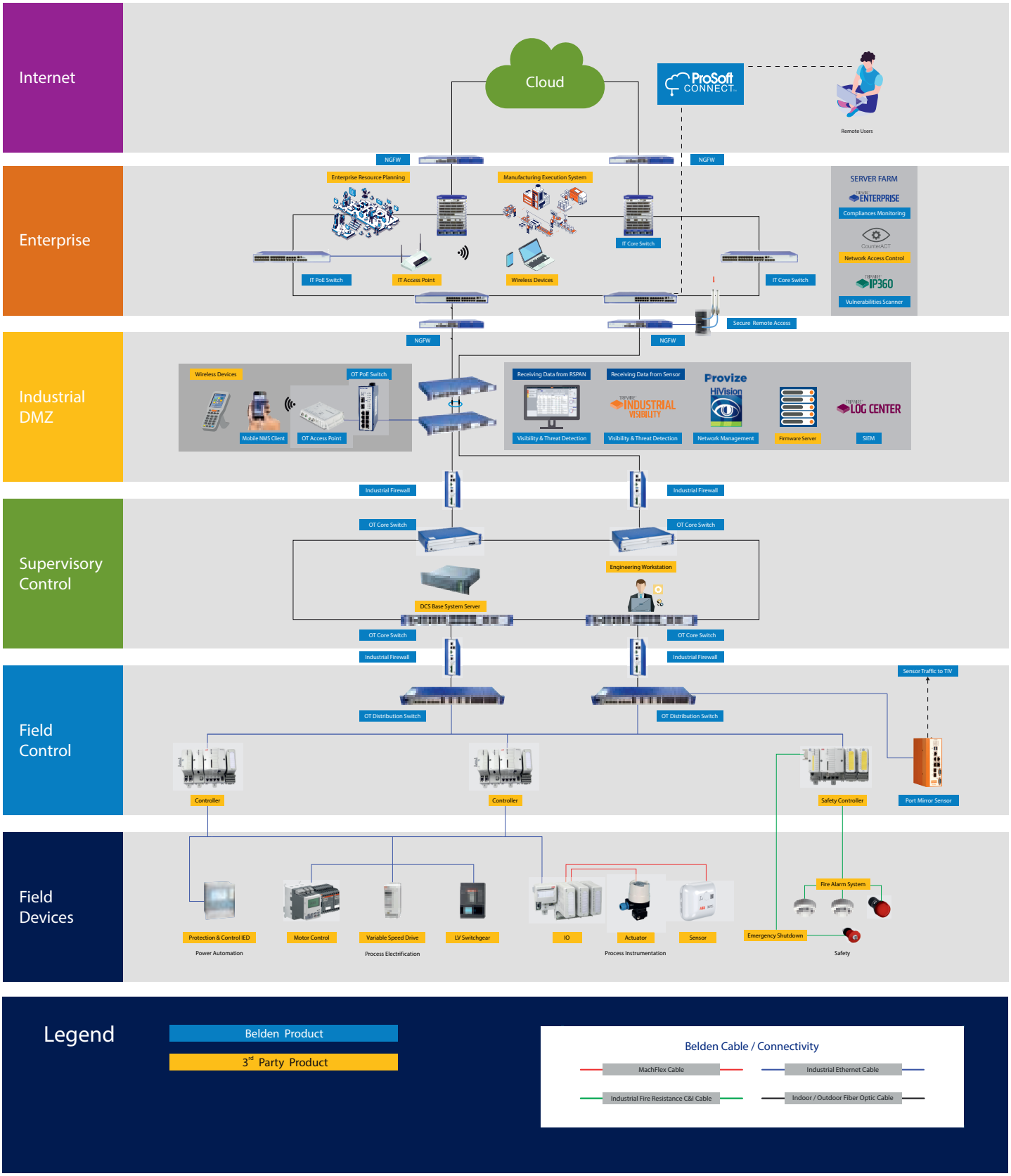
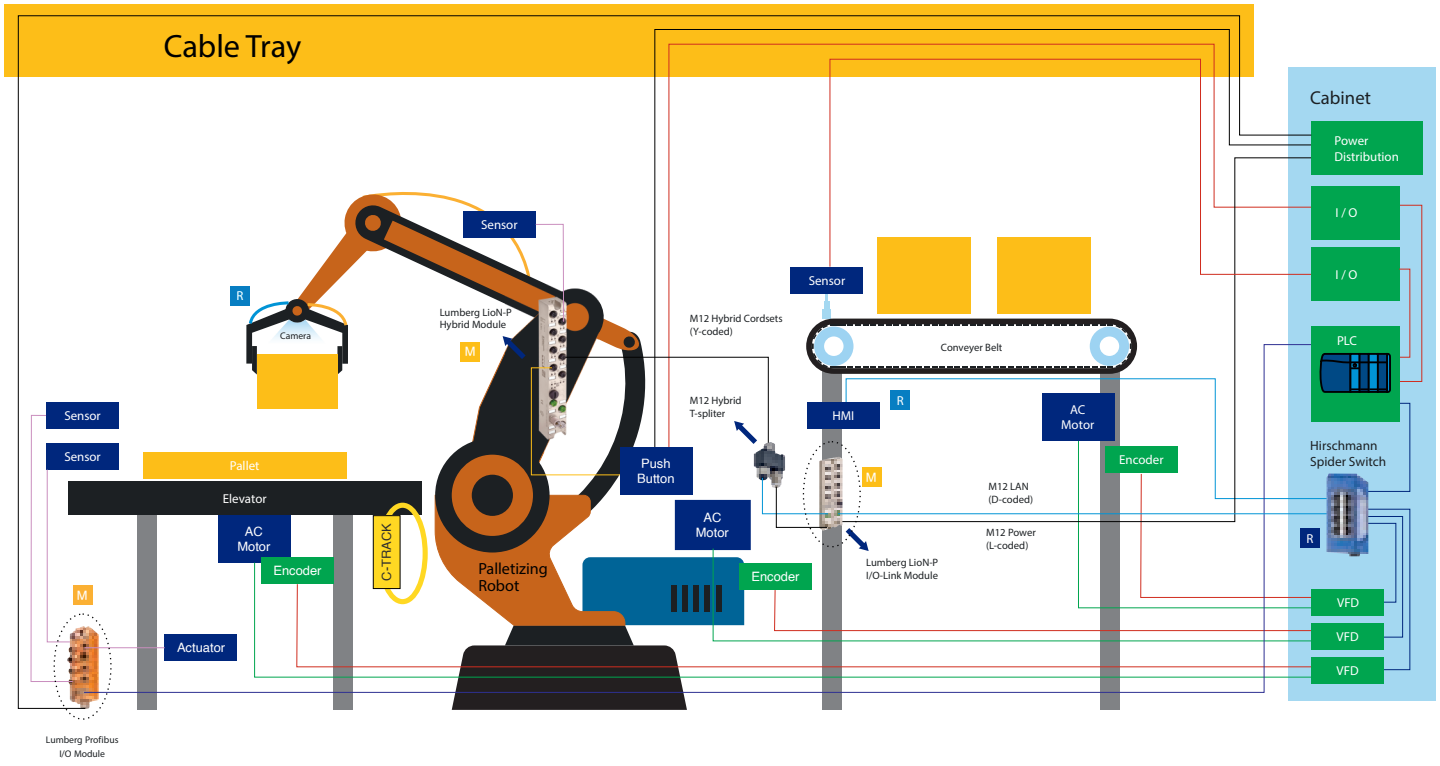


Figure 4b: Belden Industrial Automation Reference Architecture - Process Automation

Understanding the Field Devices and Integration of Our Solutions

The field devices used in the basic industrial processes of any given industry include a wide variety of sensors and actuators. These devices perform the basic functions of the IACS (Industrial Automation and Control Systems) such as driving motors, measuring physical variables, setting outputs and performing key functions like painting, welding and bending. They range from the very simple (like temperature gauges) to highly complex devices (like industrial robots) that take directions from and communicate their status to control devices in Level 1 of the reference architecture. Other IACS devices or applications may need to access field devices to perform maintenance or resolve problems.

Obtain maximum protection and performance in the field level.



Legend

- Classic Electronic Cable
- Industrial Ethernet Cable
- Industrial Ethernet Cordset
- Sensor/Actuator Cordset
- High Flexible MachFlex Cable
- MachFlex VFD Cable
- MachFlex Control Cable
- Fieldbus Cable-Profibus
- R Industrial REV Connect
- M M12 L-coded/M12 Connector/ 7/8" Power Supply Connector
- Lumberg I/O Module
- Hirschmann Spider Switch

Figure 5: Field Level Application (Robotic Palletizer)

Understanding the Field Control and Supervisory Control Levels and How Our Solutions Deliver Value Across Silos

Monitor and control mission-critical operations with precision

Field Control

The Control Level consists of controllers that direct and manipulate the automation process, primarily through the field level. In a discrete environment the controller is typically a PLC. In a process environment the controller is referred to as a distributed control system (DCS). Communication between PLC/DCS and devices at field and supervisory levels are typically based on Ethernet technology.

Hirschmann **Industrial-Grade Ethernet Switches** are specifically designed to connect industrial devices, e.g. controllers that are subject to extreme operating temperatures from - 40°C to 70°C and frequently exposed to vibrations, shocks and high humidity. They are built to comply with industrial safety requirements and approved for use in hazardous locations, making them ideal for use under harsh environment conditions. Rugged yet easy to use, Hirschmann Industrial Ethernet switches feature support for industrial protocol profiles, superior reliability, advanced security, network redundancy and easy installation and configuration.

Supervisory Control

The Supervisory Level is commonly known as the SCADA (Supervisory Control and Data Acquisition) level: the layer that contains the SCADA systems per se and their human-machine interfaces or HMIs.

SCADAs monitor and control PLCs and coordinate their functioning. The controllers in the Field Level in turn govern the processes allocated to their control.

The Supervisory Level is a central component of mission-critical OT networks in which real-time control and high availability is imperative. Key requirements on this level include safeguards against damage by harsh environmental conditions, high fault-tolerance and highly effective cybersecurity.

Highly fault-tolerant networks operate using open standard network redundancy mechanisms.

IEC 62439 defines a set of redundancy protocols for mission-critical automation networks:

- IEC 62439-1 Rapid Spanning Tree Protocol RSTP
- IEC 62439-2 Media Redundancy Protocol MRP
- IEC 62439-3 Parallel Redundancy Protocol PRP
- IEC 62439-4 High-Availability Seamless Ring HSR
- ODVA Device Level Redundancy DLR

Proprietary protocols bind users to their manufacturers, constraining customer choice. They may limit scalability and flexibility and introduce the risk that the provider will cease to support the technology.

Understanding the Field Control and Supervisory Control Levels and How Our Solutions Deliver Value Across Silos

The Hirschmann HiOS products offer the widest range of industrial open standards network redundancy protocols in a single device based on IEC 62439. They excel in interoperability, scalability and flexibility.

Integration with field devices such as Remote IOs and Intelligent Electronics Devices (IED) is straightforward. Full support is provided for standards-based redundancy protocols including MRP, RSTP, HSR and PRP.

Hirschmann HiOS supports advanced industry leading network security features that include:

- Single Sign On (SSO) via LDAP using a centralized Windows Active Directory at the Control Center
- Network protection against Man-in-the-Middle attacks using DHCP Snooping and ARP inspection.
- Access control lists
- Audit trails
- Detailed user profiles and access policies

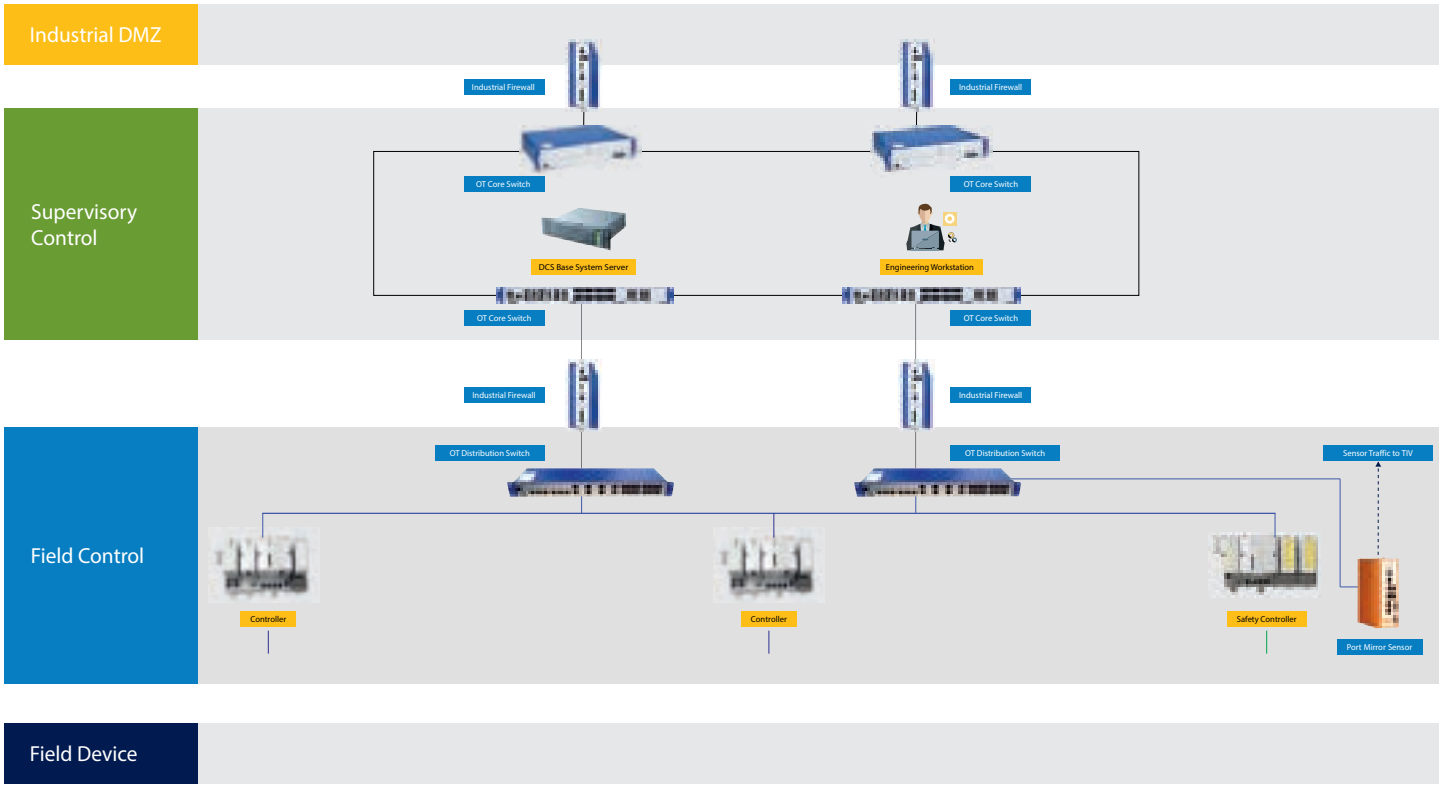


Figure 7: Field Control & Supervisory Control

Understanding the Field Devices and Integration of Our Solutions

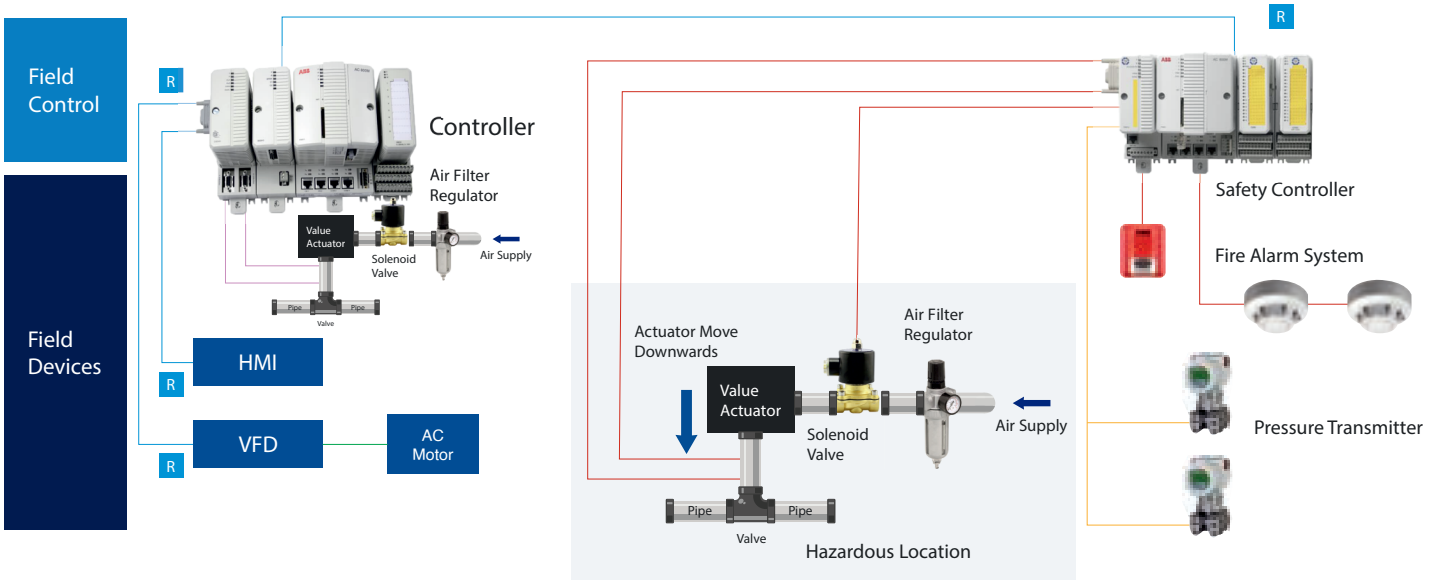


Figure 6: Field Device Application (DCS)

With the high cost of downtime in Industrial applications, Investing in Belden cables ensures maximum protection and performance.

This level where high physical stresses are typical requires durability for operational efficiency. Belden® offers highly flexible MachFlex cables for just such applications. For stationery input and output devices Belden Classic electronic, fieldbus, control and instrument cables are recommended. In addition, Belden has solutions for Industrial Ethernet connectivity that include cables, connectors and cordsets. Belden's Industrial **REVConnect RJ45** connector for example delivers fast, simple and universal cable termination. When motors absolutely must keep running you can trust Belden **MachFlex VFD** cable to provide you with the highest machine availability.

Belden **LioN-Power Active I/O Modules** support both PROFINET and Ethernet/IP protocols. LioN-Power Hybrid I/O Modules come with a compact design especially for small spaces. If reducing total cost of ownership is your priority the M12 Hybrid Y-coding technology can reduce the number of cables you need to install and enhance asset uptime and performance significantly.

The Spider, Hirschmann® entry-level rail switch that features flexible port options, cost-effectively satisfies diverse industrial network requirements at field level.

Belden cables are designed and manufactured to withstand the destructive effects of extreme temperatures, dust and oil. In industrial applications the cost of downtime can be high. Investing in Belden quality ensures maximum utilization of expensive resources, throughput and revenue.

Understanding Industrial DMZ-Demilitarized Zone and the Integration of Our Solutions

Build operational resiliency with cybersecurity

The IDMZ is a buffer that enforces data security policies between a trusted network (the Industrial Zone) and an untrusted network (the Enterprise Zone), an additional layer of defense that updates industrial devices' firmware and shares IACS data and network services between the zones. The **Hirschmann IT Raven NGFW** and **Eagle 40 firewalls** are built to support network security solutions at both ingress to and egress from the IDMZ. Because functions are separated a misconfigured rule in one firewall will not propagate through another one, significantly reducing risk and improving resilience.

Industrial Automation and Control Systems (IACS) have become prime targets for cyberattacks. In 2020 automotive manufacturer Honda fell victim to a ransomware attack, as did Norsk Hydro in March 2019, BlackEnergy malware compromised the Ukrainian power grid in 2015 and in 2010 there was a well-publicized attack on Stuxnet's uranium enrichment facility in Iran.

Such examples make it clear that IACS lacks basic security features which makes acquiring them a priority. With a portfolio built on maintaining the most critical cybersecurity practices to the highest standards, Belden and Tripwire® can provide software solutions for customers to stay on top of their game through asset management, industrial standards compliance monitoring, unauthorized change detection, vulnerability scanning and full transparency for OT environments.

Few network administrators would disagree that managing massive and complex network architecture is a challenge. To mitigate it Hirschmann's network management software Industrial HiVision provides full visibility of the whole network, managing and monitoring all network and server components even in multi-vendor environments via SNMPv3. Comprehensive security features such as authentication via Lightweight Directory Access Protocol (LDAP) permits users to benefit from a single sign-on across an organization. Customized roles enable users to be assigned with correct read/write rights for a given task. The real-time network protection and fault reporting that it provides enables customers to achieve the kind of rapid remediation that guarantees continuous uptime as well as security.

Understanding Industrial DMZ-Demilitarized Zone and the Integration of Our Solutions

The COVID-19 pandemic has dramatically expedited the needs for organizations to provide both vendors and employees with remote access to internal OT resources to perform maintenance and troubleshooting. **Prosoft® Secure Remote Access Solution** is specifically designed to address just such a need.

TIV (Tripwire® Industrial Visibility) can manage sensors throughout your OT network to provide you with complete visibility and the means to ensure integrity and resilience. With TIV you can maintain peak safety, quality and uptime using passive scanning and agentless monitoring that won't disrupt operations. It supports virtual network segmentation for implementation of protocol-specific deep-packet inspection firewall rules. With TIV you experience total ICS intelligence at your fingertips.

Moreover **Tripwire® Log Center®** brings complete, secure, reliable log collection that picks out every event of interest in the streams of data. It integrates with **Tripwire® Enterprise** and **Tripwire® IP360™** to detect and respond to anomalies and suspicious activities. This ensures the production data in real time between the ERP, MES and the workshop is always accurate, consistent and up to date.

With Prosoft and Tripwire® solutions at the Supervisory Level you can be confident that your network is world-class cyber-secure.

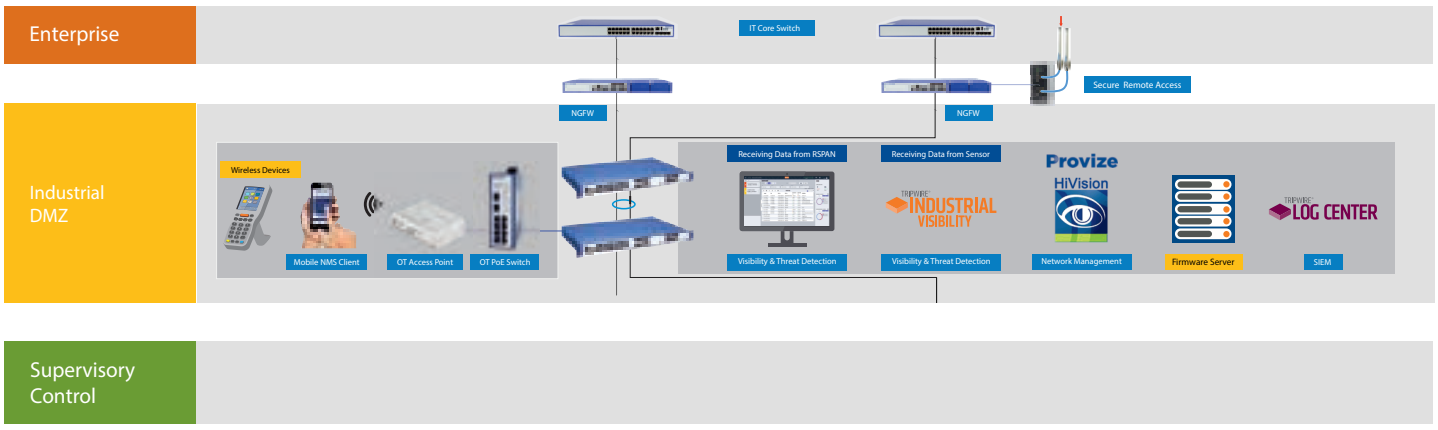


Figure 8: Industrial DMZ

Understanding Enterprise Level and the Integration of Our Solutions

Solutions to Enterprise IT problems are at your fingertips.

The Enterprise level plays a crucial role in modern day digital Industrial Automation networks, transparently connecting MES and SCADA/DCS and Historian.

It incorporates assets critical to the transformation from Industry 3.0 to Industry 4.0. Critical communication components include server farms (virtual/native cloud/server machines), distributed storage and operation servers. In the case of fog computing mechanisms distributed cloud storage is controlled at this level. Besides storage this level implements cybersecurity and network access controls, typically via central console systems

Belden's approach to solutions for the Enterprise Level can be broadly categorized in three different aspects:

> IT-OT convergence challenges for IT network administrators
> Hardware solutions for the core Enterprise networks of IA-control systems
> Software solutions for cybersecurity requirements of IA control systems

Hirschmann IT® and Tripwire® together provide the perfect solution for customers' Enterprise Level communication requirements.

Next-generation firewall hardware. Scalable, high performing switching and routing platforms.

Advanced visibility of IT-OT networks. Network provisioning and management software. Cybersecurity compliance and configuration management software.

IT-OT convergence is the new reality of Industrial Automation. Historically the Information Technology (IT) and Operation Technology (OT) user groups have functioned independently. IT-OT convergence brings new challenges to the IA-Control system user group.

The world of automation is evolving rapidly. Digitalization is entering the world of factory-floor industrial automation as more and more devices on OT networks communicate with each other and expand opportunities for data collection, analysis and monitoring and control. Put another way, digitalization brings problems to solve as well as advantages. Devising solutions will produce improvements in cross functional collaboration between IT & OT.

In describing the Industrial DMZ we offered some insights into the challenges and solutions for IT-OT converged networks. Here we focus on the perspective of network administrators.

Hirschmann IT, a Belden brand, provides high quality, high reliability, highly competitive products with rich feature sets for IT/OT convergence and IT networking.

Hirschmann IT high performance and multi purpose switches set the standard for quality, reliability and service. The full range of products offers access aggregation and a core layer of high port count switches that deliver the ever higher switching capacities needed for IT core networks.

Understanding Enterprise Level and the Integration of Our Solutions

Major challenges for an IT network administrator at the Enterprise level are:

- Lack of OT communication network visibility and control at IT network level
- Adapting best suited compliance standards for cybersecurity for the whole network
- Asset discovery and management of legacy equipment at OT
- Making IT network hardware inter-operate seamlessly with lower network levels
- Compliance with standards including IEC62443 / NIST / ISA95 / NERC-CIP for OT cybersecurity and ISO27001 / PCI DSS / HIPAA for IT

Belden provides a one-stop solution for all these issues through the Hirschmann IT Mammuthus series of core switches and the Raven range of next-generation firewalls.

Providing comprehensive solutions that fully comply with all the cybersecurity requirements specified by IT administrators for the Enterprise Levels of Industrial Automation Control System networks, Tripwire security software makes every detail of both IT & OT networks visible and provides a robust platform for managing compliance and configuration on both sides of the network.

The full range of products offers access aggregation and a core layer of high port count switches that deliver the ever higher switching capacities needed for IT core networks.

Tripwire® IP360™ and **Tripwire® Enterprise** together with Belden's exclusive partnership with Forescout bring in the Network Access Control & Network orchestration platform. Forescout detects endpoints the instant they connect to the network and simultaneously informs Tripwire IP360™ so that operators can trigger scan requests based on network activity as well as relying on Forescout policies to monitor, manage, remediate and restrict endpoints.

The seamless integration of **Tripwire®** (IP360, TE or Connect) with **Forescout** (Eyesight or Eye extend) positions Belden as one of the few providers who can offer a complete cybersecurity solution at the Enterprise Level in digitally transformed automation networks.

The combination of Hirschmann IT best-in-class, feature-rich L3 switch hardware and next-generation firewall hardware with the Tripwire-Forescout integrated solution and Belden's rich experience in OT networking and IT-OT cyber-security make our Enterprise Level and Industrial Automation Control System offering unsurpassed in the market.

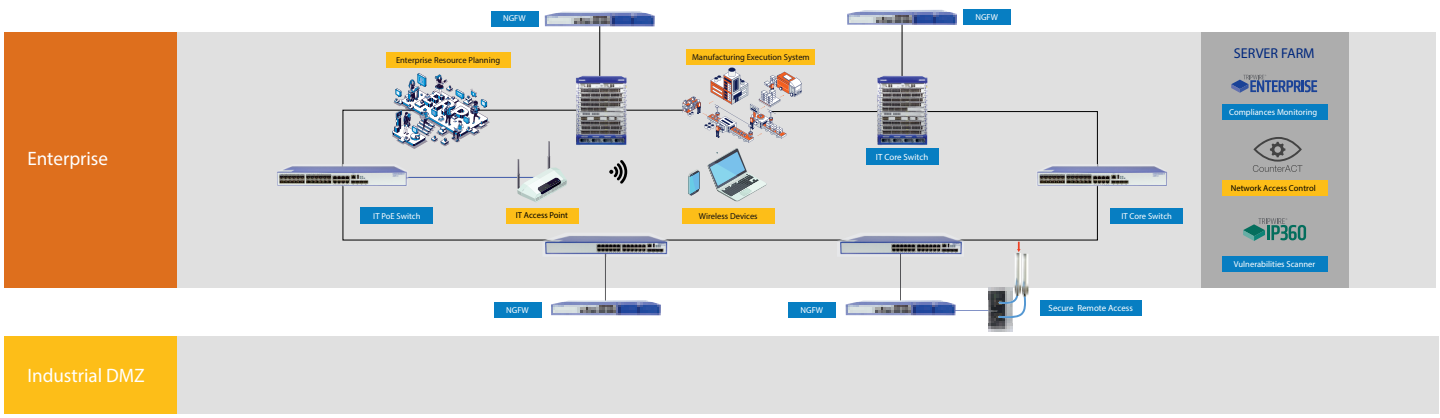


Figure 9: Enterprise Level

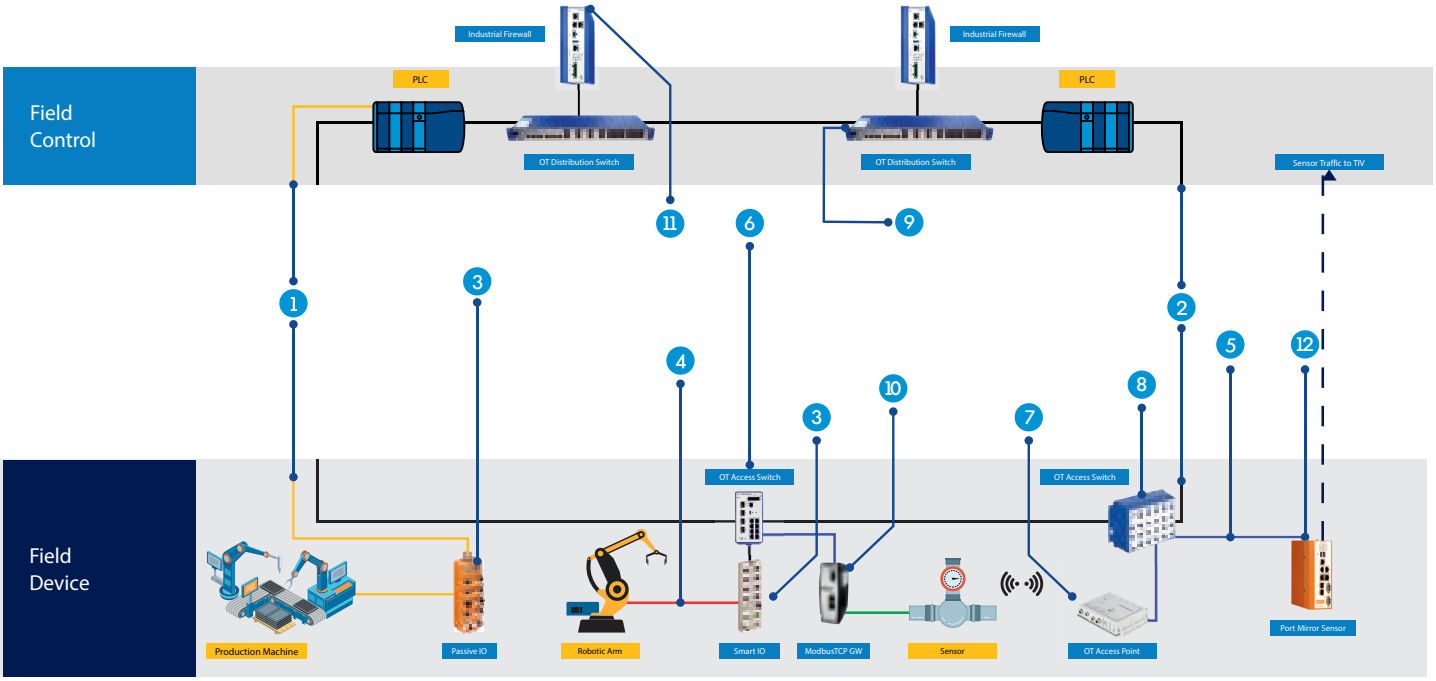
Belden Customer Innovation Center

To survive in today's competitive industrial automation landscape, IACS owners need to adapt ever more rapidly to integrate new technologies that lower total cost of ownership while consistently maintaining the highest standards of quality and delivery. Belden's Industrial Automation solutions and product technologies provide the ideal secure foundation on which customers can digitize their industrial and production environments on the way to operational excellence and superior business results. Our Industrial Automation solutions remove the barriers - security concerns, inflexible legacy networks and complexity - between customers and full participation in digitization and Industry 4.0.

BELDEN Customer ™ Innovation Center

Selected Products

Field Device & Field Control



1. Industrial Fieldbus Cables

Support all different transmission protocols and withstand harsh environment

2. Industrial Fiber Optic Cables

Support OS2, OM2, OM3, OM4 & OM5 fiber and made to withstand harsh environment

3. Fieldbus & Smart I/O Module

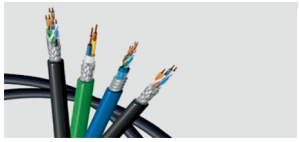
High degree of reliability in rough environmental conditions Digital Single and Multiprotocol I/O Modules for PROFINET, EtherNet/IP and EtherCAT with fast start-up

4. Sensor/Actuator Cordsets

Space-saving with M8 circular connectors with an overmolded snap-in or screw coupling

5. Industrial Ethernet Cables

Supports CAT5E, CAT6 & CAT6A
Can withstand harsh environment



6. TSN Full Gigabit Switch

Bobcat compact switch with real-time communication through time sensitive networking (TSN) technology on all ports

7. Ruggedized Access Point

BAT450-F AC industrial wireless LAN access point with 802.11ac technology in compact design

8. IP67 Layer2/3 Switch

Octopus Managed switches guarantee the highest availability in demanding environments

9. Aggregation 10G Switch

GRS106: Workgroup cost-effective full gigabit switch with Layer 2 & 3 features and high data rates

10. EtherNet/IP to Modbus TCP/IP

ProSoft Technology's EtherNet/IP™ to Modbus® TCP/IP communication gateway allows high-speed bi-directional data transfers between EtherNet/IP™ enabled controllers or devices and Modbus® TCP/IP controllers or devices.

11. Full Gigabit Multi Port Firewall

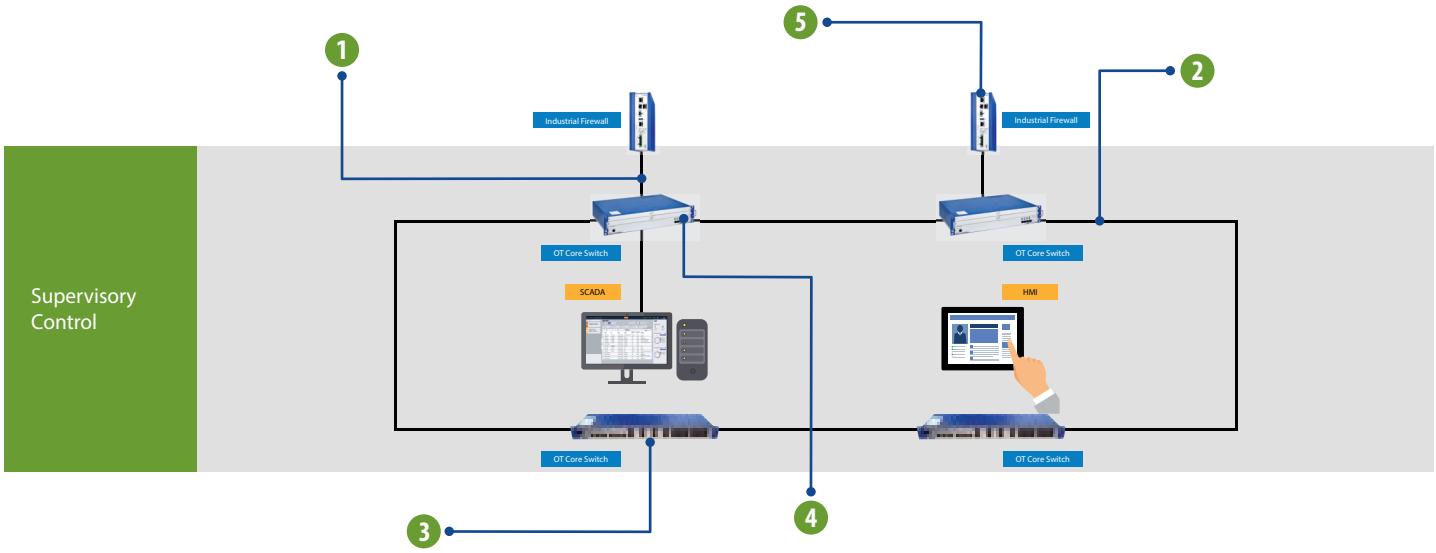
EAGLE40 offers a comprehensive cybersecurity solution to maximize uptime in today's stringent automated environments.

12. Tripwire Industrial Appliance

Industrial-grade hardware allows operational technology (OT) organizations to take full control of their CAPEX and remove their dependency on IT assets in the network.

Selected Products

Supervisory Control



1. CAT6+ Modular Patch Cords

Cords are made with **Belden's patented Bonded-Pair** cables, offering the best combination of transmission performance and physical integrity.

2. Industrial Fiber Optic Cables

Support OS2, OM2, OM3,OM4 & OM5 fiber Can withstand harsh environment

3. Full Gigabit Layer 2/3 Switch

The **GREYHOUND Gigabit Ethernet** switch is designed for use in harsh industrial environments with a need for **cost-effective, entry-level devices.**

4. High Bandwidth Backbone Switch

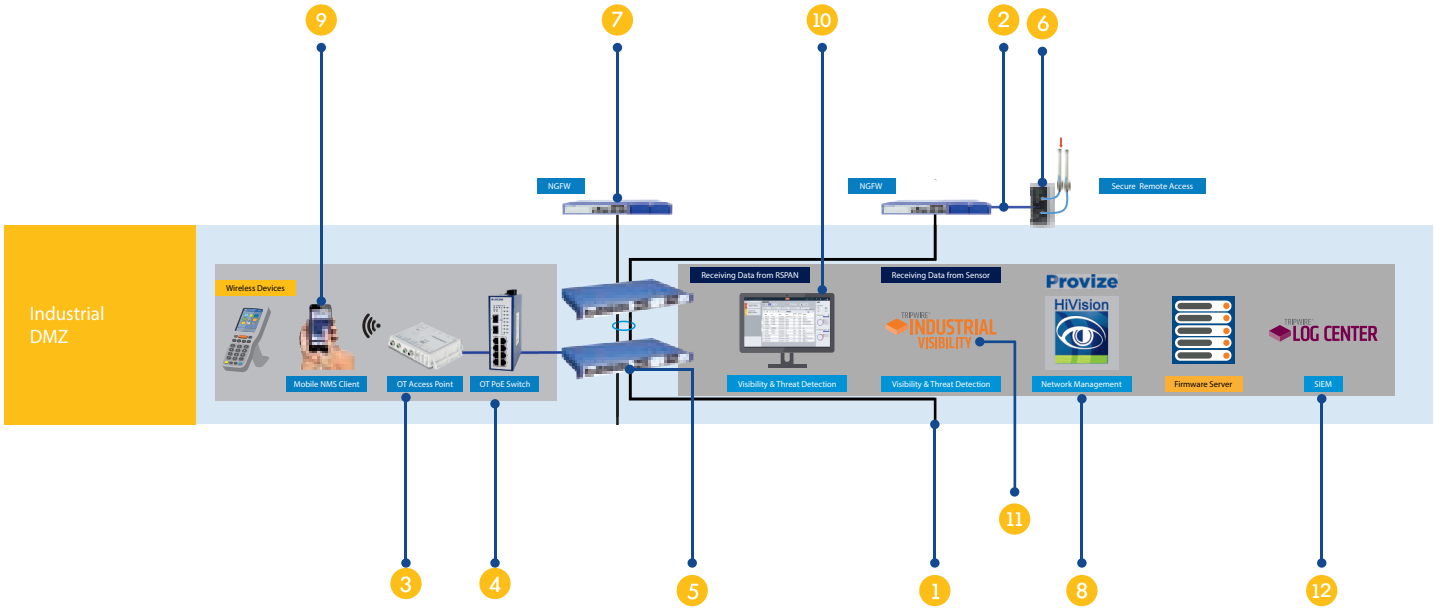
The DRAGON MACH4x00 superior **bandwidth (up to 10 Gigabit) for connecting OT and IT networks.**

5. Full Gigabit Multi Port Firewall

EAGLE40 offers a **comprehensive cybersecurity solution** to **maximize uptime** in today's stringent automated environments.

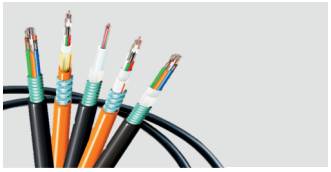
Selected Products

Industrial DMZ



1. Industrial Fiber Optic Cables

Support OS2, OM2, OM3, OM4 & OM5 fiber and made to withstand harsh environment



2. CAT6+ Modular Patch Cords

Are made with Belden's patented Bonded-Pair cables, offering the best combination of transmission performance and physical integrity.

3. Ruggedized Access Point

BAT450-F AC industrial wireless LAN access point with 802.11ac technology in compact design

4. The Full Gigabit Managed PoE Switch

Industrial full Gigabit managed 6/10 ports Ethernet switch BN44/BN48, with up to 4/8 Gigabit PoE+ port

5. Full Gigabit Layer 2/3 Switch

The GREYHOUND Gigabit Ethernet switch is designed for use in harsh industrial environments with a need for cost-effective, entry-level devices.

6. Industrial Cellular Gateway

ICX35-HWC gateway for remote connectivity applications like remote access, SCADA connectivity to remote sites, or M2M communications

7. Raven NGFW

Offer Application Identification (APP-ID), Continuous Threat Prevention and Flexible Deployment.

8. Industrial HiVision

Enables secure and easy configuration as well as the monitoring of industrial network components.

9. HiMobile App

HiMobile app is a perfect client/server solution for mobile monitoring of network nodes using smartphones or tablets - for higher network availability.

10. Awareness Platform

Tripwire Industrial Sentinel is a non-intrusive network monitoring and situational awareness platform providing visibility to and protection from events that threaten safety, productivity, and quality

TRIPWIRE INDUSTRIAL SENTINAL

11. Industrial Visibility

Tripwire provides change management, event logging, and threat modeling to help you keep your most sensitive assets out of reach of intruders.

TRIPWIRE INDUSTRIAL VISIBILITY

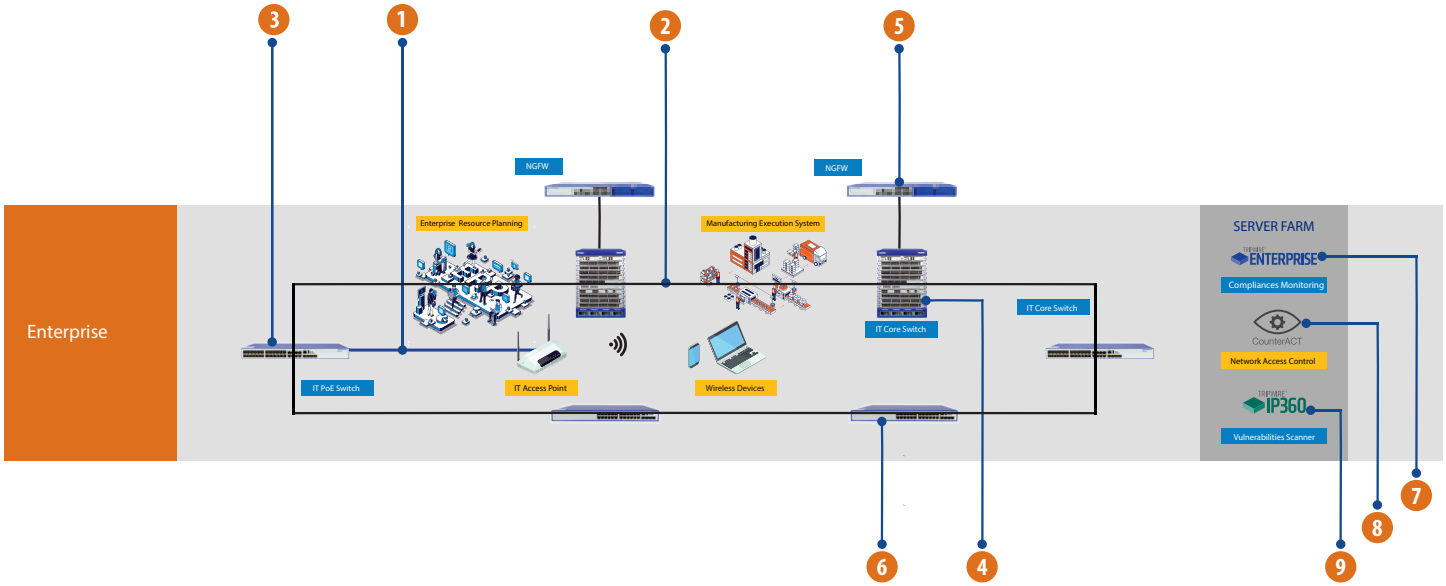
12. Log Center

Tripwire provides secure, reliable centralized log collection solution for complete OT components.

TRIPWIRE LOG CENTER

Selected Products

Enterprise Level

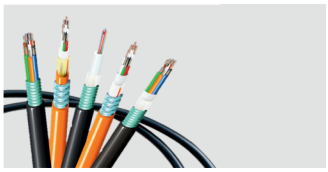


1. CAT6+ Modular Patch Cords

Are made with Belden's patented Bonded-Pair cables, offering the best combination of transmission performance and physical integrity

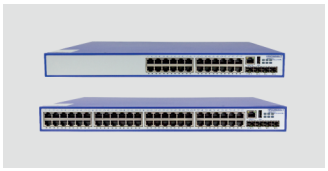
2. Industrial Fiber Optic Cables

Support OS2, OM2, OM3, OM4 & OM5 fiber and made to withstand harsh environment



3. L3 Enterprise Switch

MTS2700 series 24/48*GE PoE/PoE+ TX. 6*10GE SFP+ slots. Wire speed forwarding. Static router, RIP, OSPF, ISIS, BGP. Support -E feature set. Stacking and modular FRU PSU. Support Persistent PoE technology



4. Enterprise Modular Core Switch

MTS8000 modular core switch series with 3/6/10 slots supporting multiple types of media module cards, including 1G/10G/40G SFPP+ interfaces.

5. Raven NGFW

Offer Application Identification (APP-ID), Continuous Threat Prevention and Flexible Deployment.

6. L3 Enterprise Switch

MTS2800 series switches support wire speed forwarding, static router, RIP, OSPF and stacking. They have fixed redundant PSU and have – S/-E two different software level choices.

7. Security Configuration Management (SCM)

Tripwire Enterprise is a security configuration management suite that provides fully integrated solutions for policy, file integrity and remediation management.

TRIPWIRE® ENTERPRISE

8. Forescout Counter ACT

Asset discovery & policy based workflow Network Access Control and Segmentation Certified orchestration of applying controls to Hirschmann Classic and HiOS Switches

CounterACT

9. Vulnerability Management SW

Tripwire IP360 is an enterprise-class vulnerability management solution that enables cost-effective reduction of cyber threat risk by focusing your remediation efforts on the highest risks and most critical assets

TRIPWIRE® IP360

Headquarters

Global
Belden - St. Louis
1 N. Brentwood Blvd. 15th Floor
St. Louis MO 63105 US

Phone: +314-854-8000
Fax: +314-854-8001
info@belden.com

Division Headquarters - Americas
Belden - Richmond
2200 U.S. Highway 27 South
Richmond, IN 47374 US

Phone: +765-983-5200
Toll Free: 1-800-BELDEN1
Fax: +765-983-5294
info@belden.com

Division Headquarters - Europe
Belden - EMEA
Edisonstraat 9, Postbus 9
5928 PG Venlo, 5900 AA The Netherlands

Phone: +31-773-878-555
Fax: +31-773-878-448
venlo.salesinfo@belden.com

Division Headquarters - Asia Pacific
Belden - Hong Kong
7/F Harbour View 2
16 Science Park East Avenue Hong Kong Science Park, Shatin Hong Kong

Phone: +852-2955-0128
Fax: +852-2907-6933
hongkong.sales@belden.com

Contact us

SENDING ALL THE RIGHT SIGNALS