



Customer™
Innovation
Center

Automotive Solution Guide

How to Implement Robust Network Solutions
to Enable Production Efficiencies
for Vehicle Assembly



Table of Contents

Table of Contents	02
Purpose of the Solution Guide	03
Enabling Performance in Automotive Manufacturing.....	04
Automotive Manufacturing.....	05
Strategies for Automotive Manufacturing Improvement.....	08
Best-in-Class Network Vehicle Manufacturing	09
Element 1: Connecting Fixed Assets	11
Element 2: Connecting Mobile Assets.....	22
Element 3: Backbone Connections.....	32
Belden - The Expert for All Your Networking Needs	44





Purpose of the Solution Guide

This guide identifies challenges in automotive assembly processes and provides solutions that connect assets and workers to unlock new performance efficiencies. Following this proven, strategic approach will move your operations ahead on the journey toward a highly robust, agile, secure network solution for automotive manufacturing applications.

This guide helps you to:

- Validate the need for an interconnected operations network
- Demonstrate the process for creating that network
- Create a step-by-step plan for your robust, reliable, secure network solution design
- Identify a recommended solution package to complete each step

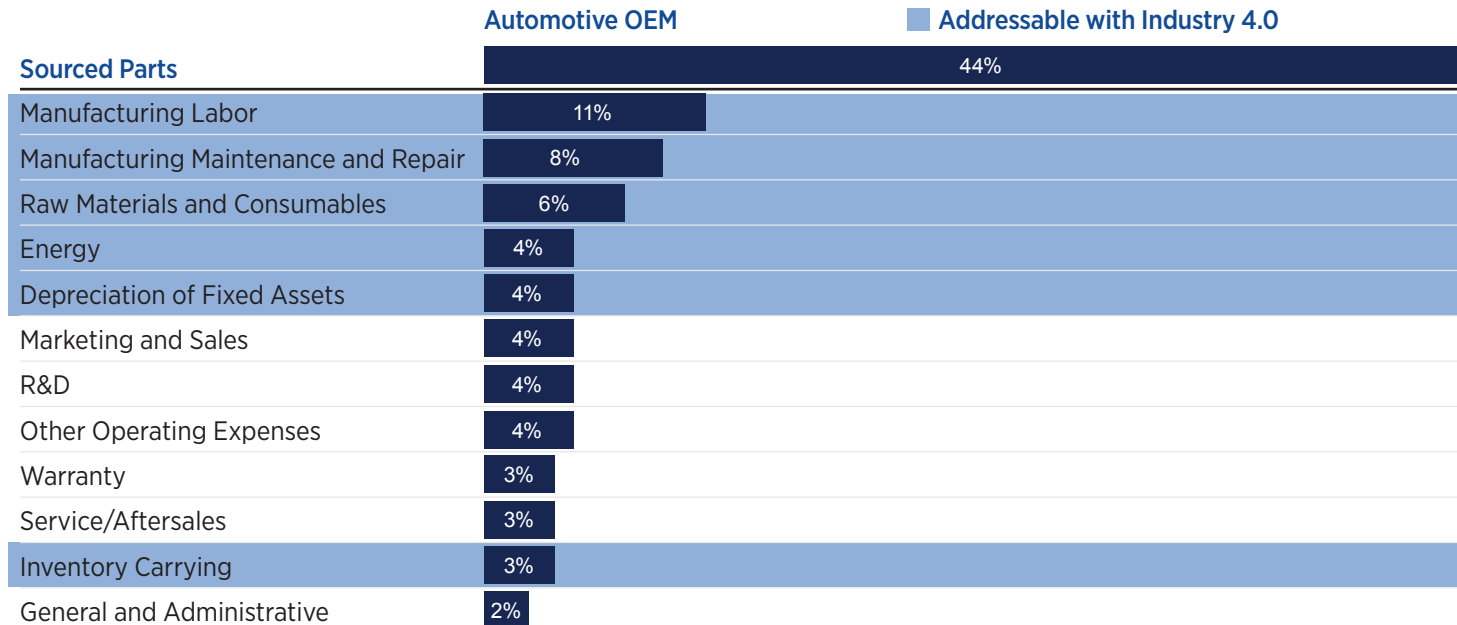




Enabling Performance in Automotive Manufacturing

Imagine responding to rising cost pressures by identifying operational efficiencies that allow you to deliver more. Industry 4.0 gives operations and maintenance teams the opportunity to leverage technology as a force multiplier. Choosing a customized Belden-enhanced network helps you capture and harness hidden inefficiencies. A customized network connects diverse production process elements and their data islands to create a holistic system. An integrated system offers your decision-makers new opportunities to make more informed choices and achieve better outcomes.

The network that underpins all aspects of production serves as the essential foundation for Industry 4.0. This data highway brings information from all layers of your operation directly to the decision-makers. In the automotive industry, operational choices significantly impact production costs—in the vehicle assembly arena perhaps more than others. Industry 4.0 can positively impact more than one-third of the costs that arise from operational decisions. Better decisions made in real time drive performance efficiencies, conserve resources, and reduce waste.



Industry 4.0 impacts
up to 36% of OEM
operations

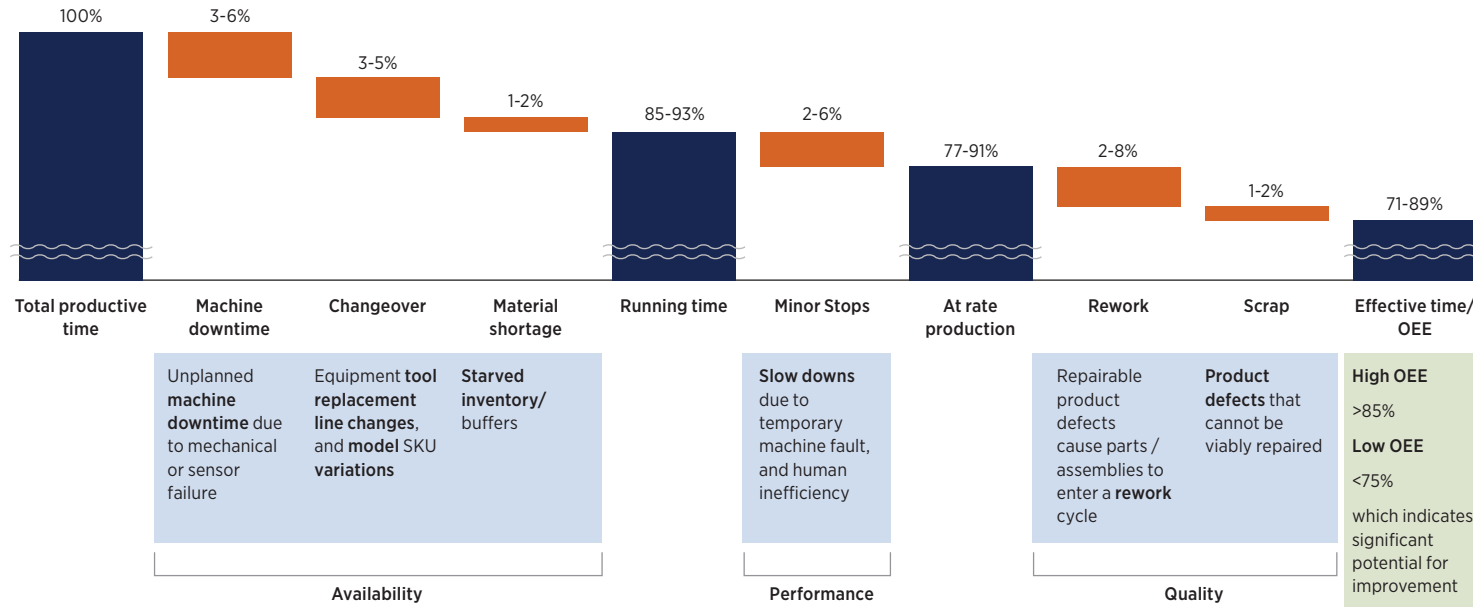


Automotive Manufacturing

Industry Snapshot

The vehicle assembly line—the final stage of vehicle production—provides the greatest share of value-added activities in a vehicle’s life cycle. On the line, a range of manual processes and automated equipment transform raw materials and prefabricated components into a completed vehicle in a prescribed color and trim.

Managing this complicated, intricate operation requires robust operational solutions. Operators must track performance, balance equipment availability, and ensure output quality. Many line managers rely on overall equipment effectiveness (OEE) as a key performance indicator (KPI).



What Is OEE?

Overall equipment effectiveness (OEE), a three-factor key performance indicator (KPI), multiplies three factors to deliver a metric reflecting how a particular system performed for a scheduled time:

- **Availability**—the uptime and downtime of a system. Divide the actual run time achieved during the specified period by the planned runtime in that period.
- **Utilization**—the production of a system. The actual amount of product produced during the specified period divided by the planned amount.
- **Quality**—the defect or scrap rate. The actual amount of usable product made during the period divided by the planned amount.

High OEE
>85%

Low OEE
<75%

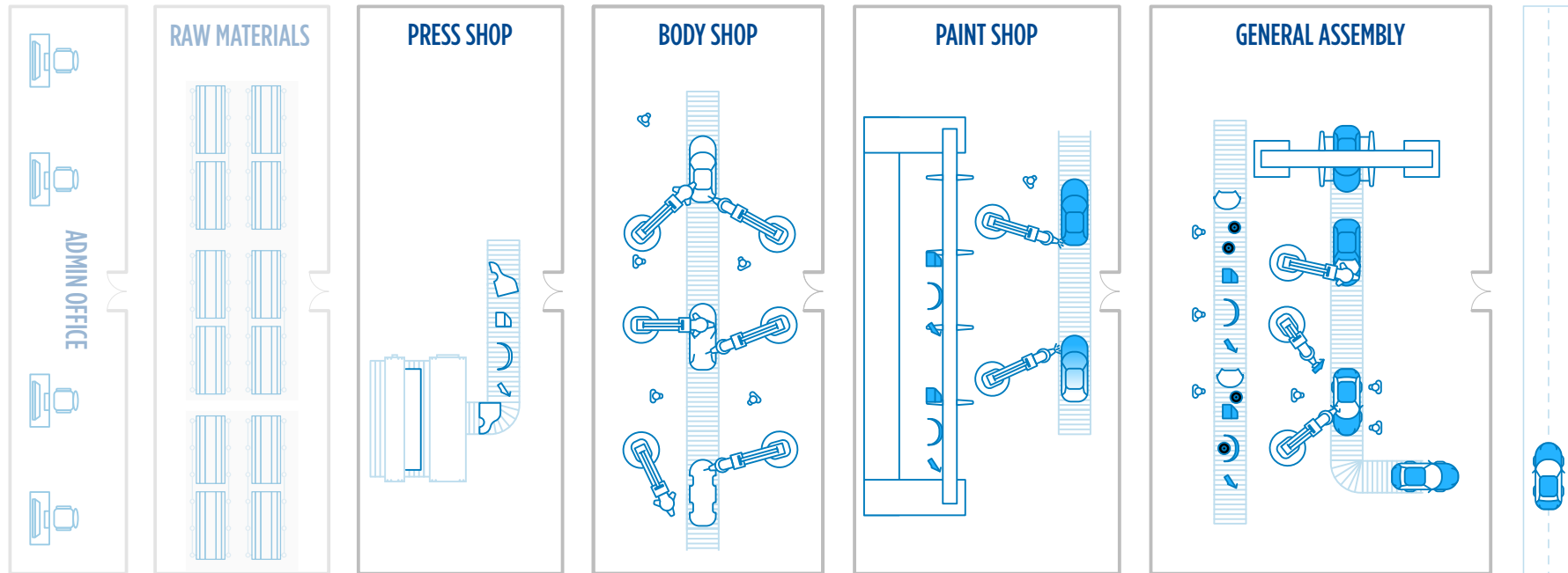
which indicates significant potential for improvement

Operation Areas

The vehicle assembly process includes four major areas of operation.

- Press Shop (Stamping)
- Body Shop (Welding)
- Paint Shop
- General Assembly

Each area can contribute inefficiencies that drive up costs. These inefficiencies often stem from common root causes.



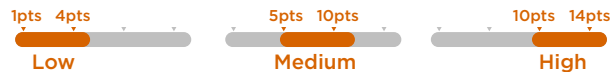


Understanding Your Process Complexity

When planning any course of action, you must first understand your current situation. In an automotive manufacturing facility, this means accurately identifying the scale of your operations, assessing your process work flows, and defining your goals. Critical dimensions to assess include:

Factor	Criteria	Low (0)	Medium (1)	High (2)	Rationale
Product variation	# trim levels	<10	10-20	>20	Drives flexibility of operations and asset management (e.g., number of changeovers per shift)
	#product SKUs offered	<1M	1M-10M	>10M	
Throughput	Production volume (parts per year)	<250K	250K-500K	>500K	Determines scale of operations and investment required
	Capacity utilization (%)	<50%	50%-75%	>75%	Drives stress placed on operating equipment
Labor force	Wages (\$US per hour, new line assembly hire)	<\$10	\$10-\$18	>\$18	Determine viability of business models for automation solutions
	Regulatory protection	No union or low union power (e.g., Meico)	Moderate union power (e.g., USA UAW)	Strong union power (e.g., Western Europe, Canada)	
Process variance	# of unique processes	<20	20-100	>100	Drives baseline operating & reporting requirements

Overall score



Digital Maturity Assessment Service

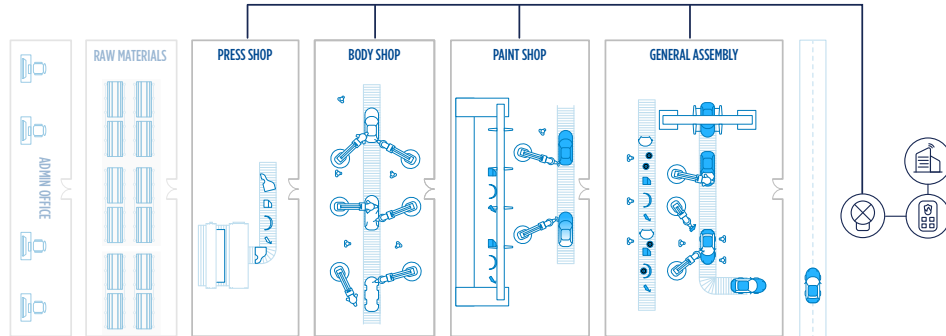
No one knows your operations better than your people. But when immersed in it over a long time, your people can develop observational bias. Belden's Digital Maturity Assessment Service brings our consultants to your environment to help you look at your business through **a new lens**.

During the assessment, Belden's consultants **map your automation journey**, starting from the current complexity of your operations, then identify opportunities to improve your effectiveness.

Strategies for Automotive Manufacturing Improvement

There are many strategies for improving operational performance in automotive manufacturing. Depending on the digital maturity and operational complexity of your processes, following one or more of these five strategies are likely to have a high impact on your bottom line.

Manufacturing Automation	Predictive Analytics	Component Tracking	Human Connectivity	OT Cybersecurity
Automation technologies help automotive facilities achieve decreased throughput, fewer minor stoppages, and better performance consistency, allowing reduced buffer sizes.	Advanced analytics software monitoring of all OT assets yields optimal predictive maintenance for minimal downtime, fewer minor stops, and less scrap from machine faults.	Managing materials with radio-frequency identification (RFID) tracking reduces part loss and buffer starvation, and prevents rework by matching bad parts to their sources.	Operators equipped with wearable technologies, like augmented reality (AR) glasses get real-time updates on production problems and immediate, accurate guidance resolutions.	Installing state-of-the-art, OT cybersecurity prevents IT attacks from harming OT systems and reduces the likelihood of downtime due to cyberattacks.



Each of these strategies relies on a highly functional, high availability network with robust connections between assets within each process area, between process areas, and between OT and IT supported networks. This guide presents Belden's solution for implementing a robust network to enable production efficiencies for automotive manufacturing.

Automotive Production Efficiency

Despite being purpose built, the four major operational areas of an automotive assembly facility share common operational challenges, namely downtime, scrap and rework, minor stops, and changeovers.

Implementing a solution affecting any of the five areas of potential in the chart at left measurably impacts each of these in all of the operational areas.

Operation	Operational challenges
Press shop	Downtime Changeovers Scrap / rework
Body shop	Downtime Scrap / rework Minor stops
Paint shop	Scrap / rework Downtime Changeovers
General assembly	Minor stops Downtime Rework

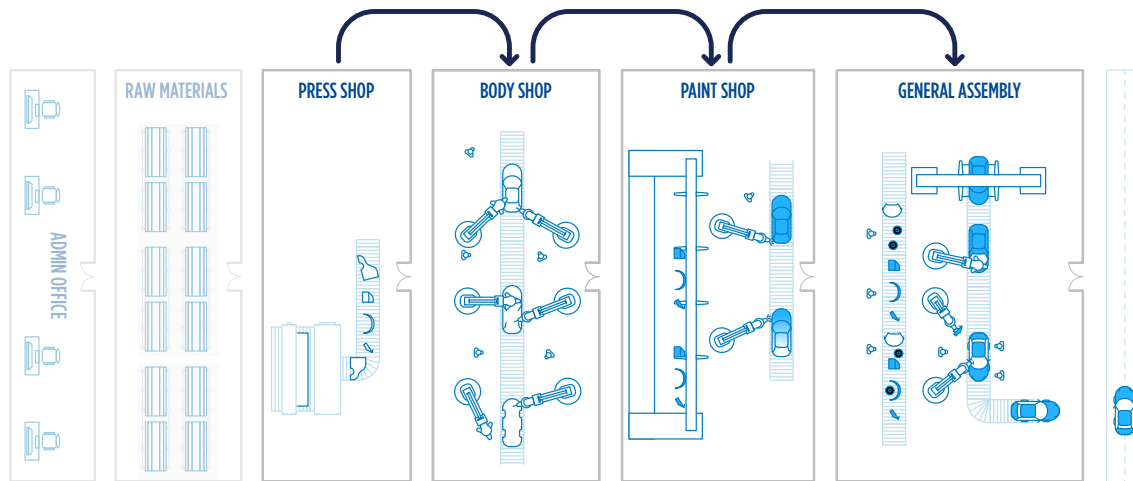
Best-in-Class Network Vehicle Manufacturing

Design Baseline

Each automotive facility presents unique challenges preventing the easy application of a one-size-fits-all solution. Fortunately, Belden experts can leverage common technologies and best practices to create a base design that is further enhanced to suit the intricacies your specific operations. Consider that a typical vehicle manufacturing facility consists of:

- Press shop (stamping)
- Body shop (welding)
- Paint shop
- General assembly

This solution guide walks you through how to design a customized network solution for a reference automotive manufacturing facility layout. The resulting network enables Industry 4.0 technologies and delivers performance efficiencies.



Project Deployment Tips

- **Assign a project manager** at the start to help define the scope of work, budgets, and timelines to ensure proper project control throughout the project's entire lifecycle.
- **Keep the lines of communication open** with the existing workforce when upgrading an active facility to ease the change and smooth the adoption of new processes.
- **Use your vendors and supply chain** to help plan the projects since their knowledge of product offerings and market forces can ensure optimal solutions and prevent procurement delays.
- **Accurately document** device configurations, connections, and physical locations to simplify system maintenance and extend the life and flexibility of your network.
- **Keep in touch** with vendors after project deployment to stay informed of technology changes, critical updates and vulnerabilities, and new best practices for continuous improvement.

Best-in-Class Network Vehicle Manufacturing

The Problem

Many vendor solutions provide operational visibility and improve key performance indicators (KPIs) but come with hidden costs. Existing network limitations, long cybersecurity approval processes, and high connectivity costs create barriers to effective change. Processes and facilities often become siloed with differently connected devices and patched solutions that result in costly maintenance, and unpredictable performance and reliability.

The Solution

Ideally, vehicle manufacturers should approach digital transformation holistically. Investing in a robust, secure, scalable network to meet current and future demands gives you the best possible outcomes and most profitable return on investment (ROI). Belden mapped a holistic approach to the network design for automotive assembly based upon three essential elements required for success in creating seamless connections between your production plant assets and personnel. The elements follow a natural order that makes it easily scalable, however, they can be deployed in any sequence as required for a given operation.



Element #1:

Connect Fixed Assets

- Robots and cobots
- Process equipment
- Machine interfaces and controls
- Process and asset monitoring devices

Element #2:

Connect Mobile Assets

- Material delivery vehicles
- Handheld and wearable devices
- Smart tools
- Mobile workstations

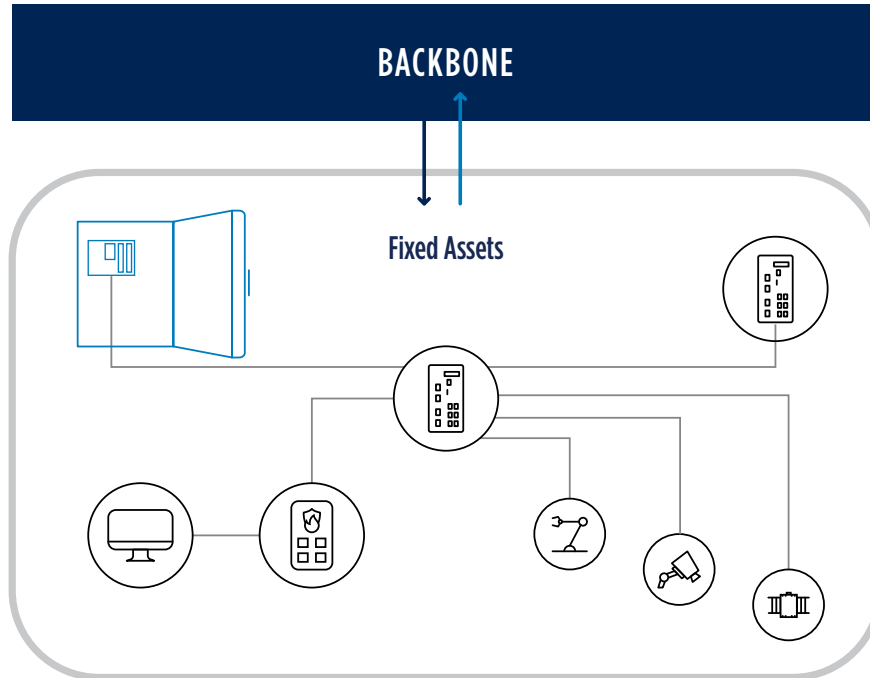
Element #3:

Create a Network Backbone

- Secured zones
- OT aggregation
- IT/OT connections
- Secure remote access

Element 1: Connecting Fixed Assets

More than just a building, your automotive manufacturing facility is a network of interconnected assets. Each asset presents unique needs and challenges. Fortunately, many of these assets fall into similar equipment categories. Grouping similar assets helps streamline planning and management of integration. Some assets are mobile, while others work in a relatively fixed location. Looking at fixed and mobile assets separately helps isolate their needs. A cohesive system integrates fixed assets within each zone and throughout the entire OT network, creating a scalable network that accommodates change over time.







What are Fixed Assets?

Fixed assets may not be “fixed” in a single location. For example, flexible and extendable conveyors are generally considered fixed because they have **a base point that links to the rest of the facility**. Even equipment that can be redeployed on demand can be considered fixed because it **does not roam** around a facility or a work cell during operation.

Element 1: Connecting Fixed Assets

Understanding the Fixed Asset Network

Robots and Cobots	Process Equipment	Machine Interfaces and Controls	Process and Asset Monitoring Devices
			
<p>Industrial robots play many roles; “pick and place” operations for loading and unloading and motion path operations, like welding and painting - all enhanced by integrating with control systems to precisely coordinate the timed movement of multiple robots. Advances in collaborative automation allow cobots to work more closely alongside humans, which requires additional integration with safety systems to ensure maximum protection for workers, products, and automation assets.</p>	<p>Discrete operations usually take momentary problems in stride, but dire consequences may result from interrupting continuous flow. Consider a heat treatment operation like a paint oven. The loss of even one data interval can trigger a system shutdown. Process equipment may produce less traffic volume but overall efficiency still requires a consistent flow.</p>	<p>Machine interfaces and controls provide inputs to assess the environment, outputs to interact with it, and data to influence controller and operator decisions. Product and machine I/O points drive units, robotic manipulators, and safety systems. Control units communicate to pass product between machine cells. The human-machine interface (HMI) allows operators to interact with the machine cell. All connections must be reliable, robust, and time-sensitive.</p>	<p>Process and asset monitoring devices stream data from the field to remote datastores. These devices can include camera systems for quality control and area monitoring, stand-alone sensors for gathering quantitative data, devices deployed inside systems reporting through their control systems, and display boards that pull information from analytical engines fed by the monitoring devices themselves.</p>
<p>Important considerations:</p> <ul style="list-style-type: none"> • Degrees of freedom and amount of articulation • Complexities of the operating environment, such as nearby welding stations or neighboring drive units • Frequency of end-of-arm tooling changes 	<ul style="list-style-type: none"> • Parameters to monitor • Level of remote process control 	<ul style="list-style-type: none"> • Whether to connect directly to the controller or route through the network • Industrial protocols for motion control and safety 	<ul style="list-style-type: none"> • Type of data transmitted • Data update rates • Location of data storage on the network • Power over Ethernet (PoE)

Element 1: Connecting Fixed Assets

Designing for Fixed Asset Connections

Connections for fixed assets require special consideration. For example, non-deterministic network technologies, which take less time to configure and suffice for many enterprise-level IT connections cannot deliver the precise performance the industrial environment requires. In many vehicle production processes, deterministic networks—though they take more time to install—provide essential safeguards and control.

Fixed assets' messaging protocols vary. They may include raw electrical signals, basic serial data, managed fieldbus methods, or Ethernet standards. Each method presents idiosyncrasies and often, a single system blends more than one method. Usually, the different protocols must be converted to a common format, but, regardless of the protocol, each connection node on the message path must be compatible.

When specifying physical cabling to transport signals, many considerations apply. The cable must match the required protocols and data rates. Ruggedized cables ensure consistent performance. For example, cables laid near welding stations and other high-temperature operations need special jacketing to prevent heat damage. Each run's end-to-end length impacts the quality and speed of transmissions. Plus, the design must:

- Allow room to maneuver as sections articulate,
- Respect minimum bend radius and
- Avoid snags that could cause damage.

Ingress protection (IP) ratings matter for fixed asset connections. While the lower cost of equipment with lower IP ratings may seem attractive, designs that use them must include an enclosure for better protection, adding unnecessary complexity and expense. Devices with ratings of IP65 or IP67 can yield cost savings. They require no cabinet, provide greater visibility and easier access, allow safe wash downs, and avoid potential arc-flashes when opening cabinets.



Deterministic Networking

Deterministic networks prescribe behavior such as when devices communicate, which network paths are used, and how and when systems fail over. They deliver predictability at the cost of the increased effort required to configure and maintain the network.

Non-deterministic networks allow the system to configure and maintain itself. Devices negotiate for the connection parameters and network paths, simplifying deployment at the cost of predictability.

Ingress Protection Ratings

Enclosures housing electrical equipment must prevent contact with internal hazards and ingress of foreign objects, dust, humidity, and water. In the ingress protection (IP) rating system adopted by many standards, such as DIN EN 60529, a two-digit code describes the protection level the casing provides. Common industrial ratings include:

- **IP20 or “finger safe”** protects against objects >12.5 mm in width.
- **IP30 or “probe safe”** protects against objects >2.5 mm in width.
- **IP65 or “wash-down”** is dust-tight for up to 8 hours and protects against jets of water.
- **IP67 or “immersion”** is dust-tight and protects against water up to 15 cm in depth for 1.5 min.

Element 1: Connecting Fixed Assets

Robots and Cobots

Robotic systems bend and twist in amazing ways, sometimes with incredible speed and at intense frequencies. A robot's cabling must handle millions of bending and twisting cycles to avoid downtime for cable replacements. Coupling shorter links in these conditions allows for easier replacement, and wireless links avoid the problem entirely.

As end-of-arm tooling grows in complexity, the extra weight adds stress to the manipulator's joints, requiring stronger actuators. Moving I/O connections to the base of the robot or cobot can reduce end-of-arm weight but adds more cabling. Using slim I/O distribution blocks saves on the weight and using them to aggregate connections on the arm reduces the cabling needs. This simplifies tool changes, decreasing change-over time.



Process Equipment

Sensors in process areas of an automotive facility are more likely to measure continuous parameters, like pressure, flow, and viscosity. When their data flow is interrupted it forces the supervisory control and data acquisition (SCADA) to react and sometimes interrupt the process.

Interrupting any operation increases waste and cost, but process equipment is even more susceptible. As interruption costs increase, so does the criticality of the network that connects the equipment. For example, paint shop ovens, considered a continuous process, require precise control of temperature and drying time to ensure quality. Interruptions can spoil the finish badly enough that it can't be recovered.

Such critical processes require the network-level redundancy offered by managed Layer 2 switches to reduce interruptions and ensure continuous process visibility for the SCADA and other systems.

Machine Interfaces and Controls

Localized management of end devices for machine controls enables more responsive, cost-effective systems. These distributed control systems (DCSs) communicate with each other to synchronize movements, match statuses, and coordinate hand-offs within the process. Similarly, distributed I/O blocks funnel data to and from the control systems, often over the same networks, reducing control requirements.

Making effective use of these control architectures requires a thorough understanding of their limitations. For example, industrial and Internet of Things (IoT) devices are often limited to a Class C network address range (192.168.1.xxx), which can lead to address conflicts that require network address translation (NAT) to resolve. Similarly, motion control and safety systems often have implicit requirements for carefully managed network latency using synchronization protocols.

Network Address Translation

Network address translation (NAT), formalized in IETF standard RFC 3022, maps an internet protocol (IP) address from one group to another in a second group. Typically, an infrastructure device serves as a gateway to a network segment and is configured to overwrite the source and destination IP address of each packet that flows through it. In effect, NAT masks IP addresses of protected devices.

Time Synchronization

Synchronized clocks simplify matching events across devices, and some use cases require it. Several protocols may be mixed and matched depending on the application of a network segment.

- **Simple network time protocol (SNTP)** is a client-driven adaptation of network time protocol (NTP), RFC 5905, that syncs to within a few hundred ms, making it well-suited to most applications
- **Precision time protocol (PTP)**, IEEE 1588, is a server-driven method that syncs to within a few μ s, making it preferred in applications like safety or motion control systems
- **Time-sensitive networking (TSN)**, IEEE 802.1Q, is a managed messaging protocol for Ethernet to enhance determinism that can be adopted in synchronized networks.

Element 1: Connecting Fixed Assets

Process and Asset Monitoring Devices

The first step to managing anything is to monitor it. Sensors and devices deployed to report on industrial processes feed data to a wide range of analytics engines, empowering resource planning, predictive maintenance, process optimization, environmental emissions compliance, and more. The equipment can be:

- Stand-alone like a gas monitor on a smokestack
- Deployed onto assets to monitor their performance like an ammeter on a power feed
- Self-reporting through parameters of control equipment, like an operations rate



A wide array of possible data sources exists.

As with other fixed assets, the physical location of process and asset monitoring devices affects their connections. To reach plant extremities may require long cable runs, driving a need for optical media. A mix of managed and unmanaged devices can extend the range and reach of a network to ensure consistent, reliable connections.

Bandwidth requirements also vary. Environmental monitoring sensors may only track a few parameters with update intervals of several minutes. Self-reporting data performance machines and equipment usage tracking sensors can manage a larger number of data points and update them much more frequently. Vision systems to evaluate production quality or monitor a facility area are an example of extreme bandwidth applications with the image resolution and the camera's frame rate dictating bandwidth, and where the video stream goes in the network impacting the speed requirements for each device along the way. Part inspection systems tend to use high resolution but operate in a localized environment, whereas monitoring cameras use high compression rates to send streams farther across the network.

When using Power over Ethernet (PoE), consider the overall power budget of the network switch when determining the maximum number of connected cameras. Proper planning and use of PoE greatly reduces the overall cost of camera installation with only a marginal increase in network infrastructure.

Edge computing devices aggregate data to reduce the cabling requirement for endpoint sensors of varying connection types and protocols. Instead of requiring connection to the backbone individually via protocol gateways, their signals are aggregated, stored for a time, and presented from a centralized location via methods such as OPC UA or MQTT.

Managed Versus Unmanaged

Network infrastructure equipment, like switches, may be passively controlled, actively controlled, or somewhere in between. The amount of control falls on a spectrum:

- **Unmanaged**—Used to extend the range and reach of a network, they handle smaller amounts of traffic, but because they typically lack an internet protocol (IP) address of their own, they offer no diagnostic information and cannot contribute to a cybersecurity strategy.
- **Managed**—Creates the core and aggregation layers of a network, providing the capacity to handle large amounts of traffic, allowing for deterministic behaviors, and providing a management interface for everything from disabling ports to defining routes through a network to delivering full diagnostic information about themselves and their connections.
- **Lightly Managed**—Aims to bridge the gap between managed and unmanaged devices, handling smaller amounts of traffic but typically with an IP address and a user interface to perform some management and diagnostic functions.

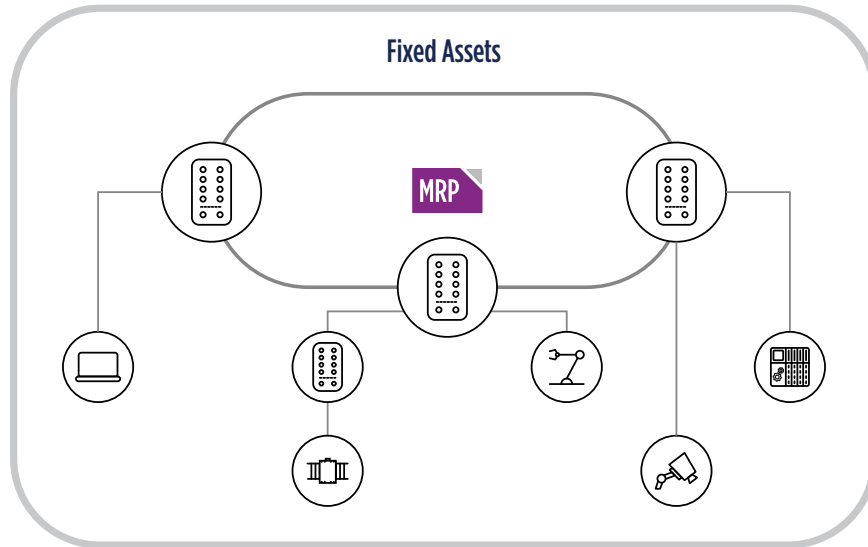
Power over Ethernet

Power over Ethernet (PoE), IEEE 802.3, allows devices to be powered by the data connection. The standard specifies the power per port and allows devices to reserve power from the switch. The ability to override this is important to maintaining an overall power budget.

- IEEE 802.3af (PoE), 15.4W per port
- IEEE 802.3at (PoE+), 30W per port
- IEEE 802.3bt (PoE++ or 4PPoE), 100W per port

Element 1: Connecting Fixed Assets

An Example Fixed Asset Architecture



Planning Network Redundancy

Media redundancy prevents single points of failure in industrial communications networks. If an automated production line has a single point of failure, the communications network can be completely disabled, causing costly consequences. With redundant structures, a single failure causes a degraded state, but communications remain viable. The redundant system enables continuous operation until a repair can be carried out to restore the fault-free state.

Network Redundancy Protocols

- **Rapid spanning tree protocol (RSTP)**, IEEE 802.1D, uses bridge protocol data unit (BPDU) messages between switches to determine the optimal network path and disable redundant connections. If the network changes (for example, a physical connection fails), paths are recalculated and alternative links are activated to restore communications. RSTP operates in many topologies and supports higher numbers of switches; however, RSTP does not guarantee deterministic failure behavior. Reaction times depend on where the failure occurs and vary between <100 ms to several seconds.
- **Media redundancy protocol (MRP)**, IEC 62439 2, an industrialized protocol for ring topologies of ≤50 devices, ensures deterministic behavior with failover times from 10 ms to 500 ms, depending on chosen parameters. A switch designated the media redundancy manager (MRM) sends test frames to probe the network while blocking one of its ringed ports. If the test frames do not flow through the ring (for example, because of a device failure or a defective media connection), the MRM will open the previously blocked port.
- **Parallel redundancy protocol (PRP)**, IEC 62439-3, uses two independent network paths to send duplicate frames between end devices, ensuring messaging between double attached nodes but increasing network traffic.
- **High availability seamless redundancy (HSR)**, IEC 62439-3, produces duplicate packets like PRP. However, HSR is optimized for ring topologies where both ports of double attached nodes connect to the same network. The standard allows for 512 nodes, but practical considerations typically limit effective HSR networks to <50 nodes per segment.



Element 1: Connecting Fixed Assets

Securing Fixed Asset Connections

Fixed assets hold a high level of criticality within any industrial network. Protecting and securing them against threats helps maintain network integrity. While not all threats target vulnerabilities or are necessarily malicious, the recommended measures for all threats apply.

- 1. Change default user credentials.** Management interfaces commonly ship with default credentials. Changing these usernames and passwords after asset commissioning helps overall security and may be a regulatory requirement.
- 2. Restrict management access.** Restricting access to the management interface adds a layer of security. Allowing admission only from specific, known internet protocol (IP) or media access control (MAC) addresses – and enabling read-only access on critical devices – prevents unauthorized or inadvertent access or changes to secure automation controller interfaces.
- 3. Create access control lists.** Use upstream network infrastructure to create a series of access control lists to prevent unauthorized read/write access to critical fixed asset control systems.
- 4. Disable unused ports.** Active ports present risk. Disabling unused ports, either statically from the device's management interface or dynamically from network management software, makes it more difficult for unauthorized devices to gain network access.
- 5. Establish zones and conduits.** Defense-in-depth strategies logically segment networks to contain traffic to within the area. Securing network segments against issues in other segments improves overall network efficiency by reducing bandwidth consumption.
- 6. Enforce traffic rules.** Ruggedized industrial firewalls deployed in the field protect devices that cannot otherwise protect themselves. These devices can hide the addresses of vulnerable devices through NAT and enforce address and port requirements on connections. Advanced units provide stateful packet inspection (SPI) and deep packet inspection (DPI). The most advanced units learn and dynamically create rules based on traffic.
- 7. Keep systems updated.** Firmware updates and software patches are released for a reason. Cyber threats are always evolving, and your networks need to be updated to keep pace. That said, patches and updates should be tested before being rolled out to ensure compatibility with your production environment.

Firewalls

Firewalls monitor and protect network connections. Most industrial devices cannot protect themselves and require an industrial security appliance to firewall hardware connections.

Firewalls implement a range of protection methods depending on the needs of an application:

- **Whitelisting/blacklisting** creates a list of source IP addresses allowed or prohibited from communicating through the firewall.
- **Stateful packet inspection (SPI)** allows inbound message traffic only when a corresponding outbound connection exists.
- **Deep packet inspection (DPI)** allows message traffic between approved devices like a whitelist but also breaks down the message to validate that it adheres to a given protocol's required format. It can also take the next step to validate that a message is allowed to target a specific memory register on the target device.





Element 1: Connecting Fixed Assets

Deploying Connections for Fixed Assets



Installation

Cable installation affects network connections; respect minimum bend radius and maximum pull tension, properly manage cable slack to allow for operational articulation and maintenance, follow guidelines for cable lengths, and prearrange a cable termination standard like Telecommunications Industry Association (TIA) 568A or 568B.

A qualified installer should deploy cable runs and test them with a device like the Fluke DSX 8000 to confirm cable terminations and length.



Configuration

Networked devices need addresses. Some communication protocols automatically assign them, like Ethernet's dynamic host configuration protocol (DHCP); however, OT networks generally need to define addresses statically for deterministic operation.

Network infrastructure devices like switches and firewalls must be configured, and communication modules must be loaded with the interface profile for slaved devices, such as the .EDS file for EtherNet/IP or .GSDML file for PROFINET. Some devices allow these settings to be applied offline, speeding deployment.



Go-Live

As devices are commissioned, backup their configurations and archive the backup in a safe, secure location. Record the location of each asset so it can be found again, and add to device IDs when possible.

When your network goes live, validate the connections. The system should establish the necessary connections when brought online, but active testing should confirm everything will run as expected.

When all the devices are connected, disable unused ports to prevent access by rogue devices and keep individuals from accidentally introducing instability to the network.

Communications Cabling

- Ethernet is standardized by IEEE 802.3, but other standards have made variations. **Clearly specify the standard or style of cabling.**
- The RJ-45 connector is a common termination for Ethernet cabling, but industrial applications often benefit from ruggedized versions that increase durability. Migration to a **threaded circular connector further enhances reliability.**
- Cable termination is prone to errors that impede messaging or bring down entire network segments. **Implement a quality control program to validate cables** and avoid issues.
- Cables are most effective when used within their specifications. Excessive heat or violations of the minimum bend radius negatively impact their performance and risk communication issues.
- Messages can be masked and disrupted by noise. Cable can pick up noise from sources that may not even be in contact with the cable itself, such as HVAC equipment and drive units. **Properly shielded and grounded cabling mitigates adverse effects.**
- **Electrical message signals degrade over distance**, so protocols and standards often specify a maximum cable length (for example, traditional Ethernet is limited to 100 meters). Exceeding these limits can have serious repercussions.
- **Not all cables are created equal.** The wide range of armoring styles, and materials got insulating and jacketing let you optimize efficiencies. For example, some cable constructions may not need a conduit in certain situations which makes them cheaper to deploy.

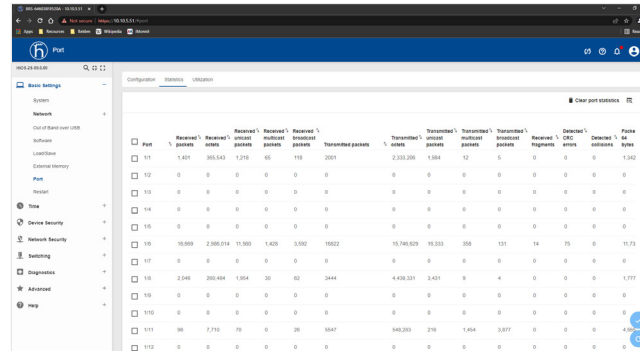
Element 1: Connecting Fixed Assets

Validating Connections for Fixed Assets

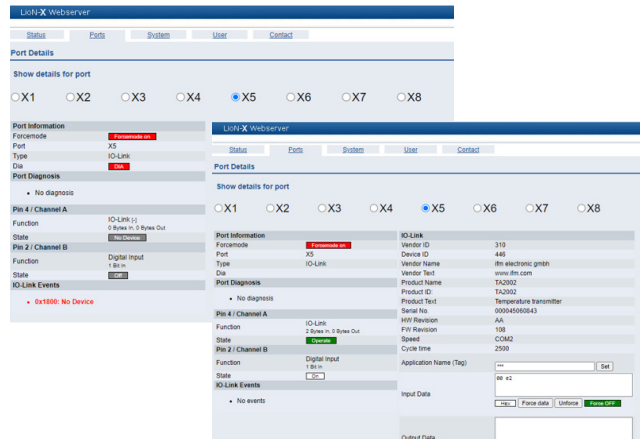
After connecting end devices to controllers and powering up the network, validate that everything works properly. The network management systems (NMS) and SCADA units should alert you to any issues connecting to end devices. During this idle stage before using the system in operations, consider stress testing various network segments. For example, use a packet generator on an Ethernet network to apply large amounts of network traffic to expose weak links before they impact operations. Also, simulate connection disruptions to trigger redundancies and confirm failover behaviors.

Of course, a visible registered connection cannot guarantee that all devices will behave as expected. Before running volume tests and the final go/no-go evaluation, consider using the management interface of critical devices to validate the flow of data. The NMS or the management interface of OT devices allows the user to validate its status and port-level connectivity. Other port diagnostics, which count fragmented packets and collisions on a link, can flag intermittent errors caused by problems like mismatched duplex settings.

For I/O data, port activity can usually be monitored from the I/O module. These aggregation devices should have a webservice with a graphical user interface (GUI) that gives port diagnostics. For example, monitoring the status of pins 2 and 4 on a typical circular connector reveals the current state of the attached I/O device. In the case of IO-Link ports, the display includes additional information related to the connected sensor and process data.



Port	Received % packets	Received % errors	Received % collisions	Received % CRC errors	Received % discards	Transmitted packets	Transmitted % errors	Transmitted % collisions	Transmitted % CRC errors	Transmitted % discards	Port status	Page #	
111	1,851	385,143	1,210	65	118	2051		2,333,206	1,684	12	0	0	1,342
112	0	0	0	0	0	0		0	0	0	0	0	0
113	0	0	0	0	0	0		0	0	0	0	0	0
114	0	0	0	0	0	0		0	0	0	0	0	0
115	0	0	0	0	0	0		0	0	0	0	0	0
116	16,889	2,385,014	11,303	1,428	3,582	16022		15,145,629	16,333	358	131	14	11,215
117	0	0	0	0	0	0		0	0	0	0	0	0
118	2,046	292,484	1,504	30	62	2444		4,419,331	3,431	9	4	0	1,777
119	0	0	0	0	0	0		0	0	0	0	0	0
120	0	0	0	0	0	0		0	0	0	0	0	0
121	36	7,710	70	26	6647			145,393	219	1,464	3,877	0	4,540
122	0	0	0	0	0	0		0	0	0	0	0	0



LION-X Webservice

Status: **Online**

Port Details

Show details for port

X1 X2 X3 X4 X5 X6 X7 X8

Port Information

Portmode: **IO-Link**

Port: X5

Type: IO-Link

IO-Link Events: **No Device**

Pin 4 / Channel A

Function: IO-Link I/O

State: **OK**

Pin 2 / Channel B

Function: Digital Input

State: **OK**

IO-Link Events: **No Device**

LION-X Webservice

Status: **Online**

Port Details

Show details for port

X1 X2 X3 X4 X5 X6 X7 X8

Port Information

Portmode: **IO-Link**

Port: X5

Type: IO-Link

IO-Link Events: **No Device**

Pin 4 / Channel A

Function: IO-Link I/O

State: **OK**

Pin 2 / Channel B

Function: Digital Input

State: **OK**

IO-Link Events: **No events**

Input Data

Output Data






Belden's Network Assessment Service

Evaluating your facility's complexity requires a thorough assessment of your assets and technologies, plus your network infrastructure. Belden's Network Assessment Service helps you determine the best solution for your use case and customize it for your environment.

Depending on your requirements, assessment steps may focus on improving operational efficiency, optimizing operational costs, or both.




Element 1: Connecting Fixed Assets

Solution Bundle for Fixed Asset Connections

Product Type	Product Reference	Purpose of the Product
Industrial Cables		<ul style="list-style-type: none"> • Highly flexible cabling, adapted to withstand repeated bending and torsion • Shielded Ethernet cabling using bonded pairs to connect switches and controllers • Armored fiber optic cabling for longer connection lengths and to connect to backbone nodes • M12 and RJ45 field terminators for on-demand cable terminations • Variable frequency drive (VFD) power cables to limit electromagnetic interference (EMI) • Hookup wire for wiring of in-cabinet devices
Industrial Cordsets		<ul style="list-style-type: none"> • Double- and single-ended cordsets with molded connectors for end devices • In-cabinet patch cords for copper and fiber optic connections
Active I/O Modules		<ul style="list-style-type: none"> • Convert IO-Link signals to the programmable logic controller (PLC) and cloud levels in industrial environments • Enable efficient wiring by converting multiple I/O signals into an IO-Link message • I/O boxes with an IP65 or IP67 rating and support for the device's communication standards
Layer 2 Switch		<ul style="list-style-type: none"> • Managed DIN rail switch with 8–24 ports, gigabit uplinks, and PoE+ support • Advanced management software with extensive redundancy, PoE control, and security features with an intuitive GUI • IP65 or IP67 ratings to direct Ethernet traffic within a given machine cell outside a cabinet • 2.5 Gbps uplink ports to communicate with the backbone • Automatic diagnostic and performance information reporting
Protocol Gateways		<ul style="list-style-type: none"> • Protocol gateways to convert between communication standards for disparate devices

Element 1: Connecting Fixed Assets

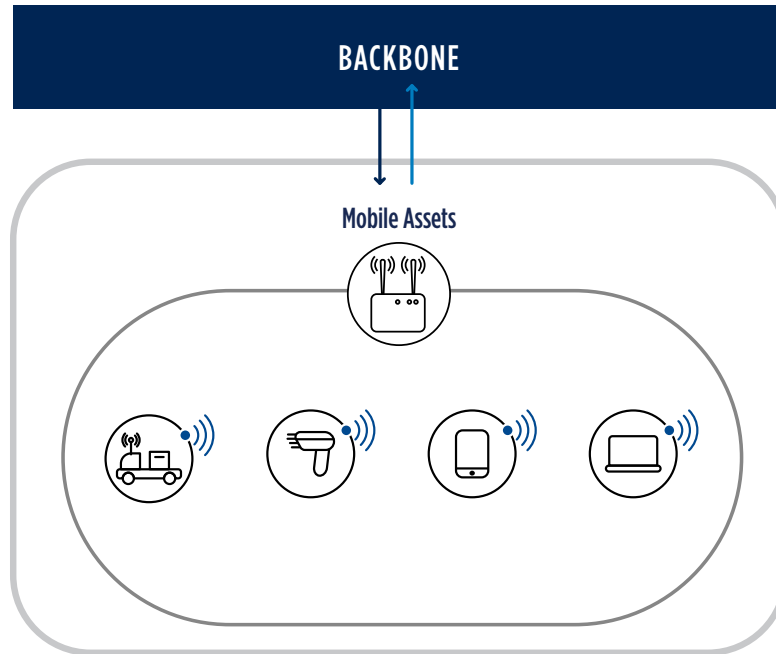
Solution Bundle for Fixed Asset Connections

Product Type	Product Reference	Purpose of the Product
Accessories		<ul style="list-style-type: none"> • Power supply to run each device • External memory module for switch configuration backups • Management software to support network operations and maintenance • Small form-factor pluggable (SFP) modules to connect fiber optic cables and switches
Cybersecurity Appliances		<ul style="list-style-type: none"> • Device protection at the field level • Strongest level of protection for the most critical assets on the network • Ability to define and filter all acceptable versus unacceptable traffic to critical assets • Ability to segment network portions and create points of demarcation between secure/unsecure points • Ability to create safe points of ingress/egress to external or third-party networks
In-Cabinet Patch Panels		<ul style="list-style-type: none"> • Passive, in-cabinet patch panels for copper and fiber optic cable runs

Element 2: Connecting Mobile Assets

Mobile assets move about a facility on their own as they complete tasks. They use multifaceted integrations of traditional and modern components to become impressively efficient tools. Their onboard intelligence takes high-level instruction from a control system that can reside at almost any layer of an organization from the field to the cloud, making appropriate network connections critical to successful operation.

As with fixed assets, many mobile assets can be grouped into equipment types, simplifying integration by highlighting common needs, and identifying unique requirements to ensure that these elements can integrate into a cohesive system both within their zone and within the entire OT network.







What are Mobile Assets?

Mobile assets **move during their active-duty cycle**. They may have elements fixed in a location but are distinct from fixed assets that remain entirely stationary in location during use. While systems like pick-and-place robotics and self-driving technologies tend to have intensive artificial intelligence (AI) controls, manual workstations and wearable technologies may also be mobile if they can be redeployed or roam while in use.

Element 2: Connecting Mobile Assets

Understanding the Mobile Assets Network

Autonomous Material Delivery Vehicles	Handheld and Wearable Devices	Smart Tools	Mobile Workstations
			
<p>Autonomous vehicles perform many functions in industrial facilities, from floor cleaning to timely delivery of parts. Reliable network communication enables these mobile assets to perform their tasks efficiently and requires detailed planning and positioning for the units and their antennas.</p>	<p>Handheld and wearable devices allow operators to interact more seamlessly with the process, providing contextual instructions and intelligent data gathering while simultaneously reducing ergonomic stress. These devices depend on wireless connections, elevating the importance of Wi-Fi coverage within their operating zone.</p>	<p>Smart tools connect to remote systems to send and retrieve data relating to their current assembly activities. Actual data transmission volumes may be low, but the criticality may be high, as it often feeds quality assurance (QA) systems and provides traceability to the assembly process.</p>	<p>Mobile workstations see countless applications:</p> <ul style="list-style-type: none"> • Engineering and maintenance stations update devices • Operator stations enable remedial actions • SCADA access stations <p>These terminals may be temporary or permanent. In some cases, they serve as the primary human-machine interface (HMI).</p>
<p>Important considerations:</p> <ul style="list-style-type: none"> • Number of fixed end devices • Number of simultaneously active automated guided vehicles (AGVs) • Location of AGVs for command instruction receipt • Location of charging stations • Size of AGV roaming area • Use of a central control station (for emergency stop messaging) • Use of a camera system with streaming video feed • Permanent network requirements 	<p>Reliance on existing versus new wireless architecture</p> <ul style="list-style-type: none"> • Database and analytics access requirements • Safety regulation requirements, such as network latency 	<ul style="list-style-type: none"> • Wired or wireless tools • Whether to provide a permanent network connection • Whether tools send and receive data • What data source, such as manufacturing execution system (MES), programmable logic controller (PLC), or both 	<ul style="list-style-type: none"> • Frequency of device connections in different locations • Information or analytics needs of devices without physical connectivity • Workstation connectivity to network infrastructure • Wired or wireless network access • Specific or flexible operations use



Element 2: Connecting Mobile Assets

Designing for Mobile Assets

Where practical, wireless network access for mobile devices and workstations—achieved via a standard network protocol such as the IEEE 802.11 standards for wireless Ethernet communication—allows interoperability of devices while avoiding proprietary technology hurdles and special licensing costs.

A range of revisions within the 802.11 standard enable increasingly faster and more secure connections. Match the version to the devices to get the most out of the connections, but the backwards compatibility of the standards generally forgives misalignments.

Right-size the network coverage for mobile devices to ensure enough capacity for client nodes within each zone without the zones interfering with each other. Poor antenna selection can seriously hamper performance. Carefully match antennas to the applications and the environment.

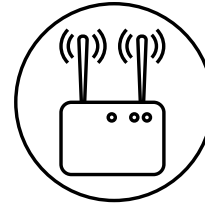
Wireless networks use the space between access points and clients as the transport medium, so all devices always share access to the medium, effectively making wireless connections half-duplex connections. This may not affect traditional IT-style devices, but industrial devices typically rely on precisely timed and unidirectional messaging. OT grade access points provide the fast connection and roaming times necessary for deployment of industrial devices.

Autonomous Material Delivery Vehicles

Keep in mind that “autonomous” does not mean “isolated.” Autonomous material delivery vehicles require input from external systems about the payload and destination. They also provide feedback upon completion of a task. Their effectiveness relies on seamless connections to control centers and to each other. An onboard wireless client device establishes connections to different access points across the plant as units travel, making use of fast roaming technology to ensure efficient operation.

Using M12 connectors for Ethernet connections onboard autonomous vehicles will help mitigate vibration as they move. Onboard sensors and actuators may share this connector type but not necessarily the same number of conductors or keyway.

Consider the form-factor of a wireless access point and any I/O blocks given the space constraints. Lower-weight options can lessen power consumption, lengthening battery life and productivity.



WLAN Communication Standards

IEEE	Frequency	Speed
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz / 5 GHz	600 Mbps
802.11ac	5 GHz	3.46 Gbps
802.11ax	2.4 GHz / 5 GHz	14 Gbps

Antenna Selection

Antenna selection affects the system’s ability to provide the best possible area of coverage for wireless networks:

- **Omni-directional antennas** offer broad coverage by spreading antenna power in all directions.
- **Directional antennas**, typically installed in a matched pair, provide line-of-sight communications from hundreds of feet to dozens of miles.
- **Radiating cable antennas**, linear cables with small slots in their shielding, create uniform coverage close to the cable.

Channel Bonding

Recent 802.11 wireless standards allow for “channel bonding” where adjacent channels within the frequency range can be combined to increase the maximum bandwidth. This can work for data-intensive operations but consumes more channels, which may interrupt high-quality area coverage for roaming devices.



Element 2: Connecting Mobile Assets

Handheld and Wearable Devices

Handheld scanners, tablets, and wearable devices, such as augmented reality (AR) glasses, have grown in popularity. Operators use them to ensure quality of work and component traceability. These on-demand devices operate in close proximity for periods of time creating variability in the connection density. Optimizing the access-point-to-client ratio enhances connection stability.

Overlapping areas of network coverage can help accommodate client density, but it is often undesirable due to interference. Antenna selection and orientation help control device access the network by location.

Smart Tools

Connected tooling communicates with industrial control systems to determine appropriate settings for a given operation, and with systems for quality assurance and traceability to confirm assembly targets achieved and log process data. These networked connections operate using wireless Ethernet technology, though other wireless standards are used as well. It is also not uncommon for some smart tooling to be connected via wired Ethernet connections, which offsets some operational flexibility for increased operational run time. In the case of the latter, selecting connectors and cable types for such tooling, consider that it will experience many impacts and its cables will undergo many thousands of bending cycles.

The communication method used determines whether data will travel unidirectionally or bidirectionally, to and from the tool. For example, if the tool connects to a remote open platform communications (OPC) server for bidirectional communication, the network design must support not only the bandwidth requirements of multiple devices but also the correct level of reliability between the server and the client tool.

Mobile Workstations

Most industries use mobile workstations in many areas. Terminals close gaps as companies advance their process controls, sometimes as a temporary measure evolving into a permanent use. Operational teams use mobile workstations in specific areas for everything from process visualization to remedial quality assurance (QA) actions. Engineering teams value mobile workstations to aid fault-finding and device management across the entire facility. Modern facilities plan for their use with facility-wide Wi-Fi coverage—a big improvement over the ad hoc approach of extending network coverage only as demanded.



Wireless Wearable Equipment

Small-scale electronics, like handheld scanners, often use the IEEE 802.15 standard for wireless communications. Bluetooth and Zigbee, popular IEEE 802.15 protocols, provide low power consumption and high client densities with low data rates. Bluetooth favors one-to-one connections, while Zigbee allows meshed networks of devices and gateways.

IEEE 802.15 can utilize the 2.4GHz spectrum which can cause interference with IEEE 802.11 networks. Carefully place access points and select appropriate antennas to minimize interference.

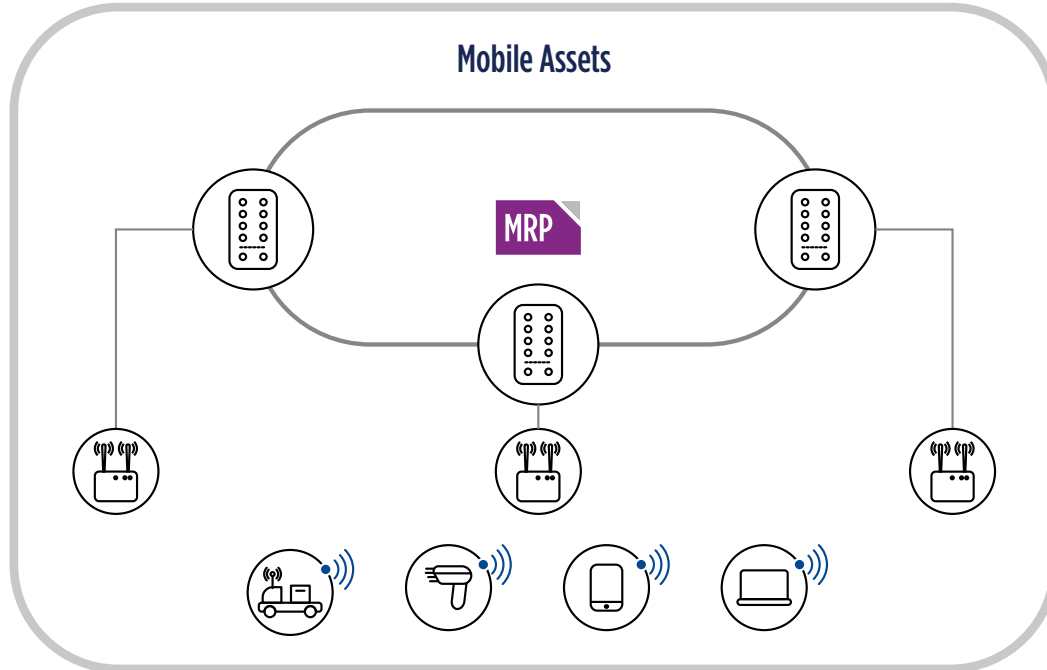
Channel Selection

Wireless communications subdivide their frequency ranges into channels to allow more networks to operate in the same area. The 802.11-based protocols for the 2.4 GHz range use channels that overlap, sometimes causing interference. Use of the limited number of non-overlapping channels to avoid interference. The available channels may differ depending on the operating country, but industrial networks tend to use channels 1, 6, and 11.

The 802.11-based protocols for the 5 GHz range employ non-overlapping channels to avoid crosstalk. However, they may overlap with other technologies like commercial radar, which has spawned a range of dynamic frequency selection (DFS) channels. DFS channels may cause non-deterministic behavior and periodic system outages, making them generally unacceptable for industrial networks.

Element 2: Connecting Mobile Assets

An Example Network Architecture for Mobile Assets



Planning Network Redundancy

Planned wireless connection redundancies help prevent faults and errors. Wireless networks succumb to the same device-level failures that wired networks do, as well as a set of transient problems like crosstalk from stray devices and duplicate signals caused by echoes and reflections within the physical environment.

Wireless Redundancy

As with wired connections, the more critical the messages traveling through wireless links, the more important redundancy becomes.

- **Multiple input multiple output (MIMO)** allows for more than one antenna per radio. Giving each antenna a different polarization provides both redundancy in the signal and noise immunity.
- Equipping wireless devices with **dual radios** gives the system a secondary network interface for communications.
- For high levels of criticality, **parallel redundancy protocol (PRP)** duplicates wireless traffic over multiple paths. The receiving end of the duplicated traffic accepts the first packets to arrive and discards the second.



Element 2: Connecting Mobile Assets

Securing Mobile Asset Connections

Networks designed for mobile assets blend wired and wireless connections to enable equipment communication. Best practices for wired networks also apply to blended networks. Many assets working collaboratively with each other and with human operators in the same spaces increase the possibility of cyberthreats. Careful mitigation of cyberthreats helps maintain a safe, secure workplace.

Wired networks inherently limit physical access, especially with good port availability control. Wireless networking lacks this level of physical control, so in addition to the standard best practices for wired networks, consider other virtual safeguards:

- Use connection credentials like a pre-shared key to prevent the system from establishing unauthorized links.
- By default, a wireless network usually broadcasts its service set identifier (SSID) to enable easier device connection, but this also makes the network an easier target for malicious attacks. If the application can function without broadcasting the SSID, then disable that feature to help obscure the network.
- Carefully select antennas to limit coverage to only the necessary area.
- Update firmware versions, especially when deploying a new network or new devices, to ensure the most current level of security.



IEC 62443

The IEC Technical Committee 65 (TC 65) publishes IEC 62443 for operational technology found in industrial and critical infrastructure, including but not restricted to power utility, water management, healthcare, and transportation. These horizontal standards, also known as base standards, are applied independent of technology and across many areas.

The IEC 62443 industrial communication network and system security series of standards consists of many chapters that emphasize:

- **Part 3-1:** Security technologies for industrial automation and control systems
- **Part 4-1:** Secure product development lifecycle requirements
- **Part 4-2:** Technical security requirements for industrial automation control system (IACS) components or products

Element 2: Connecting Mobile Assets

Deploying Connections for Mobile Assets



Installation

Correct placement of the wireless access points ensures appropriate area coverage. Consider the operating spectrum, the channels used by neighboring access points, the type of antennas, the location of walls and whatever else may cause reflections, and potential generators of interference, like motors.

Use the antenna's preferred orientation to maximize coverage and performance, especially with multiple input multiple output (MIMO) antennas that combine two or more antenna elements. Most wireless access points use two or more antennas posted in different directions to maximize coverage.

Antennas often connect to the radio of a wireless device via a length of cable. Keep in mind that longer cables require more signal strength and present more opportunity for interference. Use high quality cables with the shortest lengths practical to minimize cable losses. Inline filters protect access points from damage, especially in outdoor applications.



Configuration

Access points have several parameters to configure before use, including frequency and channel, whether a password will be required and the credentials, the network name, and whether the service set identifier (SSID) will be broadcast. Most industrial access points work with a centralized controller that simplifies larger deployments.

The client side of a wireless connection typically has fewer parameters to define but still requires configuration for network ID and credentials.



Go-Live

As the devices deploy, backup their configurations and add to the device identifier if possible, record the physical location of each asset, then safely and securely archive the backup and location guide to simplify later maintenance and upgrades.

Wireless Network Interference

Equipment operating near a wireless network can degrade performance of the network and impede stability by producing electromagnetic interference (EMI). Electric motors and their drive units commonly generate EMI, as do many other devices. Even non-industrial equipment like household microwaves can emit noise that will disrupt some communications equipment. **A proper site survey** completed when the suspect equipment is operating can help identify EMI sources so that corrective action can be taken.



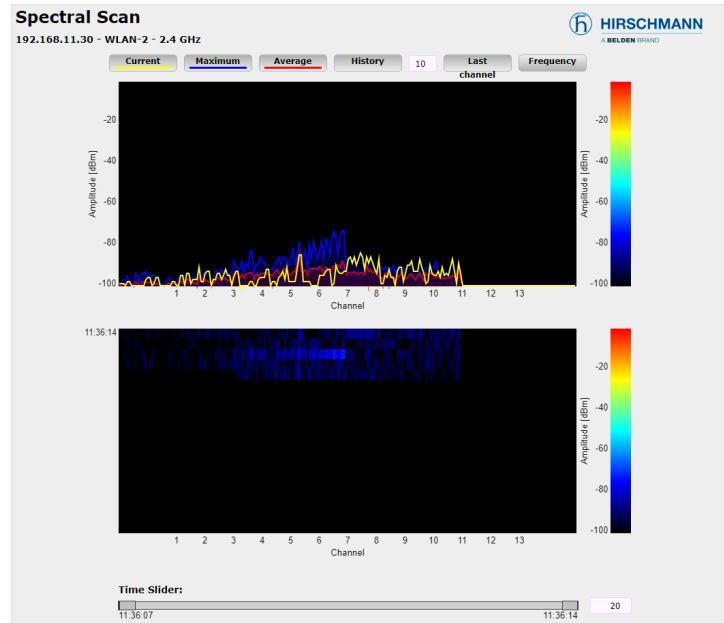
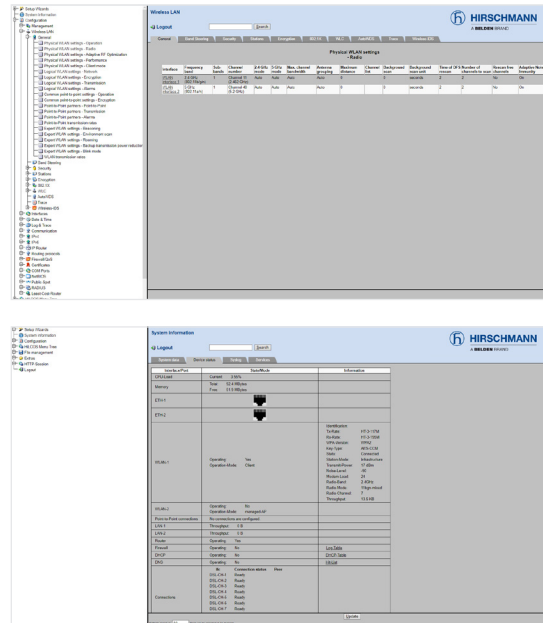
Element 2: Connecting Mobile Assets

Validating Mobile Asset Connections

As you would with wired connections, once you have deployed a wireless network and achieved operability, assess the links to ensure the stability of all connections. For wireless connections, repeat an area assessment to validate complete coverage over the operating zone of all mobile assets, and ensure the absence of dead spots they might encounter while roaming.

Also validate the client-side mobile connections for roaming devices that will hop between access points. A lack of properly managed redundancy may cause momentary signal interruptions and requires modification.

Most wireless devices offer an integrated webserver or guided user interface (GUI) to provide incoming and outgoing diagnostics that validate connection status and port-level connectivity.








Wireless Site Assessment Service

Wireless networks are key to many functions of modern industrial environments. A well-designed WLAN must include not only the location of access points and clients but also localized sources of interference like drive units, other WLANs, and even reflective surfaces. Belden's Wireless Site Assessment Service surveys your environment to **help you optimize your WLAN design.**

The survey aids in planning wireless service areas and mapping out frequency and channel use to avoid potential conflicts. The survey also helps you select appropriate antennas to align with where you expect your wireless signal to reach.






Element 2: Connecting Mobile Assets

Solution Bundle for Mobile Asset Connections

Product Type	Product Reference	Purpose of the Product
Industrial Cables		<ul style="list-style-type: none"> • Highly flexible cabling, adapted to withstand repeated bending and torsion • Shielded Ethernet cabling using bonded pairs to connect switches and controllers • Armored fiber optic cabling for longer connection lengths and to connect to backbone nodes • M12 and RJ45 field terminators for on-demand cable terminations • Variable frequency drive (VFD) power cables to limit electromagnetic interference (EMI) • Hookup wire for wiring of in cabinet devices
Industrial Cordsets		<ul style="list-style-type: none"> • Double- and single-ended cordsets with molded connectors for end devices • In-cabinet patch cords for copper and fiber optic connections
Active I/O Modules		<ul style="list-style-type: none"> • Converting IO-Link signals to the programmable logic controller (PLC) and cloud levels in industrial environments • Enable an efficient wiring concept by converting multiple I/O signals into an IO-Link message • I/O boxes with an IP65 or IP67 rating and support for the device's communication standards
Layer 2 Switch		<ul style="list-style-type: none"> • Managed DIN rail switch with 8–24 ports, gigabit uplinks, and PoE+ support • Advanced management software with extensive redundancy, PoE control, and security features with an intuitive GUI • IP65 or IP67 ratings to direct Ethernet traffic within a given machine cell outside a cabinet • 2.5 Gbps uplink ports to communicate with the backbone • Automatic diagnostic and performance information reporting
Protocol Gateways		<ul style="list-style-type: none"> • Protocol gateways to convert between communication standards for disparate devices

Element 2: Connecting Mobile Assets

Solution Bundle for Mobile Asset Connections

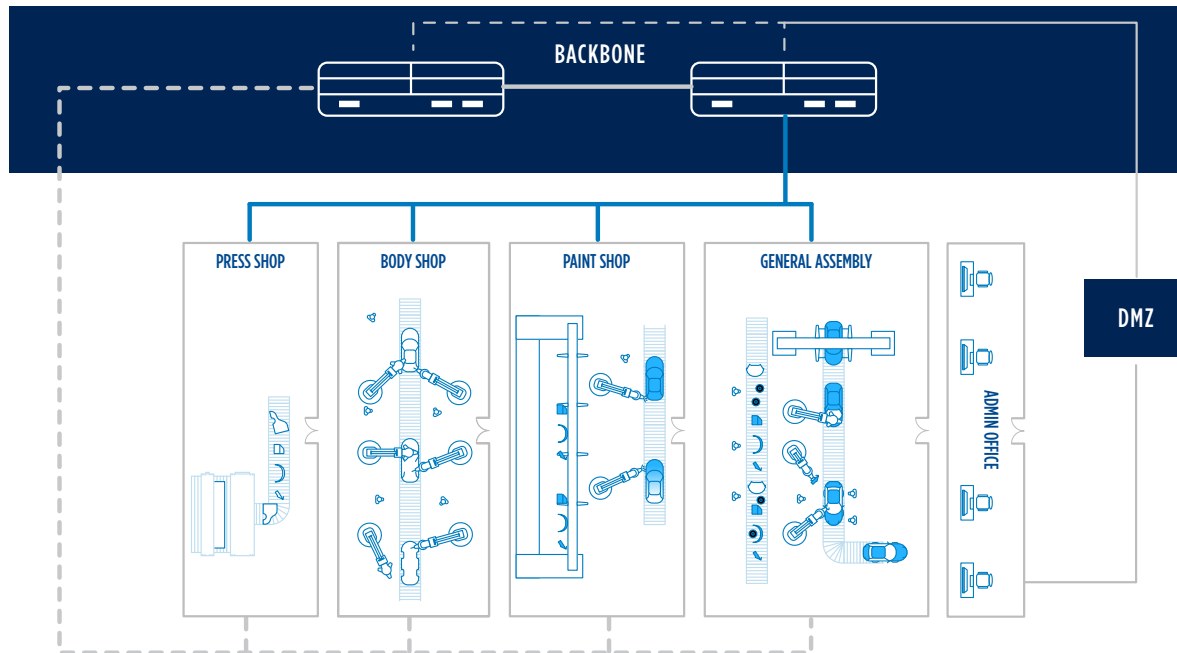
Product Type	Product Reference	Purpose of the Product
Accessories		<ul style="list-style-type: none"> • Power supply to run each device • External memory module for switch configuration backups • Management software to support network operations and maintenance • Small form-factor pluggable (SFP) modules to connect fiber optic cables and switches
Wireless Radios		<ul style="list-style-type: none"> • Wireless access points to provide constant communication with mobile devices • Wireless clients for use in mobile assets or to make fixed assets mobile • Radios that work as either access points or clients depending on configuration enable quick deployment and standardization of technician skillsets and spare parts inventory
Radio Antennas and cabling		<ul style="list-style-type: none"> • Wi-Fi antennas matched to the planned frequencies and directional coverage • Low attenuation cables to minimize signal losses between antennas and APs • Bandpass filters to protect APs from extraneous ambient noise
Cyber Security Appliances		<ul style="list-style-type: none"> • Device protection at the field level • Strongest level of protection for the most critical assets on the network • Ability to define and filter all acceptable versus unacceptable traffic to critical assets • Ability to segment network portions and create points of demarcation between secure/unsecure points • Ability to create safe points of ingress/egress to external or third-party networks
In-Cabinet Patch Panels		<ul style="list-style-type: none"> • Passive, in-cabinet patch panels for copper and fiber optic cable runs

Element 3: Backbone Connections

Your machines produce an impressive amount of information that contains insights to help you achieve better operational efficiency. The capacity required to transmit and process this quantity of data determines the scale you need for your network backbone.

A right-sized network efficiently connects workers and machines, providing current, high-quality data to inform operational decisions. The backbone of your network provides the infrastructure for reliable, secure, facility-wide transmission of this critical data in near real time.

As your facility and processes evolve, your connectivity requirements also grow. Designing a scalable, future-proof network now ensures your continued ability to pass critical data between operational areas and enterprise resources.







What Is a Backbone Network?

Smaller networks may only need a single network switch to connect several devices together. As systems grow in complexity and size, network switches must be linked together to enable end devices to communicate with each other. The **network links between switches** become the backbone of the network, facilitating communications across the entire system. Zones hang off the backbone with their own networking equipment, which may even include a spur backbone. The series of network switches and links that connects the most zones likely forms the true backbone in most cases.

Element 3: Backbone Connections

Understanding the Backbone Network

Interzone Connections	IT/OT Convergence	Remote Connectivity	Network Management
 <p>Not everything needs to talk to everything else. Most devices only need to talk to a few others to do their job. Creating segment zones keeps overall network traffic manageable and allows critical communications between zones to be prioritized. Interzone connections can be dedicated to the aggregation of data.</p>	 <p>The need for more computing power and greater flow of information in the modern industrial environment requires a convergence of IT and OT networks to provide both environments the data, context, and instruction they need. Computerized maintenance management systems (CMMs) require access to equipment performance data and enterprise resource planning (ERP) systems needs operational performance data to project system demands.</p>	 <p>Secure remote access from outside the plant—and from within—allows direct access to the OT network from inside and outside the plant. This enables authorized users to respond to issues and keep operations running by providing remote support, pushed updates, and virtual maintenance without compromising enterprise resources. Security is further increased by authorizing connections on-demand and restricting access by zone.</p>	 <p>Managing a large network requires a reliable software tool to configure and supervise all your connected assets and infrastructure. The NMS discovers new devices, reports events, alarms and configuration changes, and supports network optimization by highlighting communication bottlenecks. This reduces network downtime, increasing OEE.</p>

Important considerations:

- Interzone bandwidth requirements
- Industrial protocols used
- Specific support for redundancy protocols
- Zones requiring access to other zones
- Company policy and regulation around zoning

- Which protocols to allow
- Need for edge data collection
- OT assets managed by IT

- Who requires access to which devices from what locations
- Under what circumstances should remote access be granted
- What impacts ensue from waiting for a third-party vendor to diagnose on site issues
- Network access control policy

- Which devices need monitoring and management
- The management tool's visibility to network segments and devices
- Events to generate alarms and warnings, who receives them, and who bears the responsibility to resolve issues
- Need for routed distribution layers within larger OT networks (segmented layers)

Element 3: Backbone Connections

Designing for Backbone Connections

The connection of different zones forms the backbone for network traffic. This aggregation layer facilitates communication between the zones and segments network traffic to contain it within a zone unless it needs to move between zones. When planning capacity, factor in redundancy early in the design process to ease the work that follows. A routed backbone in combination with a dynamic routing protocol like open shortest path first (OSPF) handles this by default. Planning for even load distribution optimizes data transmission. However, consistent redundancy requires redundant connections between the backbone and the zones.

Interzone Connections

Field-level zoned networks may require integration of a range of industrial protocols and communication standards depending on the device needs. Keeping zones geographically small, limiting the length of cable runs and, in some cases, limiting the number of devices communicating on any given segment enhance design simplicity. Conversely, a backbone network—almost always a standard Ethernet-based network—often spans an entire facility, requiring careful attention to the demands of the physical size of the network.

Interconnections between zones exist primarily to guarantee data exchange to and from the zones. Redundancy mechanisms like media redundancy protocol (MRP) in combination with a routed backbone—one that moves packets along the backbone based on their network layer address—ensure reliable communication.

When creating interconnections between zones, some machine centers may be clones of others attached to the same network. This makes operation and maintenance easy but can complicate the communications infrastructure because these cloned cells may also duplicate internet protocol (IP) addresses. This problem is corrected by readdressing each device in each cloned zone or using a Layer 3 protocol, like NAT.



Interzone Communication

Despite the wide variety of IP addresses and subnet masks, private networks typically use one of three ranges, depending on the number of devices they expect to connect. Following this standard simplifies the efforts of network engineers, resulting in faster deployment with fewer mistakes. It also provides better interoperability when integrating other systems and converging with other networks.

- 10.x.x.x = 16,777,214 addresses
- 172.16.x.x = 65,534 addresses
- 192.168.0.x = 254 addresses

Element 3: Backbone Connections

IT/OT Convergence

With ever-increasing demands for service agility and real-time status updates, most industrial networks no longer operate in isolation from the rest of the company. Order entry and operational planning data from the enterprise layer continually flow to the CADA systems, and machine-layer controllers pass performance data back to the office personnel. This interface between the OT and the IT networks requires careful attention and sometimes strong lines of demarcation. The confluence of data flow places increased demand on the routing layer between the IT and OT networks, requiring high router and firewall bandwidth and built-in redundancy to the architecture.

This convergence of networks opens the door to potential cybersecurity vulnerabilities in each direction. Of the many security strategies available, system architects often choose to create a demilitarized zone (DMZ), placing firewalls in pairs to act as bridges between the different networks. Fine-tuned firewall rules and regulations prevent undesired data exchange.

Remote Connectivity

The wealth of information available in modern industrial facilities offers value beyond operational orchestration. Operations and maintenance teams in the field benefit from the insight it can provide. Sometimes dedicated taps provide fixed network connections, such as a supervisor's office, which acts as a localized monitoring station. Other devices make occasional remote connections. Mobile devices usually fall in this category and may require the ability to tap in from multiple locations within the facility or even from outside the facility—or around the world, in the case of a global company or third-party vendor.

When properly established, remote connectivity allows authorized devices and users to access targeted network segments and specific devices. Consider a maintenance technician who needs to perform an in field inspection of a drive system. In the case of process failures or outages, bringing in expert knowledge may greatly speed restoration. A network access gateway provides a secured tunnel between the target network segment and a hosting portal, allowing an authorized user access via the portal to the target network segment without the ability to interact with other network elements along the way. Thus, the network remains secure.

Unfortunately, no one-size-fits-all approach is practical and achieving remote access requires different solutions for varying situations. Generally, solutions fall into two camps: Ad hoc connections for on demand temporary access and persistent connections



Remote Connectivity

Highly secure remote access to specific devices should use the demilitarized zone (DMZ) or a perimeter network to serve as a buffer, enforcing data security policies between the network in question and an untrusted network or a network with different protocols.

Important considerations for remote connectivity:

- Industrial grade equipment for gateways and network bridges
- Strong encryption for virtual private networks (VPN) tunnels such as 256-bit advanced encryption standard (AES)
- Two-factor authentication for users attempting to create or access VPN tunnels
- Robust controls for the number of concurrent users like virtual lockout/tagout (V-LOTO)
- Configurable access levels for dashboards and administrator privileges
- Scalable subscription plans according to data consumption
- Permanent connections for WLAN coverage within specific production zones
- Internal data published to cloud-based platform via IoT protocols for data analytics



Element 3: Backbone Connections

for always-on access. The former allows remote user access only to the equipment and data they need for a specific task, sometimes with elevated permission levels. The latter provides an always-active connection effective for services usually with lower permission levels, but with access to a broader segment of the network.

When making the connection through a cellular interface, a dedicated internet service provider (ISP), a purpose-defined gateway between the IT and OT networks, or some other mechanism, the pathway involves a piece of equipment with access to the OT network and the ability to host a remote access protocol like a virtual private network (VPN). Also, remote connectivity for the broadest ranges of access always includes some element of internet connection, which involves risk. Access regulations and a high encryption level ensure security.

Network Management

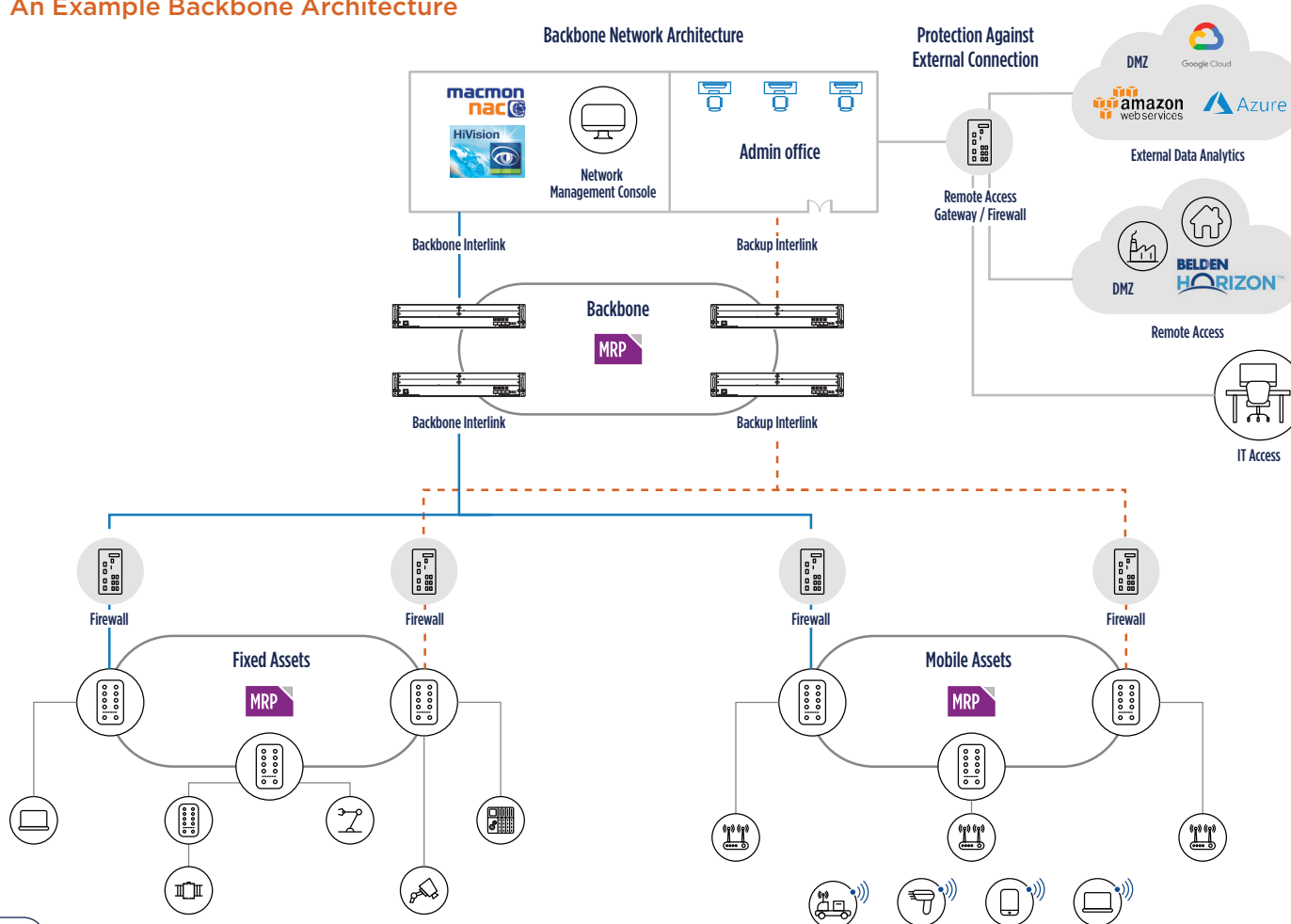
NMS collects alerts and notifications about physical and logical network issues along with real-time views of affected network topologies. Monitoring of key network metrics—link utilization, detection of unsecure protocols, and pre-emptive maintenance recommendations—ensures consistent maintenance of backbone network safety, security, and reliability. The NMS software recognizes failures of network devices and connections and produces alarms which prompt technicians to act. The monitoring and alerts keep downtime as low as possible and even enable proactive maintenance, repair, and replacement. It is more than a SCADA system for the network infrastructure. It also monitors the network for rogue device connections that lack authorization and allows administrators to remotely manage network infrastructure configuration settings.

NMS functions can be split across several software packages deployed at various points throughout a network. One common management task that is often run as its own function is the network access control (NAC). A full featured NAC application will utilize a variety of control methods, including SNMP, to interact with networked devices in order to interrogate connected equipment, authenticate assets and users, and configure connection parameters, like VLANs for infrastructure devices. A common standard for applying NAC down to the port level is through IEEE 802.1X where supplicants, or devices wanting network access, are connected to an authenticator which queries an authentication server to validate the supplicant's credentials against an ACL.



Element 3: Backbone Connections

An Example Backbone Architecture



Layer 3 Redundancy Protocols

- Virtual router redundancy protocol (VRRP)** creates a simulated gateway between two networks. A redundant pair of Layer 3 routers share administration of the virtual gateway. Should the primary fail, the secondary automatically takes up the role of the virtual gateway with other devices being unaware that anything has changed.
- Open shortest path first (OSPF)** creates and maintains a table of networks accessible from each routed port and assigns a path cost to each entry based on various link metrics including hop count, available bandwidth, and link reliability. Connections between networks are sent along the path with the lowest cost. It provides fast convergence, heightened security, and great scalability to adapt to thousands of network units.



Element 3: Backbone Connections

Planning Network Redundancy

Any industrial system should protect against faulty links and be resilient to connection problems, but even the best systems experience communications losses. Redundant pathways configured in advance help a system bypass damaged links automatically and reconfigure itself, keeping the network alive and avoiding costly breakdowns.

Crucial to sustainable operations, this resilience requires redundancy measures that behave deterministically—in consistent, known, pre-planned ways. Deterministic behavior ensures a seamless return to operation.





Element 3: Backbone Connections

Securing Backbone Connections

Prioritize cybersecurity within the backbone. The backbone network—the primary pathway between in-field systems, and the link to ingestion platforms is a critical system with broad reach—makes an attractive target for cyberattacks. Take measures to harden it against unauthorized access, interzone escalation of malware, and all other cyberthreats, malicious or otherwise.

Segmentation via the backbone network creates zones and conduits, which enable defence-in-depth:

- Obscures devices by limiting connections, making them harder for intruders to find
- Reduces the attack surface by funnelling attack vectors, concentrating protection measures
- Keeps errors, loops, and potentially malicious traffic from spreading between systems
- Makes network portions smaller, simplifying analyses and continuous monitoring

"Zero trust architecture always verifies the device's permission to access the network."

The backbone is also the ideal place to enforce a zero-trust architecture (ZTA). ZTA recognizes that cybersecurity threats come from inside as well as outside an organization and sometimes occur unintentionally. ZTA never trusts a connected device just because of its connection. It always verifies the device's permission to access the network. This practical approach works well in enterprise environments where users can enter credentials, or an administrator can build a static list of allowed devices. However, ZTA can be difficult to deploy with Internet of Things (IoT) devices and in industrial systems that sacrifice device intelligence to conserve processing speed.

- Devices may not have user credentials or a DNS gateway.
- Networks are frequently adjusted to install new devices and move workstations.
- Allowed devices that fail or are corrupted create vulnerabilities.

ZTA in industrial applications must dynamically update access control lists and switch configurations by monitoring network activity.

Security Concepts

- Defense-in-depth distributes multiple layers of security (defense) throughout the system.
- Zones group devices with similar security risks and vulnerabilities into security levels (SLs) which simplifies management.
- Conduits allow communication between zones.
- Demilitarized zones (DMZ) give mutual protection for disparate networks with different operational goals that preclude a unified set of rules. Firewalls border trans-network links with settings that support their network's goals and protocols.
- Security information and event managements (SIEM) provide organizations next-generation detection, analytics, and response. SIEM software uses security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by hosted applications and network devices.
- Network-based intrusion detection systems (NIDS) monitor and analyze network traffic to produce alerts from network-based threats. NIDS, passive devices that do not interfere with the traffic they monitor, usually operate in promiscuous mode, accessing all traffic for packet inspection.
- Host-based intrusion detection systems (HIDS) monitor a computer to detect, log, and send notifications of activity that changes that system's security policies or configurations.



Element 3: Backbone Connections

Deploying Backbone Connections



Installation

Store backbone devices somewhere secure, such as a locked cabinet, to prevent incidental access. Placing the distribution frame in an administrative office or attached to a building column establishes a permanent home for the infrastructure devices, making them easy to locate and simplifying cable management.



Configuration

With backbone units installed and zones connected, be sure to configure end point systems and infrastructure devices with the address of an appropriate default gateway. VRRP and NAT settings in the Layer 3 devices should also be reviewed to make sure that they allow bidirectional traffic. An error in these settings often presents as a failed ping test since the destination can't properly respond.



Go-Live

When all the devices are connected, disable unused ports to prevent access by rogue devices and keep individuals from accidentally introduce instability to the network.

Backup device configurations and archive them in a safe, secure location. Keep a record of where asset as installed so they can be located again, and, if possible, add that information to the device ID.

Proof of Concept Service

Mission-critical communication networks are often complex and represent a **significant part of total investment dollars**. You want to feel confident that your chosen solution will work as expected before the systems go live. Using the deployment phase for troubleshooting causes delays and drives up project costs. Testing mission-critical connections and scaled versions of the network architecture early in a project helps **validate designs before installing them** in the field, preventing costly delays.

Belden's Customer Innovation Centers (CICs) host proof-of-concept deployments in a lab setting complete with a wide array of hardware and enough space to house equipment you need to test in a **"bring your own device" (BYOD) environment**.

Element 3: Backbone Connections

Validating Backbone Connections

After the network comes online, validate that everything communicates as expected. Aside from the end devices communicating with each other and the machines performing their roles as designed, look at endpoints and network infrastructure devices for signs that point to potential issues:

- Collisions and cyclic redundancy check (CRC) fragments point to speed and duplex mismatches on either end of a link.
- Link flaps suggest problems with link media and connections or the network interface card (NIC) of the end device.
- Speed settings listed at values less than expected suggest termination issues with connection media.
- High bandwidth usage suggests excessive traffic like flooding, and network outages suggest the presence of unmanaged loops within connection paths.
- Frequent network outages also suggest faulty connections like those caused by overly long cable runs for the media type.
- Use traffic generating software to simulate high-bandwidth applications to validate bandwidth capacities and simulate cyberattacks.
- Consider using a packet capture software at various points in the network to “sniff” for erroneous broadcast traffic.

Port	Received % packets	Received % octets	Received % unicast packets	Received % multicast packets	Received % broadcast packets	Transmitted packets	Transmitted % octets	Transmitted % unicast packets	Transmitted % multicast packets	Transmitted % broadcast packets	Received % fragments	Detected % CRC errors	Detected % collisions	Packet % 64 bytes
1/1	1,401	365,543	1,218	65	118	2,001	2,333,206	1,984	12	5	0	0	0	1,342
1/2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/6	16,669	2,895,014	11,560	1,428	3,592	16,822	15,748,629	16,333	358	131	14	75	0	11,73
1/7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/8	2,046	280,484	1,954	30	62	3,444	4,439,331	3,431	9	4	0	0	0	1,777
1/9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1/11	96	7,710	70	0	26	5547	548,283	216	1,454	3,877	0	0	0	4,595
1/12	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Network Design Service






Designing a data network can be a challenge, and it only increases as networks get more complex. Belden’s Network Design Service offers you peace of mind. Our architects do the heavy lifting to create an efficient, reliable, and robust design that you can trust.

During the design phase, Belden’s network architects and solution consultants

- create a logical map of how end points and infrastructure devices connect and
- provide recommendations for the bill of materials (BOM) that achieve your desired business objectives.







Element 3: Backbone Connections

Solution Bundle for Backbone Connections

Product Type	Product Reference	Purpose of the Product
Industrial Cables		<ul style="list-style-type: none"> • Ethernet copper patch cords to connect between in-cabinet devices • Armored fiber optic cabling to connect between backbone nodes
Secure Remote Access Gateway		<ul style="list-style-type: none"> • Network gateways to connect to cloud-based services via Ethernet, wireless, or cellular media
Layer 3 Switch		<ul style="list-style-type: none"> • High number of Layer 3 features to enable the routed network • Rackmount 19-inch, high-bandwidth switch with a high number of uplink ports for IT connection • Layer 3 switches with an IP65 or IP67 rating to route Ethernet traffic without needing a cabinet
Accessories		<ul style="list-style-type: none"> • Power supply to run each device • External memory module for switch configuration backups • Small form-factor pluggable (SFP) modules to connect fiber optic cables and switches
Cybersecurity Appliances		<ul style="list-style-type: none"> • Device protection at the field level • Strongest level of protection for the most critical assets on the network • Ability to define and filter all acceptable versus unacceptable traffic to critical assets • Ability to segment network portions and create points of demarcation between secure/unsecure points • Ability to create safe points of ingress/egress to external or third-party networks

Element 3: Backbone Connections

Solution Bundle for Backbone Connections

Product Type	Product Reference	Purpose of the Product
Networking and Switch Cabinets		<ul style="list-style-type: none"> Storage of 19-inch, rack-mounted equipment and cable management
Enclosure Patch Panels		<ul style="list-style-type: none"> Cable management for high-density, rack-mounted equipment
Security Management Suite		<ul style="list-style-type: none"> Full set of security applications to detect and visualize abnormalities in the network and provide in-time warning to OT or IT administrators
Network Management System (NMS)		<ul style="list-style-type: none"> Easy-to-use, graphical NMS to enable real-time monitoring of network data flow and component status Network management client installed in the operational zones to monitor active components of each zone Subset of the plant-wide NMS
Authentication Server		<ul style="list-style-type: none"> A RADIUS authentication server for user & device validation Advanced, port-base network access control supporting 802.1X and SNMP communications
Remote Connectivity Software		<ul style="list-style-type: none"> Cloud or server-based VPN tunneling software to establish secure connections between systems



Belden – The Expert for All Your Networking Needs

As an end-to-end network solution provider, Belden enables you to access the solutions, services and tools you need to take major steps in your digitization journey.

Global Customer Innovation Centers

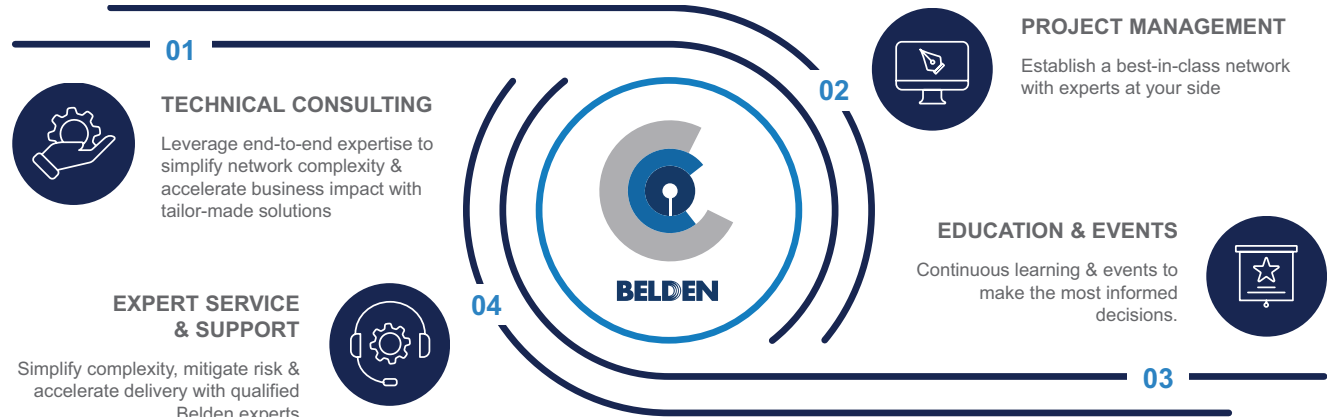
The digitalization journey is about unleashing the power of data to build a world of possibilities where customers will be able to shape their own business' future, proactively responding to the ever-changing market trends.

The Customer Innovation Center™ (CIC) is a space where innovation, creativity and collaboration are nurtured to find always better solutions to the digital challenges. Our experts and consultants offer their deep knowledge of the different hardware, software, and operations elements to guide the customers step by step in their digitalization journey.

To ensure that our customers are confident in their network we assess their processes and network to identify challenges and opportunities. We design and tailor the best solution from ground up to meet specific KPI's while delivering a network that outperforms industry benchmarks. Our state-of-the-art technology and expertise enable us to validate the solution before implementing it and provide post-sales services and support, effectively taking the risk away from the customers.

To guarantee our support on a global scale we opened five Customer Innovation Centers across the world: Stuttgart (DE), Santa Clara (US), Chicago (US), Shanghai (CN), and Bangalore (IN). The CIC locations offer the possibility to touch and feel our solutions and the opportunities are endless: we bring the offline and online worlds together to foster innovation through our collaborative labs and training spaces.

Our customers are building the future. We build the network that makes it possible.





End-to-End Solution Portfolio

Belden offers the most comprehensive networking portfolio for your sensor to cloud solution. This includes:

Data Acquisition & Transmission

Cable

Fiber | Copper | A/V



Connectivity

Fiber | Copper | A/V
Racks | Connectivity Tools



Cable

Fiber | Copper



Connectivity

Active I/O Modules | Passive
Distribution Boxes | Connectors



Networking

Wireless | Gateways |
Switches | Routers



SW and Services

Network Management Software
| Firewalls | SCM & VM



Our Experts at Your Side

Selecting the right solution for your business needs is not an easy task and Belden will provide direct access to our experts to be your trusted advisors in each phase of your automation journey.



Solution Architects

Deep technical knowledge of network architectures

Develop, design, and validate best solutions tailored to the complexity of each customer unique business challenge



Digital Automation Consultant

Industry expertise with deep networking know-how

Lead process, workflows, and data assessments to identify digital transformation opportunities and calculate potential value of network solutions for the customer



Solution Consultant

Deep technical knowledge of applications and industries

Guide the customer in their digital transformation journey conducting industrial network audits and positioning the ideal solutions



Solution Engineers

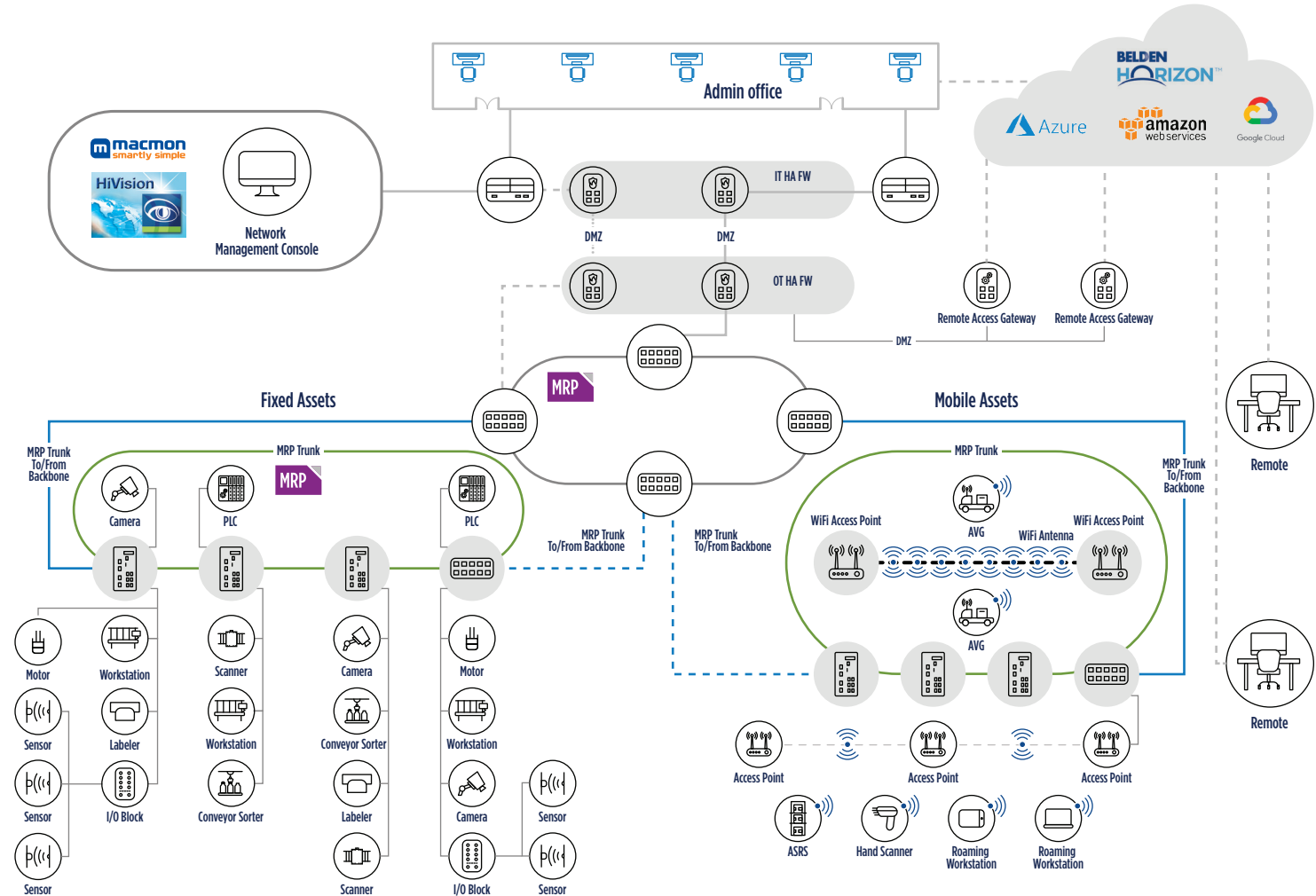
Deep technical knowledge of products and technologies

Conduct trainings, testing and commissioning networks

Lead network assessments and deliver high quality pre-sales and post-sales technical support

Bringing It All Together

With our experts at your side throughout your complete digitization journey, we'll work together to bring your automation plans to life by combining Belden's extensive network portfolio and third-party tools and services.








Deep Dive into Belden’s Network Offering for Labor Productivity Solutions

Solution Package for Fixed Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
Control and Power Cables	Machflex 350 and 375 Cables		A complete line of highly durable, flexible cables specially designed for machine builders to use in ruggedized and harsh environments
Servo Cables	MachFlex SERVO Classic and Hybrid 610BCY		Designed for connecting servo controller with motor. Cable applications include motor speed control, production machinery and machine tools. This type of cables suits both static and flexible uses in plant engineering.
VFD Cables	MachFlex SERVO Symmetrical 610BCY		Cables that suit both static and flexible uses in plant engineering. Double-screened power cable for large servo drive systems with high electrical load
2-pair, legacy Ethernet cable	DataTuff 7933A		Industrial-grade, shielded cabling to suitable for legacy connections like the M-12 D-coded connector only use 4-wires.
4-pair, weld-splatter resistant Ethernet cable	DataTuff 7938A		Industrial-grade, high flex cabling suitable for use in welding applications with thermoplastic (TPE) jacketing
4-pair, extended length Ethernet cable	DataTuff 7903A		Ethernet cable capable of achieving link lengths of greater than 100m in different environments
4-pair, high voltage Ethernet cable	DataTuff 7958A		Ethernet cable suited to high voltage environments
4-pair, future proof Ethernet cable	10GXS		Category 6A cable designed for up to 10 Gb applications with performance optimized for in-building standard and wireless networks
Ethernet Field Terminations	Ind REV Connect RV-series		Industrial-grade, male and female field connectors for Ethernet cabling with class-leading performance minimizing insertion loss and maximizing pull strength. Available in various colors and shielded configurations
OM3/OM4 50µm Multimode Fiber Cable	GUXT- series		Belden’s tight-buffered multi-fiber distribution cables come in fiber counts from 2 to 72, designed for both indoor and indoor/outdoor applications. Their small bend radius and 900 µm tight-buffered fibers allow for fast installations and easy terminations.
Fusion fiber optic Field Termination	FX Fusion		FiberExpress (FX) Fusion Splice-On Connectors combine the benefits of fusion splicing with the simplicity of a field-installable connector, improving installation performance and reliability when compared to mechanical splice connectors.
Industrial Protocol/Data Bus Cables	CANBus: 9841, 9842 & 3105A DeviceNet: 3084A Profibus: 3076F, 3079A, 3079F		A range of cabling products compliant with various industrial communications protocols like PROFIBUS, CANbus, DeviceNet, and many more







Solution Package for Fixed Asset Connections


Product Group	Product Code	Belden Brand	Why this product?
M8 and M12 Sensor/ Actuator Cordsets	RST 4-RKMV 4-225 RST 3-RKMV 3-224 RST 4-RKT 4-225 RST 4-RKT 4-1006 RST 5-RKT 5-228 RST 5-RKT 5-458 RST 4-RKWT/LED R 4-1006 RST 5-RKWT/LED R 5-458	 lumbergautomation A BELDEN BRAND	Industry proven connection technology for sensors and actuators. Ruggedized for performance: Proven reliability in wet, welding, dusty, and harsh surroundings
M12 Data Cordsets	0985 342 1 0985 856 1		CAT5e M12 D-coded cordsets for Industrial Ethernet Fieldbus protocols. High-quality 360° shielding provides excellent electromagnetic interference (EMI) protection. Drag chain compatible up to 2 million bending cycles with abrasion-resistant polyurethane (PUR) sheathing
M12 Power Cordsets	RST 5L-RKT 5L RKT 5L RKWT 5L		High-performance energy transmission of up to 16 Amps in hot, damp, dusty, or moving applications. Flexible solutions thanks to a wide variety of designs with angled and over-molded versions as well as versions that can be freely assembled
RJ45 Ethernet Patch Cords	CAD4Z1		Space saving RJ45 patch cords use a thinner gauge to free up space within cabinets. Cordsets are available in a range of colors and lengths, with options for RFID tags and LEDs for easier tracing.
FO Patch Cords	FX@E LSZH GP-32-series		FiberExpress (FX) Patch Cords deliver a robust design to withstand the rigors of daily use in off-the-shelf, standard configurations and rapid, custom-tailored installations.
DIN Rail Patch Panel	MIPP - series		Easily installed on any standard 35 mm DIN Rail, Modular Industrial Patch Panel (MIPP) features high port-density to meet expanding network connectivity needs within limited space
Layer 2 unmanaged rail switch	SPIDER III		Unmanaged industrial switch for DIN rail, fanless design suitable for simple media conversation, PoE injection, and high port densities.
Layer 2 lightly managed rail switch	GECKO	 HIRSCHMANN A BELDEN BRAND	Lightly-managed industrial switch for DIN rail, fanless design suitable for extended network reach with redundancy support and device diagnostics.
Layer 2 fully managed rail switch	BRS52-8TX/4SFP BRS40 BRS44		Managed industrial switch for DIN rail, fanless design, all gigabit type with 2.5 Gb uplinks and power sourcing equipment in accordance with IEEE 802.3at (PoE+ inline power) to power up process related equipment
Layer 2 unmanaged IP67 switch	OCTOPUS 8TX- EEC-M		Layer 2 managed switches with fanless design built to fit within the formed sidewalls of conveyors. The IP67 compliant form factor provides M12 twist/lock connectors instead of RJ45 for vibration and shock tolerance



Solution Package for Fixed Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
Layer 2 and 3 fully managed IP67 switch	OS3-40 OS3-44	 HIRSCHMANN A BELDEN BRAND	Layer 2 and 3 managed switch with fanless with IP67 compliant form factor provides M12 twist/lock connectors instead of RJ45 for vibration and shock tolerance
Digital I/O block	0980 ESL 0960 IOL 0980 XSL	 lumberg automation A BELDEN BRAND	IP-67 rated digital I/O modules suitable for multiple communication protocols with variations available for IO-Link masters, IO-Link Hubs, and ladder logic control.
Protocol gateways	PLX3	 ProSoft TECHNOLOGY	Protocol specific communication gateways for high-speed bi-directional data transfers between two different protocols
Industrial firewall	EAGLE40-03106	 HIRSCHMANN A BELDEN BRAND	Full gigabit firewall capable of providing with stateful packet inspection (SPI) and deep packet inspection (DPI) at line-speed. Complete with routing functionality like NAT, the device ensures protection and connection reliability for critical production cells.
Edge computing platform	OpEdge-8D		The Hirschmann edge-compute platform uses a fanless, DIN rail mounting design built for industrial environments. Capable of Layer 2 and Layer 3 networking, the unit comes with 8 GB of RAM, 64 GB SSD, and an array of ports including 5x GbE RJ45, 2x GbE SFP, 2x USB3.0, 2x DB9 serial. The system offers an in-built web user interface (UI) for loading containers and virtual machines, as well as native support for app orchestration through the cloud-based Belden Horizon.
Rail-mounted power supplies	RPS-80 EEC RPS-480/POE EEC		Compact 24 and 48V DC power supplies for in-cabinet, rail mounting uses
External memory modules	ACA22-USB-C EEC ACA22-M12 EEC		External memory modules suitable for Hirschmann products in industrial environments

Solution Package for Mobile Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
Control and Power Cables	Machflex 350 and 375 Cables	 BELDEN	A complete line of highly durable, flexible cables specially designed for machine builders to use in ruggedized and harsh environments
Servo Cables	MachFlex SERVO Classic and Hybrid 610BCY		Designed for connecting servo controller with motor. Cable applications include motor speed control, production machinery and machine tools. This type of cables suits both static and flexible uses in plant engineering.






Solution Package for Mobile Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
Control and Power Cables	Machflex 350 and 375 Cables		A complete line of highly durable, flexible cables specially designed for machine builders to use in ruggedized and harsh environments
Servo Cables	MachFlex SERVO Classic and Hybrid 610BCY		Designed for connecting servo controller with motor. Cable applications include motor speed control, production machinery and machine tools. This type of cables suits both static and flexible uses in plant engineering.
VFD Cables	MachFlex SERVO Symmetrical 610BCY		Cables that suit both static and flexible uses in plant engineering. Double-screened power cable for large servo drive systems with high electrical load
2-pair, legacy Ethernet cable	DataTuff 7933A		Industrial-grade, shielded cabling to suitable for legacy connections like the M-12 D-coded connector only use 4-wires.
4-pair, weld-splatter resistant Ethernet cable	DataTuff 7938A		Industrial-grade, high flex cabling suitable for use in welding applications with thermoplastic (TPE) jacketing
4-pair, extended length Ethernet cable	DataTuff 7903A		Eethernet cable capable of achieving link lengths of greater than 100m in different environments
4-pair, high voltage Ethernet cable	DataTuff 7958A		Eethernet cable suited to high voltage environments
4-pair, future proof Ethernet cable	10GXS		Category 6A cable designed for up to 10 Gb applications with performance optimized for in-building standard and wireless networks
Ethernet Field Terminations	Ind REV Connect RV-series		Industrial-grade, male and female field connectors for Ethernet cabling with class-leading performance minimizing insertion loss and maximizing pull strength. Available in various colors and shielded configurations
OM3/OM4 50µm Multimode Fiber Cable	GUXT- series		Belden's tight-buffered multi-fiber distribution cables come in fiber counts from 2 to 72, designed for both indoor and indoor/outdoor applications. Their small bend radius and 900 µm tight-buffered fibers allow for fast installations and easy terminations.
Fusion fiber optic Field Termination	FX Fusion		FiberExpress (FX) Fusion Splice-On Connectors combine the benefits of fusion splicing with the simplicity of a field-installable connector, improving installation performance and reliability when compared to mechanical splice connectors.
Industrial Protocol/Data Bus Cables	CANBus: 9841, 9842 & 3105A DeviceNet: 3084A Profibus: 3076F, 3079A, 3079F		A range of cabling products compliant with various industrial communications protocols like PROFIBUS, CANbus, DeviceNet, and many more








Solution Package for Mobile Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
M8 and M12 Sensor/ Actuator Cordsets	RST 4-RKMV 4-225 RST 3-RKMV 3-224 RST 4-RKT 4-225 RST 4-RKT 4-1006 RST 5-RKT 5-228 RST 5-RKT 5-458 RST 4-RKWT/LED R 4-1006 RST 5-RKWT/LED R 5-458	 A BELDEN BRAND	Industry proven connection technology for sensors and actuators. Ruggedized for performance: Proven reliability in wet, welding, dusty, and harsh surroundings
M12 Data Cordsets	0985 342 1xx/x M 0985 856 1xx/x M		CAT5e M12 D-coded cordsets for Industrial Ethernet Fieldbus protocols. High-quality 360° shielding provides excellent electromagnetic interference (EMI) protection. Drag chain compatible up to 2 million bending cycles with abrasion-resistant polyurethane (PUR) sheathing
M12 Power Cordsets	RST 5L-RKT 5L-xxx/x M RKT 5L-xxx/x M RKWT 5L-xxx/x M		High-performance energy transmission of up to 16 Amps in hot, damp, dusty, or moving applications. Flexible solutions thanks to a wide variety of designs with angled and over-molded versions as well as versions that can be freely assembled
RJ45 Ethernet Patch Cords	CAD4Z1		Space saving RJ45 patch cords use a thinner gauge to free up space within cabinets. Cordsets are available in a range of colors and lengths, with options for RFID tags and LEDs for easier tracing.
FO Patch Cords	FX@E LSZH GP-32-series		FiberExpress (FX) Patch Cords deliver a robust design to withstand the rigors of daily use in off-the-shelf, standard configurations and rapid, custom-tailored installations.
DIN Rail Patch Panel	MIPP - series		Easily installed on any standard 35 mm DIN Rail, Modular Industrial Patch Panel (MIPP) features high port-density to meet expanding network connectivity needs within limited space
Layer 2 unmanaged rail switch	SPIDER III	 A BELDEN BRAND	Unmanaged industrial switch for DIN rail, fanless design suitable for simple media conversation, PoE injection, and high port densities.
Layer 2 lightly managed rail switch	GECKO		Lightly-managed industrial switch for DIN rail, fanless design suitable for extended network reach with redundancy support and device diagnostics.
Layer 2 fully managed rail switch	BRS52-8TX/4SFP BRS40 BRS44		Managed industrial switch for DIN rail, fanless design, all gigabit type with 2.5 Gb uplinks and power sourcing equipment in accordance with IEEE 802.3at (PoE+ inline power) to power up process related equipment







Solution Package for Mobile Asset Connections


Product Group	Product Code	Belden Brand	Why this product?
Layer 2 unmanaged IP67 switch	OCTOPUS 8TX-EEC-M	 HIRSCHMANN <small>A BELDEN BRAND</small>	Layer 2 managed switches with fanless design built to fit within the formed sidewalls of conveyors. The IP67 compliant form factor provides M12 twist/lock connectors instead of RJ45 for vibration and shock tolerance
Layer 2 and 3 fully managed IP67 switch	OS3-40 OS3-44		Layer 2 and 3 managed switch with fanless with IP67 compliant form factor provides M12 twist/lock connectors instead of RJ45 for vibration and shock tolerance
Digital I/O block	0980 ESL 0960 IOL 0980 XSL	 lumberg automation <small>A BELDEN BRAND</small>	IP-67 rated digital I/O modules suitable for multiple communication protocols with variations available for IO-Link masters, IO-Link Hubs, and ladder logic control.
Protocol gateways	PLX3	 ProSoft <small>TECHNOLOGY</small>	Protocol specific communication gateways for high-speed bi-directional data transfers between two different protocols
Industrial firewall	EAGLE40-03106		Full gigabit firewall capable of providing with stateful packet inspection (SPI) and deep packet inspection (DPI) at line-speed. Complete with routing functionality like network address translation (NAT), the device ensures protection and connection reliability for critical production cells.
Edge computing platform	OpEdge-8D		The Hirschmann edge-compute platform uses a fanless, DIN rail mounting design built for industrial environments. Capable of Layer 2 and Layer 3 networking, the unit comes with 8 GB of RAM, 64 GB SSD, and an array of ports including 5x GbE RJ45, 2x GbE SFP, 2x USB3.0, 2x DB9 serial. The system offers an in-built web user interface (UI) for loading containers and virtual machines, as well as native support for app orchestration through the cloud-based Belden Horizon.
Rail-mounted power supplies	RPS-80 EEC RPS-480/POE EEC	 HIRSCHMANN <small>A BELDEN BRAND</small>	Compact 24 and 48V DC power supplies for in-cabinet, rail mounting uses
External memory modules	ACA22-USB-C EEC ACA22-M12 EEC		External memory modules suitable for Hirschmann products in industrial environments
Single and Dual-radio 802.11 wireless access point	BAT-R BAT-F		Industrial-grade access points suitable for establishing OT connectivity via 802.11 wireless networking
Single radio 802.11 wireless client	BAT-C2 BAT867 F		IP-67 rated wireless clients suitable for on-machine access to 802.11 wireless networks.
Fast roaming 802.11 wireless access points	RLX2-IHNF RLX2-IHNF-W	 ProSoft <small>TECHNOLOGY</small>	Industrial-grade, wireless access points for 802.11n networks suited to fast roaming networks with requirements for 10ms roaming



Solution Package for Mobile Asset Connections

Product Group	Product Code	Belden Brand	Why this product?
Wireless LAN Controller	WLC	 HIRSCHMANN A BELDEN BRAND	Centralized management for automated configuration and control of wireless access points
Antenna and connection accessories	A-2503S3-O A2504NBHW-OC	  	Omni, sectional, directional and radiating-cable antennas for 2.4 GHz and 5 GHz wireless networks with associated cabling, couplers, and inline filters.

Solution Package for Backbone Connections

Product Group	Product Code	Belden Brand	Why this product?
Category 7 Bulk Ethernet Cables	DataTuff 74004		Category 7 cables for the most bandwidth-intensive applications. These ultra-reliable cables answer the growing demand for high-performance networking and offer consistent, reliable performance in even the harshest environments.
Category 6A Bulk Cable	10GXS IEA001		Category 6A cable designed for up to 10 Gbps applications with performance optimized for in-building standard and wireless networks
Ethernet Field Terminations	Ind REV Connect RV-series		Industrial-grade, male and female field connectors for Ethernet cabling with class-leading performance in minimizing insertion loss and maximizing pull strength. Available in various colors and shielded configurations
RJ45 Rackmount Patch Panel	KeyConnect AX1069-series		Provides maximum network performance and helps keep up with network changes. Designed for networks and data center applications
10Gb Ethernet Patch Cords	CAD4Z1		Space saving RJ45 patch cords use a thinner gauge to free up space within cabinets. Cordsets are available in a range of colors and lengths, with options for RFID tags and LEDs for easier tracing.
OM3/OM4 50µm Multimode Fiber Cable	GUXT- series		Tight-buffered multi-fiber distribution cables available in fiber counts from 2 to 72, designed for both indoor and indoor/outdoor applications. Their small bend radius and 900 µm tight-buffered fibers allow for fast installations and easy terminations.






Solution Package for Backbone Connections

Product Group	Product Code	Belden Brand	Why this product?
Fusion fiber optic Field Termination	FX Fusion		FiberExpress (FX) Fusion Splice-On Connectors enable splice-on technology combining the benefits of fusion splicing with the simplicity of a field-installable connector, improving installation performance and reliability when compared to mechanical splice connectors
FO Rackmount Patch Panel	Wirenet NNO140-series		The FX Wirenet connectivity system offers a simple solution for incorporating flexibility, manageability, and scalability into high-density fiber channels. Multiple connectivity options such as LC, SC and ST
FO Patch Cords	FX@E LSZH GP-32-series		FiberExpress (FX) patch cords deliver robust design to withstand the rigors of daily use in off-the-shelf, standard configurations and rapid, custom-tailored installations.
Enclosure/Cabinet	19" Compact Cabinets E-SERIES		For use in 19-inch LAN and data center applications. Varying depths for various applications. Offer a modular scalable system that adapts to changing requirements for hosting multiple generations of IT/OT equipment
Layer 2 and 3 managed rack switch	GRS		Ruggedized industrial 19-inch rack switch with modular expandable media modules and modular hot swappable power supply units. 10 Gbps capabilities with port aggregation abilities to allow a scalable backbone network bandwidth. Common field level network aggregation switch to manage industrial network ring redundancy, such as media redundancy protocol (MRP) and multiple MRP sub-ring topologies.
Layer 2 and 3 managed rack switch	Mach4500		Industrial modular/expandable aggregation switch up to 88 ports 10 Gbps capable. Industrial-grade hardware for use in core switch/routing environments with all Layer 3 and security features of Hirschmann HiOS software
Layer 2 and 3 Modular rail switch	MSP42		Full Gb modular, rail-mounted backbone switch/router with up to 7 modules and extensible to two 10 Gbps or four 2.5 Gbps. Optional M12 twist/lock connectors for enhanced vibration and shock tolerance.
Remote access gateway	ICX35-HWC PLX35-NB2		WAN gateways provide an OT-side access point for secure remote connections to production cells from external locations. Connections from cloud-based services like Belden Horizon cloud environment to allow secure connectivity, with user-based credentials, to some or all devices within the automation network.
industrial firewall	EAGLE40-07206		Full gigabit firewall capable of providing with stateful packet inspection (SPI) and deep packet inspection (DPI) at line-speed. Complete with routing functionality, like NAT, the device is suitable for creating demarcation between OT and IT networks along with demilitarized zone (DMZ) creation for third-party network connectivity.
Rail-mounted power supplies	RPS-80 EEC RPS-480/POE EEC		Compact 24 and 48V DC power supplies for in-cabinet, rail mounting uses



Solution Package for Backbone Connections

Product Group	Product Code	Belden Brand	Why this product?
External memory modules	ACA22-USB-C EEC ACA22-M12 EEC	 HIRSCHMANN A BELDEN BRAND	External memory modules suitable for Hirschmann products in industrial environments
Network management system	HiVision		Control Room software license to configure, monitor and manage complete OT network
Network access control	NAC	 macmon smartly simple	Centralized port-based security software that enables 802.1x of network equipment with SNMP control of devices, dynamic VLAN control. The software functionality is completed with an inbuilt RADIUS authentication serve and guest network portals to protect networks against intrusion from unauthorized devices
Remote access platform	Belden Horizon	 BELDEN	Secure remote access and edge ap orchestration via a cloud-based platform that host encrypted virtual private network (VPN) tunnels



Contact Us

Email

emea.cic@belden.com

apac.cic@belden.com

americas.cic@belden.com

www.belden.com/CIC

[in linkedin.com/company/beldeninc](https://www.linkedin.com/company/beldeninc)

twitter.com/BeldenInc

[youtube.com/user/beldenvid](https://www.youtube.com/user/beldenvid)