BELDEN

# Upgrading to EV Production?

## Belden's solution will ensure fast, reliable, communications across all operations in your automotive manufacturing plant.

EBOOK

**Will this be the year you enhance your industrial networks to meet future market demands?** Can you protect your investments, and ensure your new lines run as expected as you complete today's EV-driven auto plant transformations? How about guarantee the ability to add capacity and value as you secure your position in tomorrow's automotive market?

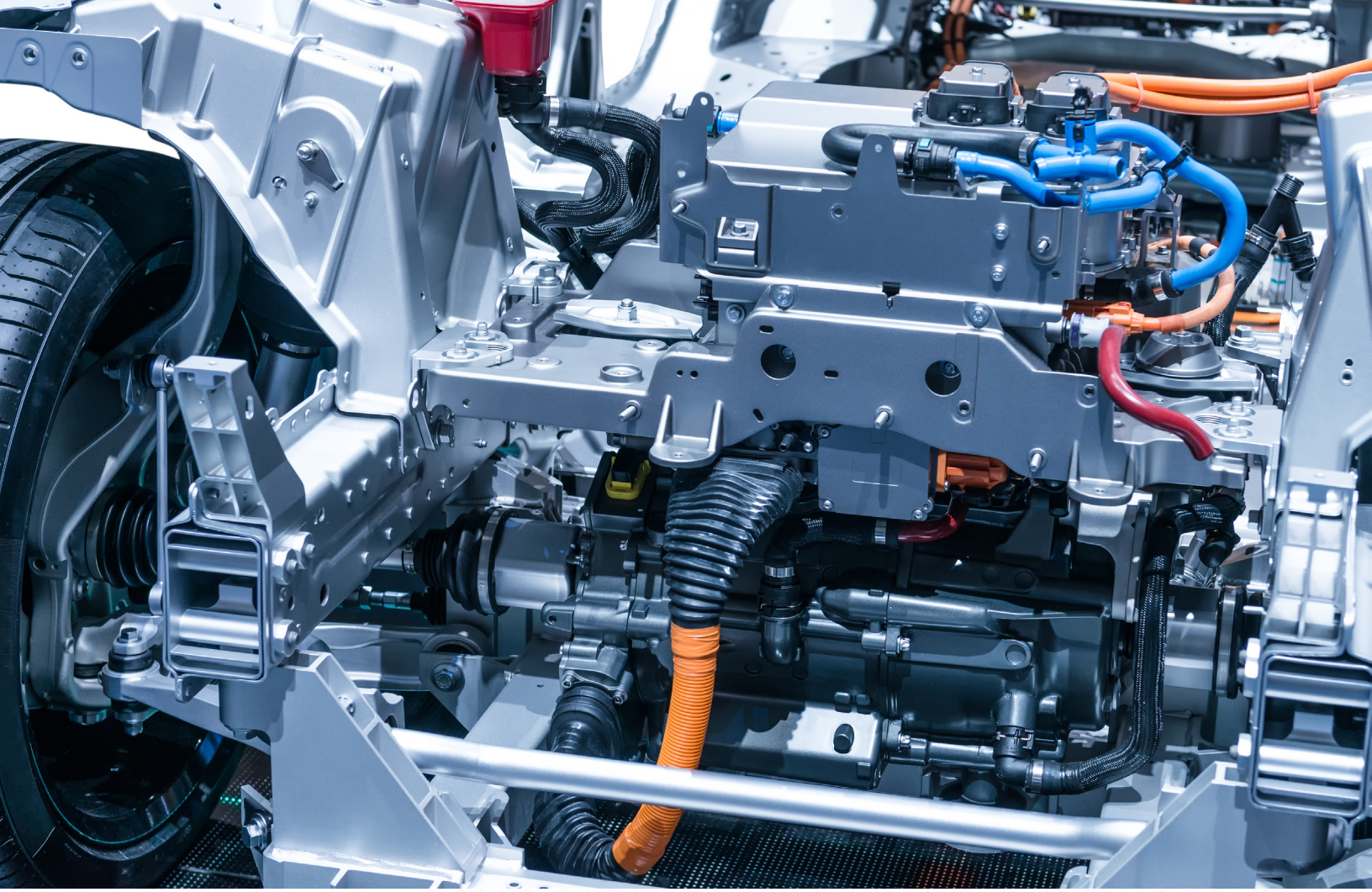
Yes... **If you optimize your network.**

With demand for electric vehicles (EVs) quickly supplanting demand for traditional ones, most automotive manufacturers have embarked on line transformations unparalleled since the introduction of the Modicon 084 PLC in the 1960s.[1]

This massive effort presents the perfect opportunity to complete your migration to Industry 4.0.

And, you can't reach Industry 4.0 without a deep, pervasive, robust network solution.

1 "Shift to EVs Triggers Biggest Auto-Factory Building Boom in Decades." Wall Street Journal. January 1, 2023.



## The Opportunity

Savvy auto manufacturers like you know that consumers are all in.

**EVs made up the fastest-growing segment of the auto market,** with 2022 sales exceeding 150% of 2021.[2] So far, 2023 doesn't appear to be bucking that trend.

Savvy auto manufacturers like you also know that regulatory bodies are all in, too.

The state of California is moving to ban the sale of gasoline-powered vehicles by 2035 and at least 15 other states plan some version of restrictions.[3]

At the national level, the Inflation Reduction Act in the United States encourages the manufacture of more EVs in North America.

Internationally, many countries are moving in a similar direction:[4]

- Germany, Iceland, Ireland, India, Israel, Netherlands, Singapore, Slovenia and Sweden aim to ban gasoline-powered vehicles by 2035.
- Norway has a more progressive goal of 2025.
- The United Kingdom, Canada, Chile, Denmark, Japan, Korea, and Thailand are aiming at 2035.
- Armenia, Austria, Azerbaijan, Belgium, Cape Verde, Croatia, Cyprus, Egypt, El Salvador, Finland, France, Lichtenstein, Lithuania, Luxembourg, Malta, New Zealand, Poland, Portugal, Spain, Sri Lanka, Taiwan and Uruguay have pledged a phase-out by 2040.

Aside from these target end states, many are planned to be phased in starting within the next few years. This means that the markets are poised to see rapid growth in the very near future. The faster producers can make models available, the sooner they can establish market share.

2 "Global EV Sales for 2022." EV Volumes

3 The International Council on Clean Transportation

4 EU Lawmakers Vote to Ban Sale of New Gasoline-Powered Cars From 2035

## Massive Investment in Line Transformations

The resulting rise in demand for EVs has sparked a fire under manufacturers to quickly scale up production.

Reuters reports that the world's top automakers plan to spend nearly $1.2 trillion through 2030 to establish EV production lines.[5] "The world is changing very, very fast," Herbert Diess, then CEO of Volkswagen, told Fortune, in early 2022. "Eighty-plus years' success in auto manufacturing and design is not sufficient for the future.[6]"

Diess may have understated just how fast and how hard the EV future is hitting.

Throughout 2022, demand increased.

In 2021, 10% of drivers planned to make their next purchase an EV and in Canada, that number is much higher at 58%.[7]

The number rose to 14% in 2022.[8]

In October 2022, the World Economic Forum reported that EV sales had grown by 75% over the prior year—that's not even counting the 37% growth in plug-in hybrid EVs.[9]

In the U.S. alone, projections indicate that by 2030 EV sales will increase to 4.7 million from only 500,000 in 2021.[10]

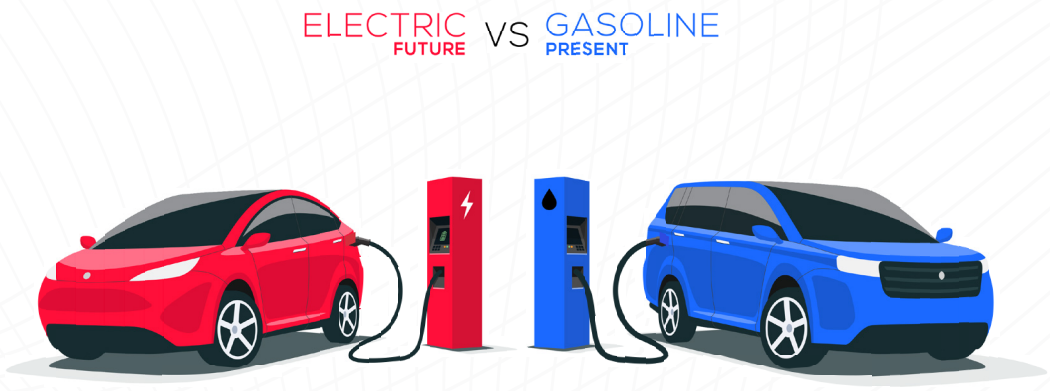
## Transformation Headaches

As you know, demand still somewhat outpaces supply.

In December 2022, buyers who wanted the most popular models still faced waiting lists.[11] For one manufacturer, wait times ranged from three months to several years depending on the model.[12]

Manufacturers like you already face the headaches of component shortages and supply chain issues.

The last thing you need is for your production resources to hold you back when your restrictors finally loosen. If you don't give your network the proper attention now, you will face line issues with your new configurations in the next few years — or when you attempt to expand capacity down the road.




5 "EV battery production faces supply chain, geopolitical headwinds – report," Reuters, Oct. 31, 22

6 "The EV race is one of the most fascinating business stories of our times," Fortune, Jan. 31, 2022

7."Rising interest rates pushing EVs out of reach for Canadians," Financial Post

8 "Electric vehicles: The 3 main factors holding back sales," World Economic Forum, Oct. 26, 2022

9 "Electric vehicles: The 3 main factors holding back sales," World Economic Forum, Oct. 26, 2022

10 "EV Sales Forecasts," evadoption.

11 "Next year is a good time to buy an EV — but for many consumers, 2024 might be better," NBC News, Dec. 13, 2022

12 "Wait time for new Toyota Vehicles," EVTO Blog, January 2023

## The Dilemma

Like many auto manufacturers, you may feel pulled in two directions.

On the one hand, you have a profitable assembly line designed to provide still-in-demand gasoline-powered vehicles. After all, traditional vehicles accounted for more than 95% of the new car market worldwide in 2020 and still show strong demand.

But you see the future coming fast and want to retool production to capitalize on market trends.

To meet the market demands, you need to retrofit or build new capacity for the EV-dominated future that is arriving faster every day.

The dilemma will continue for many years, since EVs aren't expected to capture even 60% of all new vehicle sales until 2030.[13]

## The Network Opportunity

As you plan and deploy new manufacturing capabilities in the race to EV production, it's easy — and perhaps more fun — to focus on the visible, tangible parts of the production process.

We understand — robots and autonomous vehicles are exciting.

But these advanced technologies are only effective if they can integrate and communicate efficiently with the rest of your operations.

And not just your production assets.

So many interrelated systems interact with data points across your operations — from performance dashboards for the operations team to predictive analytics software for the maintenance department to quality assurance equipment to order entry and control systems and many more.

Because production technologies change almost as fast as market demands, it's important to keep in mind that building flexibility and adaptability into your network now will translate to future-ready operations tomorrow.

After all, who wouldn't like the freedom to incorporate new technologies as they come along rather than letting legacy technologies dictate what your operations can accomplish.

While you are planning, why not hedge your CapEx bets and invest in the robust network solution you really need to power Industry 4.0 operations?

At the very least, bring in an expert to assess your current and future needs.

Even if the robust solution you might dream of today isn't completely achievable in one step, you can prepare a more flexible solution that will be easier to upgrade as your plans develop.

## Get Future-Ready

Unfortunately, it's no longer enough to be future-proof.

Auto manufacturers must be ready for what the future holds.

This means you must prepare at the network level for greater manufacturing autonomy and interconnectivity, for 24/7 production schedules and the heightened security risks of our digital age.

A consultation with a Belden expert can help you capitalize on the momentum of consumer demands while also leveraging the capabilities of Industry 4.0.

The result? More agile, adaptable and profitable operations now and into the future.

## Don't Just Catch Up, Get Ahead

If you're simply future-proofing your operations for today's EV boom, you may be missing a critical opportunity.

Current line transformations offer the perfect opportunity to optimize your OT networks — from the operational backbone down to the production floor and out to the building automation systems — to make them ready for tomorrow's technological advances.

13 "Automotive Industry: What the future holds," infomineo, May 17, 2022

## Follow a Proven Path

Belden's experts have a step-by-step roadmap to help manufacturers like you take advantage of network enhancement opportunities as you plan for and pursue production line transformations.

Our plan defines the seven considerations to incorporate today, whether the project is a brownfield upgrade/retrofit or a greenfield startup.

Plus, our plan recognizes the reality that legacy infrastructures still hold value in an EV world — value that can only be leveraged with a flexible, powerful migration solution.

The path to future-ready starts with these seven considerations.

## Understand Your Motivation

Think beyond what you want to do now.

What do you dream your manufacturing processes might do in the future?

An optimized network can pave the way to making those dreams a reality.

Your network is the single-most critical enabler of your manufacturing capabilities and the only way Industry 4.0 innovations can bear fruit.

Distinguishing between the must-have-now and the nice-to-have-in-the-future features will allow for the strategic implementation of network updates.

Start with an assessment of your current-state and future-ready aspirations within these common, broader use cases:

1. **Performance Monitoring:**
   Catalog your current performance measures — everything from cycle counts to pass/fail rates to temperature and power consumption data and beyond. How do you gauge success in your production operations?
   Think about how those measures and the devices may evolve with Industry 4.0.

   Consider where the data is coming from and going to.

   As the data transitions from OT to IT networks and back, integration between the OT and IT systems needs to help ensure production line and plant-wide operational excellence.

2. **Intervention:**
   As your continually more powerful performance monitoring mechanisms identify potential opportunities for process improvements, how do you plan to implement each change?

   Automated interventions powered by advanced artificial intelligence (AI) interacting with remotely connected devices to perform things like tooling offsets demand more bandwidth from your IT and OT networks.

3. **Troubleshooting:**
   Ever-tightening production schedules mean troubleshooting must be fast and seamless, calling for:

   a. Improved redundancy to prevent bumps in the road from derailing your operations.
   b. Real-time monitoring of equipment and production so that problems can be identified early.
   c. Remote access capabilities so that the right technicians, engineers, and equipment vendors can be engaged directly, without delay, no matter where they may be in the facility, country, or world.

4. **Proactive Maintenance:**
   Software is eating the world, and your production line is next on the menu.

   Maintaining a growing arsenal of software-enabled devices and processes requires the controls engineers who administrate your OT network to push frequent firmware and program updates.

   And, the OT network has to be capable of delivering those upgrades at the speed of production demands.

## Know Your Data

Right-sizing the mechanisms that transport your data requires a clear understanding of data volume, flightpaths and destinations.

Like the volume of water that can flow through a pipe, the more bandwidth a network has, the more data it can send and receive at once.

As we evolve to adopt more bandwidth-heavy operations—moving from periodic temperature checks to streaming camera data, for example—bandwidth capacity must account for not just the data traffic but also the added overhead of management components.

Network redundancy protocols like rapid spanning tree protocol (RSTP) and media redundancy protocol (MRP) and device management protocols like simple network management protocol (SNMP) and link layer discovery protocol (LLDP) all demand additional bandwidth concurrent with standard network management traffic—and that's on top of the data needed to coordinate, monitor and perform the production operations.

## Assess Your Criticality

Designing your most critical environments with the right network topologies safeguards against failures now and makes the addition of future technology easier, faster and safer.

How critical is each device in your network?

What is the cost of Device A failing versus Device B?

Will your network continue to function after two or three failures within one system but come to a grinding halt with a single failure in another?

This type of assessment is essential to determining appropriate network topologies and bandwidth requirements.

In a linear network topology where all nodes are connected to a single line, like with an old string of Christmas lights, a break at any point will take down all the connected devices.

Alternatively, a ring topology, where infrastructure nodes are redundantly coupled to each other to form a ring of connections, can withstand the loss of a single link and won't fail until the loss of a second.

On the other hand, the aptly named star network topology connects single-point end devices to a central switch, offsetting the introduction of more potential failure points by limiting their influence on other connections.

A smart network topology isn't just important for limiting network failures and doesn't have to be made up of only a single topology.

Done well, the right network architecture allows your entire organization to understand how different network elements work together and connect.

Perhaps more importantly, a smart network topology enables deterministic behaviors so that you always know what will happen next.

Combining the right network topology with advanced digital insights about what's going on inside your network can improve performance now and enable strategic connection of new technology in the future.

## Plan to Expand

It's hard to estimate what your network needs will be tomorrow, but being future-ready requires that you try and Belden experts can help you make more accurate predictions.

An automotive manufacturing client recently turned to us with a bandwidth challenge.

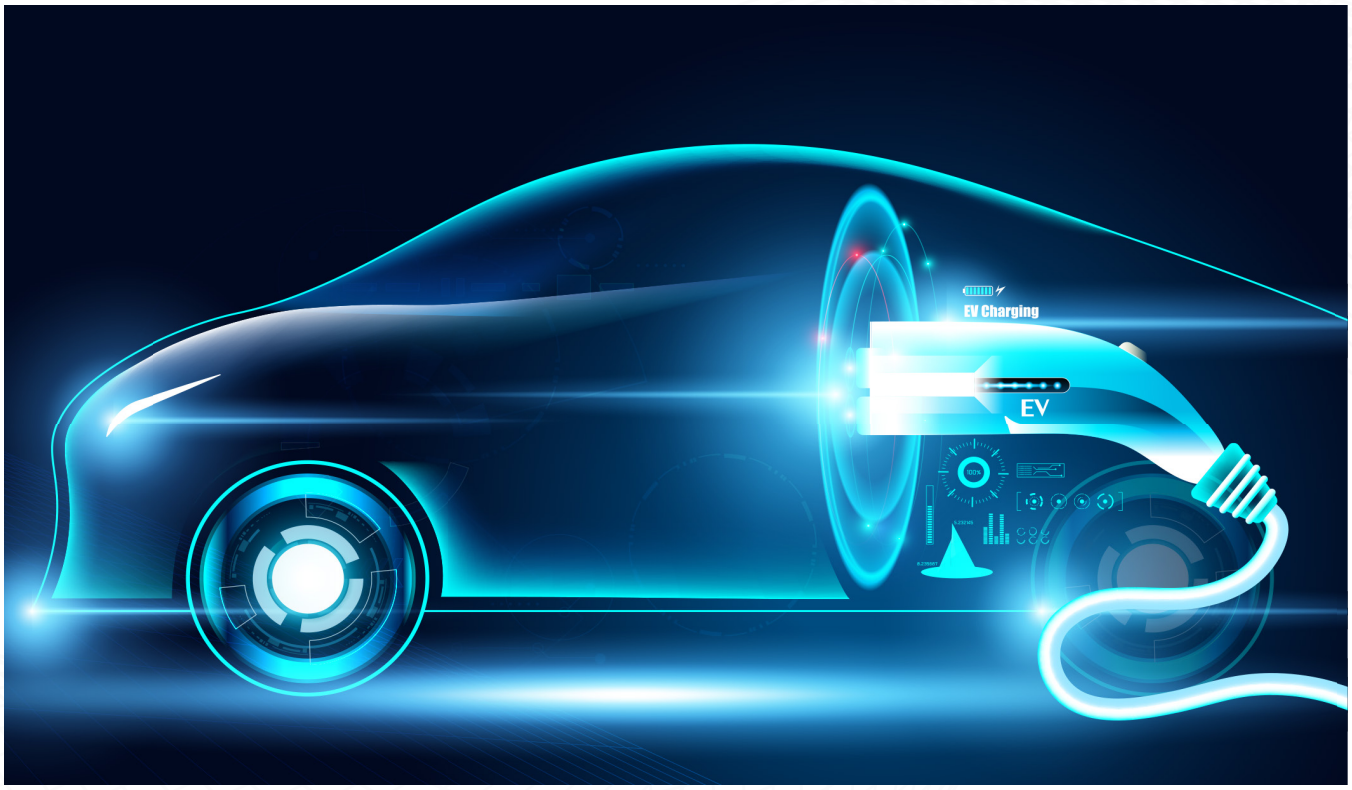
When their standards were established and networks built in 2016, their bandwidth was more than sufficient. But by 2021, their network was failing to keep up with the demands.

They had added video cameras to monitor processes and equipment for quality control – cameras that gobbled up bandwidth to a degree that would have been unfathomable five years earlier.

Had they installed higher-bandwidth connections before, even when steaming video was just nascent technology, they could have very quickly and easily captured the full value of a range of new technology add-ons.

Instead, the streaming video sources overwhelmed the network, dramatically reducing the video quality and impact.

It's hard to guess what the future holds.




But we can be confident that Industry 4.0 is introducing a lot more data producers and consumers to the network:

- Expanded partnerships with technology and government entities.
- Extended reality.
- An automation explosion.
- The fully "dark" factory.[14]
- Whatever else human ingenuity introduces…

For each advancement, your backbone network can only enable success if you follow a smart plan that balances future growth projections with today's implementation costs.

14 "The 10 Biggest Future Trends in Manufacturing," Forbes, Jan. 25, 2022

## Build in Security

As the number of processes and functions touched by IoT (Internet of Things) devices grows, improving endpoint security must be a priority.

Physical security is one thing.

Usually, you can easily physically secure access to your plant, your departments, and your ports. But how are you securing the increasing number of connected endpoints?

Endpoint security is highly complex, and Industry 4.0 certainly doesn't simplify the challenge.

Most IoT devices connected to your network can't be authenticated like an employee with a username and password. Even equipment with more intelligence like a programmable logic controller (PLC) can't log in when it wants to connect.

Yet, these devices are consuming bandwidth and data.

It's common that these devices are built on legacy tech stacks from OT and IT systems, then streamlined for production speed, shop floor efficiency and process control.

Security was a secondary consideration if it made the list at all.[15]

Often, this makes traditional end-point protection impossible, forcing network administrators to resort to isolating devices within segments of a network behind layers of additional security. This obviously adds cumbersome complexity.

Moreover, your network needs to be assessed constantly against three future-ready security priorities:

1. Check connected devices for vulnerabilities against an incessantly updated list of known threats.

   Organizations like the Cybersecurity & Infrastructure Security Association (CISA) track and report threats against operating systems, but the effort to review the list and flag network devices that appear in the list requires a full-time person… maybe more.

   Software tools that digest the updating list of vulnerabilities and probe end-devices through the network are a core feature of future-ready security.

   Belden and our ecosystem partners provide this service for many of our auto manufacturing clients to keep them on top of potential vulnerabilities.

   Of course, deploying the firmware updates to shore up vulnerable endpoints requires resources and bandwidth, too.

   This excess loading necessitates that tools be not just available but actively working in order to simplify the update process.

   Approving and installing updates to your devices — cameras, control blocks, network switches, computer terminals, and the like — can eat up as much or more time than it took to install the devices.

15 "The manufacturing industry's security epidemic needs a zero-trust cure," VentureBeat, Nov. 15, 2022

2. Authenticate users and equipment as they connect. We've established that many devices can't authenticate themselves by logging in to a network, but that doesn't mean they should be given a free pass.

   Hardware and IP addresses provide a measure of control, allowing the network's infrastructure devices to selectively permit and deny access.

   Moreover, a networks management tools can challenge devices by attempting to log in to them and query for key pieces of information.

   This is easy to handle when standing up the network and configuring the switches and firewalls the first time, but your production operations aren't static.

   On any given day you may move a piece of tooling, a camera or another asset to elsewhere in your production area.

   Every time a device moves, your network requires reconfiguration — relabeling of ports, updating virtual local area network (VLAN) assignments, revising access control lists (ACLs).

   These adjustments take an inordinate amount of time to implement manually.

   In fact, the time spent implementing a change can consume much of the value that the change was intended to provide.

Consider, instead, a scenario where your network is empowered to dynamically reconfigure itself based on predefined rules.

Solutions such as 802.1X server software partnered with 802.1X-compliant switches provide a framework that authenticates users via a central authority — automatically — enabling a network to adjust to changes on the fly.

It's scalable, flexible, and more secure, and it's the only sustainable authentication method in Industry 4.0.

**"Vulnerability exploitation was the top initial attack vector in manufacturing, an industry grappling with the effects of supply chain pressures and delays."**

Source: IBM Security's X-Force Threat Intelligence Index 2022

## Monitor Network Messages for Suspicious Traffic

Network traffic is the canary in the coal mine to auto manufacturing facilities.

Certain traffic patterns indicate trouble may lie ahead and provide clues to the solution that will cut it off at the pass.

Intrusion detection software (IDS) plays an important role in identifying problematic traffic patterns.

Yet for IDS to do its job effectively, all network infrastructure devices must funnel information to and through the IDS.

That essential safeguard instantly doubles your network traffic.

Distributing that intelligence through your network allows you to reduce bandwidth requirements.

Edge firewalls performing deep packet inspection (DPI) live at line speed can recognize suspicious traffic as it flows through the cables.

And a robust edge firewall system doesn't stop at identifying suspicious traffic.

A next-generation edge firewall system takes automated, preventive action to block bad traffic and protect your sensitive assets.

## Allow for Remote Access

A traditional VPN won't enable full accessibility in an IoT world.

There are two parts to remote access:

- Ad-hoc connections for on-demand access to network drives, servers, OT assets and the like.
- Persistent connections that mimic a hardwired connection for an always-on flow of data like what's needed for off-premises data services.

Ad-hoc connections in the OT world are traditionally difficult to deploy since OT assets can't initiate an outbound VPN connection.

An IO Link thermometer or a PLC isn't likely to have a desktop display, much less a VPN client.

Further complicating the issue, IT networks shouldn't allow inbound connections from the internet without specific exceptions.

What's needed in a modern system is a gateway device deployed within a network segment to establish the outbound connection for secured remote access though a server to which pre-approved remote users can log in using one-time VPN credentials.

Persistent connections take this same problem to a new level. The must provide a stable, consistent interface for the attached systems because the operational tools that use them are very sensitive to disruptions.


These connections likely stream performance and telemetry data from the OT systems to a cloud-based analytics engine or historian.

Such steaming requires use of the same connections and addresses on both sides every time, even after network interruptions or reboots have temporarily cut the link.

Also, the endpoints need to perceive each other as though they were on the same physical network, regardless of what network paths may lie between them.

In any case, to avoid exposing your critical assets to unapproved systems, internal or otherwise, secure remote access and persistent data connections need to be authenticated in both directions.

Local gateways must be corroborated, and remote users and systems must be validated.

The only way to achieve that is through an intermediary management platform.

Aside from ensuring the security of your connections, this platform should also enable you to:

- Designate who has access to what.
- Log connections as they are made and broken.
- Track how much data is moving.
- Allow an administrator to manage how many active connections are allowed at a given time.

## Consider Your Connection Media

The connection media you use now will impact your flexibility to be future-ready tomorrow.

Copper, fiberoptic, and local and cellular wireless technologies each have their own best use scenarios:

- Copper is more flexible than fiber and the only option to offer power over ethernet (PoE), but it has far less range.
- Fiber has minimal cable flexibility but greater range and bandwidth.
- Local wireless connections via “Wi-Fi” provide the greatest flexibility but are more susceptible to noise and bandwidth constraints.
- Cellular wireless networks like those in the 5G band—often the only choice for remote location—are becoming available for private applications, but they face a traditionally higher and more granular cost structure.

It’s important to avoid defaulting to a one-size-fits-all mentality.

Belden experts help you consider your network needs on a link-by-link basis, not just today but into the future, and let that inform a custom-fit media type strategy.

## Conclusion

The rapid adoption of EVs to the automotive market is driving automotive manufacturers to re-examine how they approach all facets of the business.

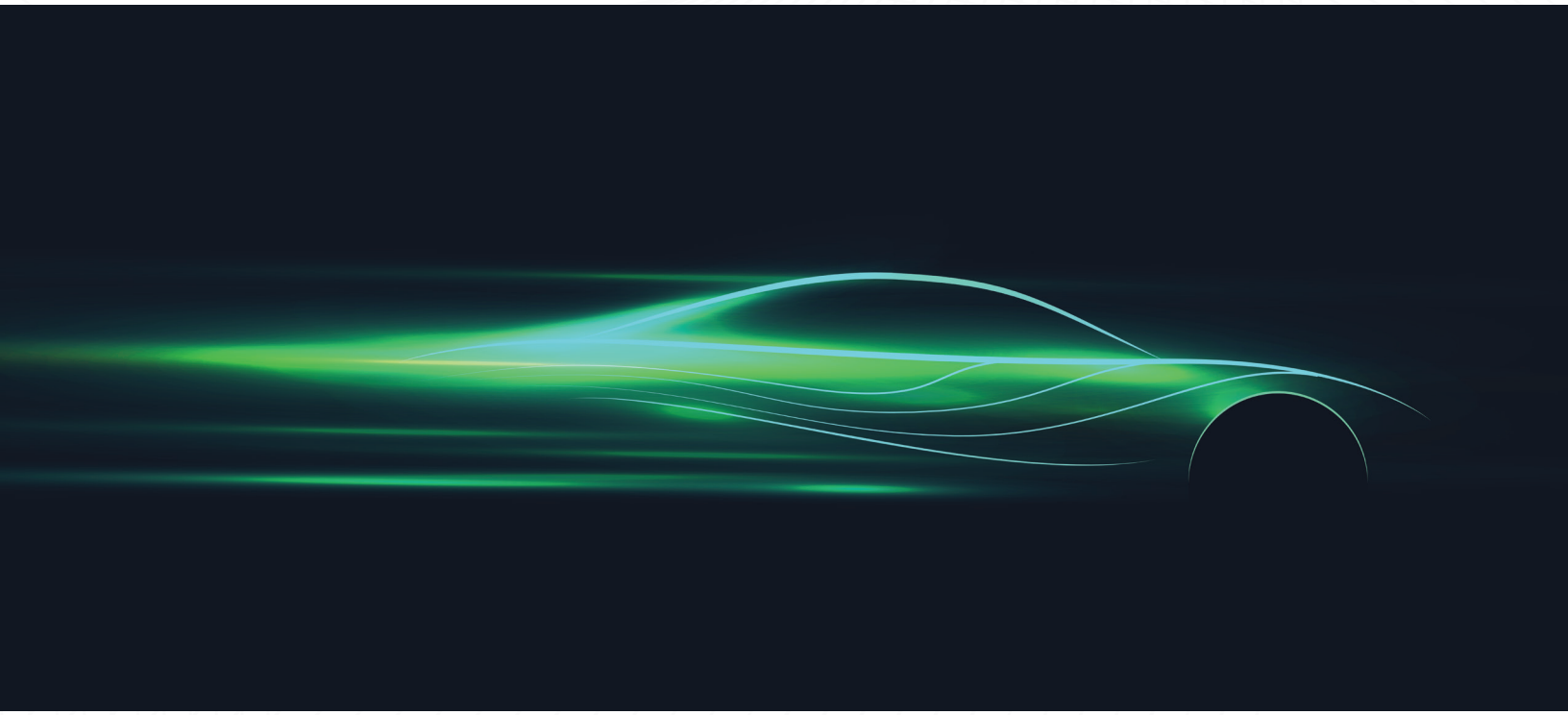
This massive disruption provides an opportunity for established names to augment the solutions that have powered their success thus far and for new players to establish themselves in a very competitive marketplace.

Now is the time to consider new OT network connectivity models enabled by new technologies that can make any production environment future-ready.

As you prepare strategies to secure your position in this bold, new frontier, it's the perfect time to also reach out to Belden to help you prepare your OT networks.

Our experts are eager to discuss and assess your vision, your capabilities, and your needs.

We work with you to imagine and implement future-ready solutions that will maximize the return on your technological investments.



**Let's build the future of automotive manufacturing.**

## About Belden

Belden Inc. delivers the infrastructure that makes the digital journey simpler, smarter and more secure. We're moving beyond connectivity—from what we make to what we make possible through a performance-driven portfolio, forward-thinking expertise and purpose-built solutions. With a legacy of quality and reliability spanning 120-plus years, we have a strong foundation to continue building the future. We are headquartered in St. Louis and have manufacturing capabilities in North America, Europe, Asia and Africa.

## Learn More

Visit belden.com for additional information and to contact our automotive solution experts.