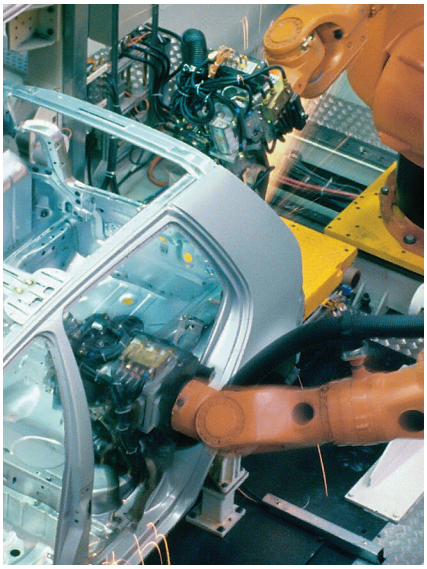
BELDEN
SENDING ALL THE RIGHT SIGNALS

Solution Guide

Discrete Automation Vertical: Cyber Security Solution Guide

Market Dynamics Facing all Discrete Automation Sectors

How do discrete manufacturers stay competitive and productive, reduce costs and cycle times, increase yields and gain market share? Through digitization. Digitization means connectivity and data. As more and more devices - from field I/O to every layer of the supply chain – are connected to networks, silos are removed and data from each device can be transformed into a treasure chest of valuable information. This digitization revolution is Industry 4.0 and it is no longer optional - it's all about survival in this new data-centric, connected world.



Connectivity Comes with Concerns

Connectivity drives industrial automation. Connectivity drives process monitoring. Connectivity drives remote access. Connectivity also opens the once air-gapped or physically-isolated control networks to the world of cyber security, where malicious, unintended, or accidental human behavior - all of which could happen remotely through the network - could have negative impacts to brand reputation, human safety, operational productivity, and product quality.

Belden – Sending the Right Signals, Securely

Belden is a strategic partner to discrete manufacturers, allowing you to embark and excel on your Industry 4.0 journey. Belden's solutions drive connectivity from industrial cable to connector to IO block to network switch, router, and industrial firewall - these are key foundational components in the new world of Industry 4.0.

Step One: **Visibility**

Having visibility of your manufacturing environment is the first step to a cyber-secure environment. How can something be secured if you do not know it exists on the network? **Tripwire Industrial Visibility** and **Tripwire Log Center** provide this visibility by:

- Allowing you to understand all the devices on your control network, what they are communicating with, and when their configurations change.
- Correlating log events from multiple sources and writing rules to flag events of interest. For example, if a failed login is attempted 5 times on an important device, **Tripwire Log Center** emails an automatic notification to the network manager.

Step Two: **Protective Controls**

Start with two basic, fundamental measures: network segmentation and device hardening. **Belden Industrial Networking** solutions and **Tripwire Enterprise** can both be leveraged to implement solid protective controls:

- Network Segmentation: **Hirschmann Eagle** and **Tofino Security** appliances enable robust network segmentation (the practice of organizing networks in smaller segments or zones), so that applications or devices can be separated.
- Device Hardening: Ensure all devices—HMI (human-machine interface), engineering workstations, switches, routers, etc.—are configured to industry best practices and frameworks, such as IEC 62443 or NIST SP 800-82.

Step Three: **Continuous Monitoring**

Once a foundation of visibility and protective controls has been established, you can begin to continuously monitor the environment to have ongoing situational awareness. This awareness allows you to keep your process operational and avoid unnecessary or unplanned downtime. **Tripwire** solutions can enhance awareness via a continuous monitoring solution:

- Understand when controller modes have been changed
- Know if a newly-installed IO block has vulnerabilities
- Monitor engineering workstations to ensure correctly configured against internal build specifications or selected cybersecurity framework

Customer Testimonials

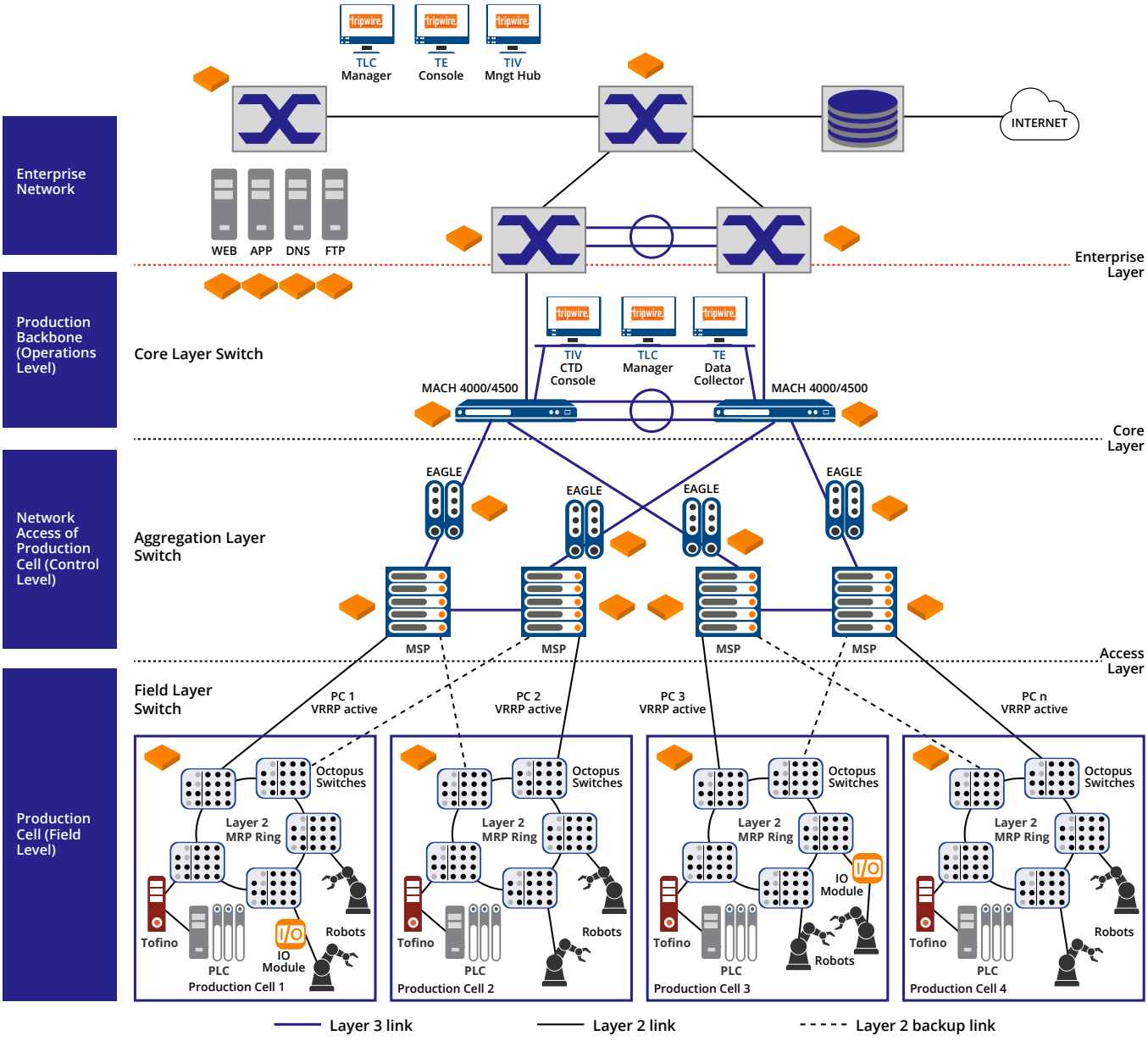
- **Global Automotive Manufacturer:** Excited to learn that Belden could auto-discover all assets on their networks by querying with their native industrial protocol (Ethernet/IP) and provide vulnerability information related to those assets.
- **Food and Beverage Manufacturer:** Loved visibility and context around log management solution from Tripwire that allowed diagnosis of impending cable failure: the connected switch was sending out a vast number of CRC errors detected through syslog to our solution.
- **Consumer Product Goods Manufacturer:** Saved hundreds of man-hours evaluating device configuration against IEC 62443 by using Tripwire solutions, which automated the collection and assessment of device configurations.

BELDEN
SENDING ALL THE RIGHT SIGNALS

Discrete Network Reference Architecture Example

In this example of a discrete reference architecture, Belden's solutions can:

- Provide complete asset inventory and industrial protocol communication
- Identify vulnerabilities to all assets
- Identify changes to controllers – configuration, mode and firmware
- Measure the configuration for HMI, SCADA, engineering workstations and network infrastructure to IEC 62443
- Provide visibility to all log information from controllers, SCADA, HMI, engineering works and network infrastructure
- Provide network segmentation between plant and corporate IT, inter-zone/cell communication and enforce all industrial protocol communication to controllers



TLC = Tripwire Log Center | TE = Tripwire Enterprise | TIV = Tripwire Industrial Visibility
Industrial visibility, protective controls and monitoring enabled through active and passive solutions: Tripwire Enterprise, Tripwire Log Center and Tripwire Industrial Visibility

Call your Belden or Tripwire sales representative to schedule a demonstration or visit our websites at www.belden.com and www.tripwire.com.

Belden US 1-855-400-9071 ■ Tripwire US 1-503-276-7500
Belden EMEA +49 (0)7127 14 1809 ■ Tripwire EMEA +44 (0) 16 2877 5850

CYBER-SECURITY-DISCRETE-SELLING-GUIDE_SF_INET_BDC_0319_ENG