Belden

Optimizing warehouse networks: an expert guide for OEMs & system integrators

White Paper

Mike Fisher

Senior Manager, Solution Architecture

Aaron Hammer

Professional Services Manager

Kevin L. Mayo

Director, Solution Consulting - Cybersecurity

Achieving top network reliability, security and performance

Designing and managing a warehouse network to handle anything thrown its way takes real expertise. It goes far beyond connecting routers and cables. It's an elusive balance of science and art.

As an original equipment manufacturer (OEM) or systems integrator (SI), building and integrating a warehouse network typically involves overcoming poor network performance and managing cybersecurity threats, spotty connections between warehouse systems and data that's not available when and where it's needed.

In this guide, we turn to Belden experts who bring years of industry experience and insights into the complex world of network design. Together, they explore four key concepts to consider during your next warehouse network design.

Table of contents

1. Optimizing network design: it's all about the data

When building a warehouse network, everything starts and ends with data. Mapping the flow of information from source to destination helps you plan physical and wireless connectivity and frame logical connectivity (data topology) for your customers' networks.

"Focus on your customer's systems and connected devices — controllers, servers, computers — anything that needs to produce or consume data," advises Fisher.

Whether your customer is starting from a greenfield state or rebuilding in a brownfield environment, ask them:

- Where are systems and devices located within the warehouse?
- What are they doing with the data?
- What type of data are they pushing or consuming?

Holistically mapping asset locations and understanding how data is used helps you determine where to make physical and logical connections and how information flows within network segments.

"Unless you know the data side of your customer's network story, you can't really plan the network connectivity side," Fisher says. "It's like planning a highway. Without identifying the neighborhoods and where the offramps should go, how will the highway you build be useful?"

Example: A variable frequency drive (VFD) takes instruction from a programmable logic controller (PLC) to run a conveyor. If the PLC can't tell the VFD to operate, nothing's going to move.

Says Fisher, "Besides the PLC telling the VFD when to move the conveyor, the VFD needs to tell the PLC, 'I'm moving' or 'I've faulted.' There's a conversation between these two devices that the network needs to support."

Let's make this clear: contextualizing data

After data flow is defined for your customer, Fisher recommends focusing on data contextualization next. "Once you determine where your customer's data needs to move in the network, add context to remove ambiguity," says Fisher.

> "Unless you know the data side of your customer's network story, you can't really plan the network connectivity side"
>
> — **Mike Fisher**,
> Senior Manager of Solution Architecture

For instance, a raw data tag might be "18." But that leaves many questions:

- Does "18" refer to temperature? Fahrenheit or Celsius?
- Does it refer to weight or an electrical property, like amperage?
- Where is the decimal point actually located, if there is one? The "18" might be 0.18, depending on the units.
- If several assets are producing the same values, how will your customer tell which one came from which machine?

Whether integrating SCADA software, a computerized maintenance management system (CMMS), a warehouse management system, an execution system or an AI engine, reducing ambiguity makes integrations faster and less error prone. This is often the first step in creating a **unified namespace** for your customer—a foundational model of data to promote consistency and transparency in information exchange.

Start making sense: data orchestration

Lack of data availability at the OT level is a critical blocker for your customers. It prevents implementation of proactive measures for security and predictive maintenance. The right data at the right time helps them act fast, like when minimizing the impact of cybersecurity incidents.

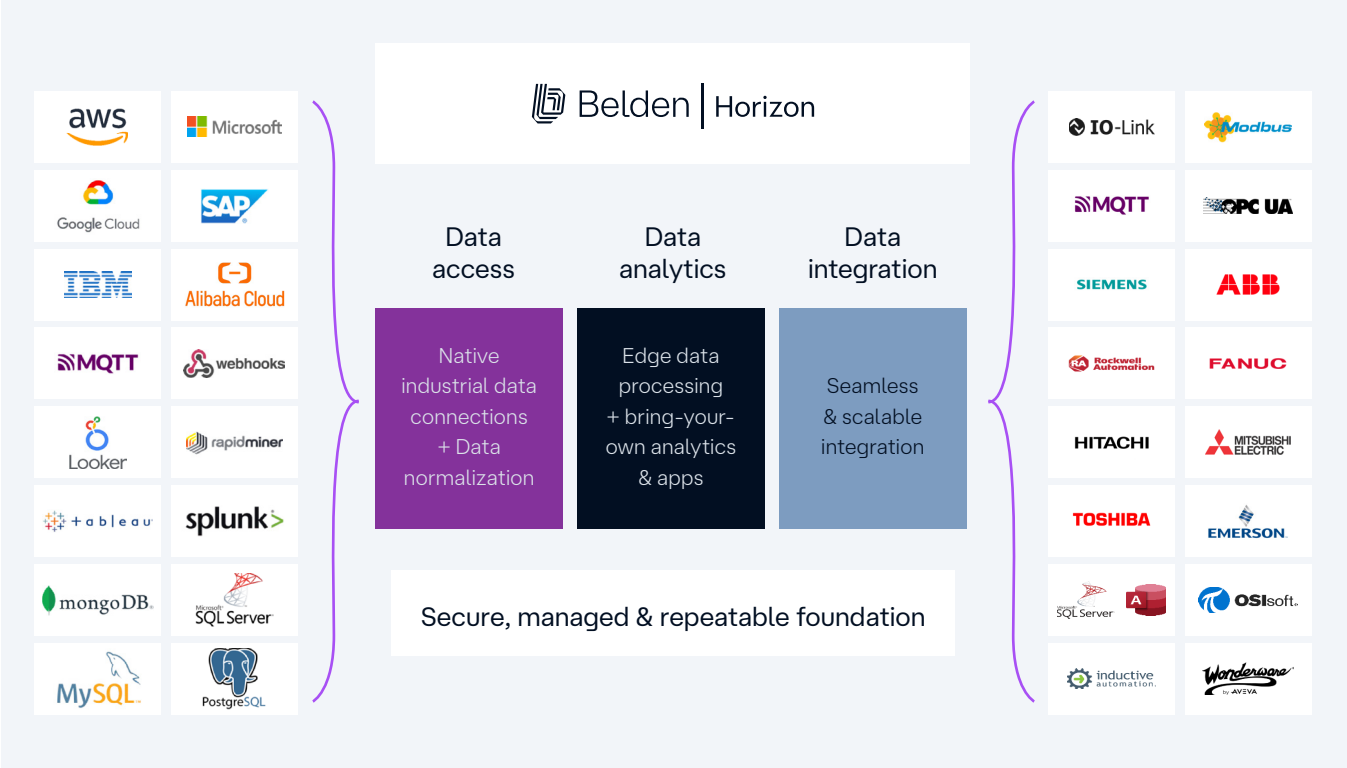
The problem of data availability can be compounded by a lack of integration and protocol translation between control and management systems across the warehouse. Without this interoperability, systems operate in silos, which reduces efficiency. Smart data management and planning on your end can prevent these scenarios for your customers.

It may make more sense to have these devices talk to a central platform that aggregates information from many sources and acts as a broker, passing information to other systems. For example, Belden Horizon Data Operations (BHDO) collects data from OT devices for contextualization and analysis at the edge and then transfers data to IT systems for storage, further visualization and analysis.

This simplifies data management by limiting the number of clients that data-producing elements need to communicate with directly, creating a central point to focus management efforts. It also improves cybersecurity posture by reducing the network's threat surface.

"Data orchestration happens when you bring everything together in a single platform," says Fisher. "You can add context and do data manipulation to generate new or synthesized data." This reduces device load by shifting calculations to the orchestration layer to derive metrics like overall warehouse efficiency. It also helps avoid conflicting results. When this information is distributed, your customer can be confident it comes from a single source of truth.

Belden solves industrial data complexity



All types of machines connected

300+ PLC protocols, OPC Unified Architecture, industrial sensors, smart meters

Managed edge environment

Edge-native deployments, clouds, data lakes, machine learning studios

Seamless data integration

Best-in-class connectivity to AWS, Microsoft Azure and on-premises systems

Figure 1. Belden creates interconnected, end-to-end automation solutions to unify warehouse data across protocols.

2. Together and apart: segmentation and optimizing connections

Next up, a different form of optimization: **physical and logical connectivity** and the concept of **segmentation**.

Physical connectivity for equipment like cables and network switches is constrained by the warehouse operating environment. It's critical to consider the physical environment when designing and optimizing network hardware.

Environmental conditions also work against a healthy industrial network. Sunlight on aluminum roofs pushes temperatures up. Conveyors cause heavy vibrations. "An office space's network switch is not the same as you'd use in a warehouse," says Fisher. "An office has good HVAC and airflow, which office-grade IT equipment needs. A warehouse's minimal climate control and operating equipment contribute to the fine residue some call 'box dust,' and that dust will choke a regular IT switch. You need something more robust."

Beyond prematurely failing equipment, the primary causes of network failure encountered by Fisher and Hammer relate to cable installation: not only substandard cabling but also poor-quality installation and incorrect termination.

This can cause difficulties that are hard to isolate later. Networking equipment may try to compensate and salvage the connection by shifting to a lower bandwidth. "We often see intermittent errors as a result," says Fisher. "The network may work fine for a while and then stop when it hits a critical threshold, like traffic volume, ambient humidity or some other random trigger."

Evaluating physical routes between data assets helps optimize connectivity paths. The physical path layout is also important for redundancy.

Some OEMs and SIs think they're creating a redundant connection by simply installing two cables right next to each other. But, if an errant forklift cuts the primary cable, it will likely cut the cable right next to it, too. Routing the cables along independent paths provides true redundancy.

This concept also plays into segmentation. "The ability to segment your customer's network is essential," Fisher says. "It's never too early to start planning that, especially in the physical layer. Grouping connections for assets and devices can help you route them through the network so unrelated systems don't need to interconnect until higher up in the network."

The path from physical to logical

Logical connectivity can route network traffic flexibly and efficiently through different physical links. This segmentation enables connections that provide redundant paths within a network.

Logical connectivity can be optimized by sizing connections appropriately for anticipated data flow. "The regular traffic baseline is typically only a small proportion of the total link capacity," says Fisher. "But infrequent tasks like remote access and equipment backups and updates add substantial traffic. You also need space for increased future traffic."

OEMs and SIs can optimize data structures, too—usually the second step in creating a unified namespace. It's possible for individual pairs of data devices to communicate directly; in smaller systems, this might make sense. As systems scale, however, data devices often need to communicate with multiple assets. Nearly all devices will eventually reach their maximum connection limit.

As discussed earlier, a centralized platform like BHDO can reduce total network traffic flow and the total number of data connections needed. This streamlining happens only when the network's disparate devices and systems speak the same language.

OEMs and SIs need the ability to harmonize protocols with an agnostic open standard (and to use protocol translation to help bridge languages where needed).

This is where data contextualization pays off. Adopting a common nomenclature and using metadata helps with context while consolidating data in the unified namespace.

It also highlights the need for **logical segmentation**. It's common in warehousing and logistics to have a relatively flat network, with everything in the same address space, perhaps even in the same virtual local area network (VLAN). "I've gone into facilities with thousands of network-connected devices, and you can see all of them from anywhere in the network," recalls Fisher. "That's a cybersecurity nightmare."

Lack of segmentation can also cause problems with network stability. Typical protocols can only work for so many hops through a network before they break down and actively cause problems.

VLANs are commonly used to add segmentation to network infrastructure without end devices being aware of it. “It adds an ID onto Ethernet messages so the networking infrastructure knows where it can and can’t send that message,” says Fisher. This approach streamlines network traffic and prevents connections from talking to each other.

“It’s important to know that each of these strategies introduces complexity to your network. You don’t want complexity without good reason,” Fisher notes. A flatter network is simpler to understand but more prone to problems, such as a broadcast storm.

Caught in a broadcast storm

Broadcast storms can occur for many reasons:

- An uncontrolled loop in the network circulates traffic endlessly.
- A failing networked device inundates the network with traffic.
- Multicast messaging — when data is sent simultaneously to select receivers or nodes — malfunctions and floods your customer’s network.

The result is a denial of service, which is a tough problem for a large network to handle without proper segmentation.

Hammer elaborates: “If you have a small network of 50 devices, you don’t have to worry as much about segmentation because the traffic level is low and the Ethernet standard protocol automatically enables retransmission. It can heal itself for a small number of dropped packets.”

But, for a full warehouse or distribution center with thousands of networked devices, it’s a lot to manage. “It’s hard to find the source of a broadcast storm,” says Hammer. “But, with network segmentation, only the segmented part experiences the error. A segment may only have a few hundred devices and 20 switches or routers, so it’s easier to troubleshoot and doesn’t take down tens of thousands of devices.”

> “With network segmentation, only the segmented part experiences the error. … It’s easier to troubleshoot and doesn’t take down tens of thousands of devices.”
>
> — **Aaron Hammer**, Professional Services Manager

Greenfield or brownfield, Belden has the solution

Planning for physical and logical connectivity applies to new greenfield scenarios and the modernization of established brownfield installations. “Although a ‘rip-and-replace’ approach offers advantages, we find that many clients don’t choose that route,” says Fisher. “It’s usually expensive, and switching out hardware can cause significant downtime.”

Belden’s experts find solutions that fit into gaps and seamlessly integrate with what’s in place. “We’ve helped clients who installed their systems but encountered problems,” continues Fisher. “We re-engineer their network based on what they have. Keeping as much existing infrastructure as possible usually means a smoother rollout.”

You can exercise control over segmentation even after your customer’s network has been deployed. In a brownfield state, you can tweak settings and manipulate elements late in a project’s lifecycle. **Belden’s superpower is deep experience and expertise with all forms of networking**.

As Hammer explains, “Many engineers in the industry know automation well, but networking, not so much. They may make a network change but don’t have a good metric to measure effectiveness. They fix symptoms that mask an issue’s root cause, which later causes unplanned downtime. The wise ones reach out to our networking experts and ask, ‘Can you help?’ ”

3. Zones and conduits: securing your network

The industrial space has received its share of malicious attention from hackers. A 2024* Gartner report predicts that supply chain organizations will continue to face cybersecurity risks, including potential attacks from AI-generated tools. The supply chain is also raising security concerns as vendors become increasingly interconnected.

“It’s imperative to understand the risks your customer’s partners can present to cybersecurity,” notes Mayo.

But amid the fear and uncertainty, it’s important to help your customers avoid the misconception that good cybersecurity is overly complex. “The industry has made cybersecurity sound far more complicated than it really is,” continues Mayo. “The basics are easier to implement than you think. Don’t be overwhelmed—cybersecurity is achievable for your customers.”

Another misconception common among some industry professionals is that cybersecurity is something you can add at the end of a project. “That’s like saying a car’s seat belt is an optional element. If you don’t have a seat belt, the car will still start and drive down the road,” remarks Fisher. “But, if you crash, you’re going to get hurt.”

Cybersecurity should be baked into your customer’s network design and management from the start. Whether you use dedicated network tools for monitoring, or a network management system (NMS) like Belden HiVision, network segmentation is essential. Designing this security measure into the network ensures that only authorized elements can connect to each other.

To be truly effective, security must be deployed throughout all zones and conduits of a network and considered part of foundational design. Ideally, network cybersecurity uses a defense-in-depth strategy so multiple firewalls and processes contain damage if individual systems are compromised.

*Gartner Identifies Top Trends in Supply Chain Technology for 2024, Gartner, March 2024

Layering IT & OT with a DMZ

Warehouses and distribution centers face heightened security challenges due to how they combine IT and OT. “It’s very common for security breaches on the IT side to bleed into the OT space,” says Fisher. “Gone are the days of air gaps. IT pockets are distributed throughout the OT environment.”

OT assets are usually less able to protect themselves. Most industrial devices are optimized for speed and reliability and can’t host anti-malware programs.

A “demilitarized zone” (DMZ) offers a way to control information that passes between IT and OT. Within the DMZ’s layers of protection and management, IT and OT each have their own firewall that connects to a shared server area. Both sides can access that inner zone but not reach beyond.

Typically, IT/OT boundaries are funneled through a single DMZ. In warehousing and logistics, depending on facility complexity, multiple boundaries and DMZs can be created. Throughout the security design process, segmentation and redundancy should also play a role.

“We have routers that provide redundancy for issues like cable breaks, when you need to reroute traffic,” explains Hammer. “These routers enable you to change subnets and IP addresses, which blocks multicast and broadcast. This provides efficient communication and an extra layer of security.”

Hammer continues, “In a facility with 10 production areas, a hacker would have to break into 10 different areas to access everything in that network. Segmentation is another layer of security that slows hackers down. More effective monitoring and management helps you detect and respond to breaches sooner.”

4. Manage it, monitor it: fine-tuning your network

A well-functioning network is not a set-it-and-forget-it proposition. It requires constant tuning and updates for optimal effectiveness.

The best method for tracking increasingly automated warehouse networks is using an NMS like Belden HiVision. Systems like this have long been a linchpin in the OT world.

As your customers' networks grow larger and more complex, the demand for comprehensive and efficient management correspondingly increases. The goal is to be able to identify, map and configure all network devices, no matter the manufacturer.

Many NMS options are IT-centric, with limitations regarding OT protocols. "In the IT world, data security is paramount," notes Fisher. "But the OT world is about availability, making sure the network is up and running."

Offering the right NMS can help you create a thorough asset inventory for your customers. "They can have the NMS find everything in a particular area, in minute detail, or actively assess the entire network," says Hammer. "This visibility is critical, yet most of our clients lack full visibility into what's happening in their network."

Move along, uninvited devices

NMS asset inventory capabilities also help you improve security and segmentation for your customers. "At one facility, we discovered a wireless router someone added because they wanted Wi-Fi in the lunchroom so they could work there," says Hammer. "It wasn't malicious, but it was an opportunity for bad actors to harm the network."

Hammer encountered several instances of employees adding devices that shut down a network due to duplicate IP addresses. The right NMS can perform an asset inventory on the OT side—known as rogue device detection—and automatically identify and quarantine any unauthorized device. This is another reason segmentation is important: Issues like these can be localized to reduce impact.

An NMS also helps make the updating process significantly simpler, with fewer missed patches. "It would be great if you could deploy a piece of software or hardware and never need to touch it again," states Fisher. "But there's new functionality to add and vulnerabilities and bugs to fix. Teams need to consistently update the firmware in network infrastructure devices."

With even 30 switches, let alone 300 or 3,000, manual updates simply aren't practical. With the right NMS, mass updates can be performed by selecting a collection of devices and pushing the update in a few quick steps.

"The NMS can also give you information about how long an update took and whether it completed successfully," adds Hammer. "Running these technology updates in a multiconfiguration situation is a huge time-saver.

Can't stop, won't stop: continuous network monitoring

An NMS is a powerful tool, but your customer can't react to something they can't see.

Ethernet technology makes networks highly resilient. But there's a problem. "Network resiliency without monitoring can work against you in the long run," explains Hammer. "Issues may occur in the background, and an unhealthy network can function for quite a while before a major incident. This is why you need to monitor continuously rather than getting snapshots."

If network monitoring software is used to specify which devices to monitor, the NMS can request data from those devices periodically, perhaps every 30 seconds. Rather than a data push, the software pulls information from the devices, which isn't best practice.

"It can be harder to get root cause analysis when you pull information," says Hammer. "Our network infrastructure equipment proactively alerts the monitoring software when it notices an issue like Ethernet retransmissions hitting a certain threshold. Retransmissions aren't troubling if there are only a couple a week. But, if you have 10 issues within five minutes, something's going bad."

Continuous monitoring captures all events and tells the NMS to send an alert to the right people, providing actionable information to help address errors before they can bring down the whole warehouse network.

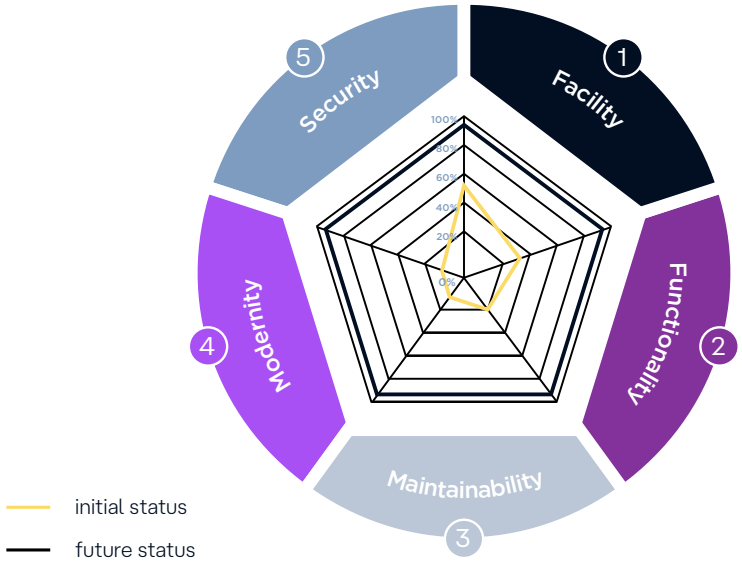
Assessing your customer networks: Why Belden

We've covered a lot of information in this guide, but it's only the beginning. Designing and integrating OT networks is a complex, never-ending process. A warehouse network may seem stable on the surface, but hard-to-detect issues may lurk underneath. The good news? Belden has the experts, experience and insights to be a knowledgeable and reliable resource that can empower you to help your warehouse customers thrive.

Belden's Network Assessment Service (NAS)

Our Network Assessment Service (NAS) includes a five-step evaluation of your customer's network strengths and weaknesses, plus guidance on prioritizing and implementing targeted improvements.

Network panoramic rating framework: a holistic assessment approach



1 **Optimize facility:** Ensure network application, environment, and standards align with best practices for management, connectivity, physical installation, and documentation.

2 **Maximize functionality:** Harness the full capabilities of network to maximize availability. Our assessment evaluates redun-dancies, features, and data transmission performance, ensuring optimal performance and uptime.

3 **Enhance maintainability:** Streamline network maintenance for optimal performance and availability. Our assessment includes evaluating operation, repair, monitoring, and remote access to simplify and improve network maintenance processes.

4 **Embrace modernity:** Stay ahead of the curve with the latest technology advancements. Our assessment analyzes hardware, software upkeep, protocols, and data technologies to ensure you are leveraging cutting-edge solutions for improved network performance and future-proofing.

5 **Strengthen security:** Safeguard network from threats and vulnerabilities. Our assessment evaluates network architecture, device configuration and operation, and maintenance practices to reinforce network segmentation, access control, patch manage-ment, and security mindset, ensuring robust protection for critical assets.

Networking can get very complicated very fast.

Belden lives and breathes this every day. We're ready to do a network assessment for your customers at any stage to determine what needs to be upgraded, what needs to be replaced and what they should keep. This saves you time, saves them money, gives their network room to grow and gives you an unmatched competitive edge.

Request a network assessment

Connect to what's possible.

White Paper

About Belden

Belden Inc. delivers complete connection solutions that unlock untold possibilities for our customers, their customers and the world. We advance ideas and technologies that enable a safer, smarter and more prosperous future. Throughout our 120+ year history we have evolved as a company, but our purpose remains – making connections. By connecting people, information and ideas, we make it possible. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia and Africa.

For more information, visit us at:
belden.com

follow us on

Belden