HIRSCHMANN

A BELDEN BRAND

White Paper

WP00002

Cyber Security in Electrical Substations

Andreas Dreher
Strategic Technology Manager, Hirschmann Automation and Control, a Belden Brand
Andreas.Dreher@belden.com

Germán Fernández
Global Vertical Marketing Manager, Power Transmission and Distribution, at Belden Inc.
German.Fernandez@belden.com

Executive Summary

Many factors have led to the new range of security challenges faced by electrical substations today. The adoption of new technologies – such as transmission control protocol/internet protocol (TCP/IP)-based technologies for both substation automation networks and wide area network (WAN) communications between substations – has opened these networks up to more cyber threats. A good cyber security policy, however, is a simple first step to maintaining the reliability and the safety of substation and grid operations.

Cyber security is often used to describe protection against online attacks, but a more holistic view of cyber security involves a collection of measures adopted to prevent unauthorized use, malicious use, denial of use, or modification of information, facts, data or resources. Cyber security not only refers to intentional attacks from outside the network, but also internal issues and unintentional modifications of information.

With both internal and external threat sources in mind, it is important to establish preventative processes for any issue that could lead to network downtime. These measures could include devices, configurations, internal security policies, and employee and contractor training. And since it's not realistic to assume all threats can be prevented 100 percent of the time, recovery strategies after issues occur are also critical to protect network uptime.

Table of Contents

Gas-insulated switchgear (GIS) and bay control units in a substation.

Be certain.
Belden.

HIRSCHMANN
A BELDEN BRAND

Cyber security is about making a facility more reliable and reducing network downtime to improve productivity. It's not about hackers or terrorists – they only account for 10 percent of known incidents.

Cyber Security in Utility Communication Networks

Historically, substation control networks were based on local connections and proprietary applications. Systems were designed for safety, reliability and ease of use, and security was not traditionally a concern of network managers or installers. But this approach is no longer valid.

Today's communications networks are characterized by the use of:

- Commercial off-the-shelf technology
- Ethernet and TCP/IP-based communications protocols
- Open standards, IEC60870-5-104 and IEC61850
- Integration of legacy industrial protocols (DNP3) and Modbus TCP
- Remote connections (multiple devices and mobility)
- Interconnection with company IT systems
- Use of public networks

The complexity of power grids has increased over the years. As they have become interconnected with systems across countries, it has made failures and mistakes more likely – and their potential impact greater in scope and cost.

A thoughtful cyber security policy, combined with a well-designed network infrastructure, can help minimize or contain threats. Cyber security policies strive to meet three main objectives:

- **Confidentiality:** Preventing unauthorized access to information
- **Integrity:** Preventing unauthorized modification or theft of information
- **Availability**: Preventing denial of service (DoS) and ensuring authorized access to information

In IT networks, confidentiality is the main objective. However, in industrial networks, availability is the critical design parameter[1].

Analysis of Threats

Most network security incidents are accidental instead of intentional. According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) vulnerability analysis[2], authentication flaws were the most abundant vulnerability type identified in 2013. This liability is of particular concern because an attacker with a minimal skill level could potentially gain administrator level access to devices that are accessible over the Internet. Other common vulnerabilities identified in the analysis include factory hard-coded credentials and weak authentication keys.

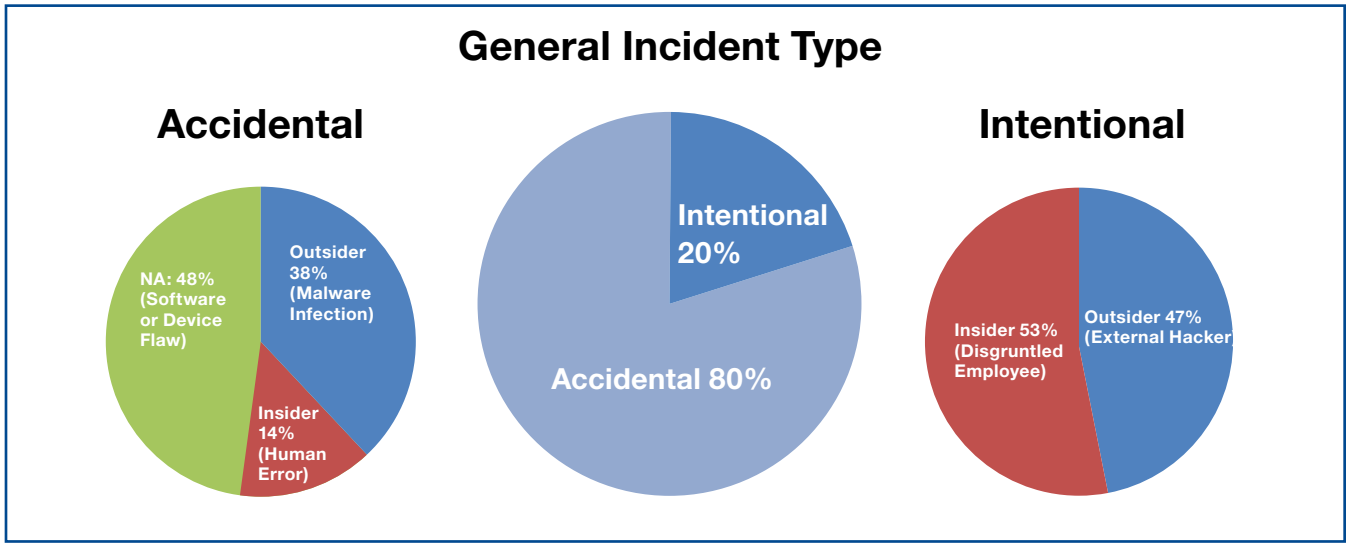


Figure 1: The majority of network security incidents are unintended. Source: The Repository of Industrial Security Incidents, 2011.

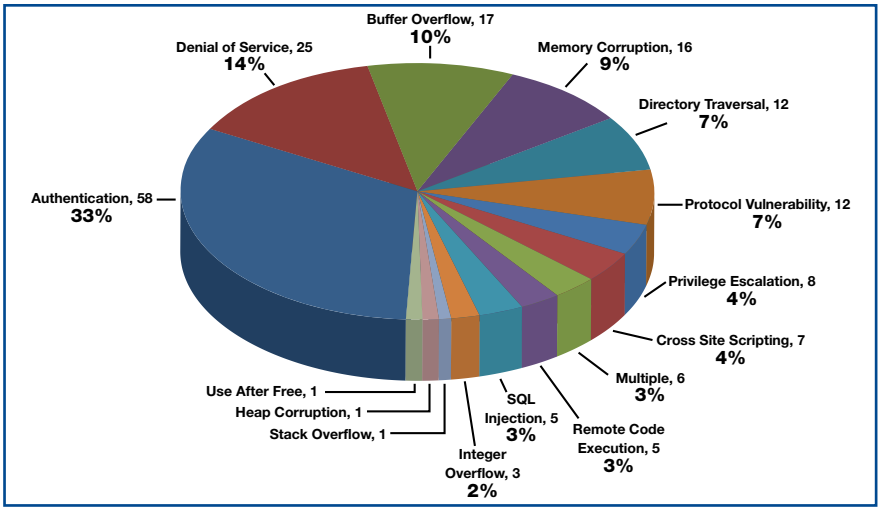


Figure 2: Breakdown of industrial control system vulnerability types. Source: ICS-CERT Vulnerability Analysis, per text use 2013.

Unintentional threats, such as equipment failures and employee carelessness, and deliberate threats, like cyber hackers and viruses, have different types of consequences. They impact information systems, network infrastructure management and power system assets differently. Due to the critical role the communications network plays in the operation and protection of the high voltage and medium voltage grids, a DoS attack may lead to service disruption and financial losses, as a result of repairs and equipment replacement.

Five Levels of Security

Cyber security is an iterative process – not static. As surrounding conditions or threat sources change, systems and policies may need to be updated to address those changes.

To understand this process, it's important to differentiate between risks, vulnerabilities and threats. While a risk is the likelihood that something bad will happen that causes harm to an information asset (or the loss of the asset), a vulnerability is a weakness that could be used to endanger or cause harm to an information asset. A threat is anything (manmade or an act of nature) that has the potential to cause harm[3].

Belden defines five levels of security, which include:

1. **Preventive security** controls are intended to prevent an incident from occurring, reducing the number and type of risks and vulnerabilities. Best practices include preventing external USB drives to access open ports and strong password policies.
2. **Network design security** minimizes the vulnerabilities and isolates them so if an attack occurs it will not affect other parts of the network. This can be achieved by limiting the number of connections between network zones through a zones and conduits method[4].
3. **Active security** takes place both before and during an event. Active measures and devices will block traffic or operations that are not allowed or expected in a network. Best practices include encryption, protocol-specific deep packet inspection[5], Layer 3 firewalls and antivirus use.
4. **Detective security** controls identify and characterize an incident in progress or after it occurs by evaluating activity registers and logs. This can include log-file analysis and intrusion detection system monitoring.
5. **Corrective security** controls aim to limit the extent of any damage caused by an incident. It is necessary to build in protocols for retrofitting preventive security and the network design security measures once a vulnerability is detected. These security measures include a configuration parameter backup policy, as well as firewall and antivirus updates.

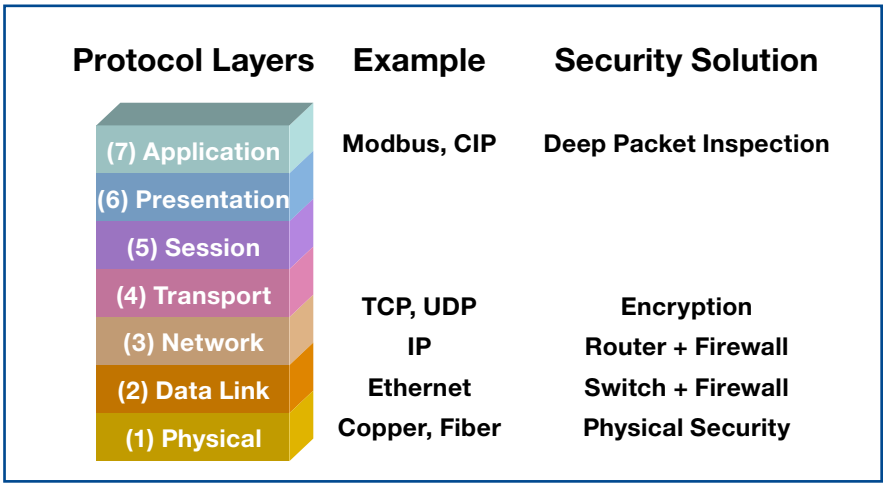


Figure 3: Seven layers of the open systems interconnection (OSI) model.

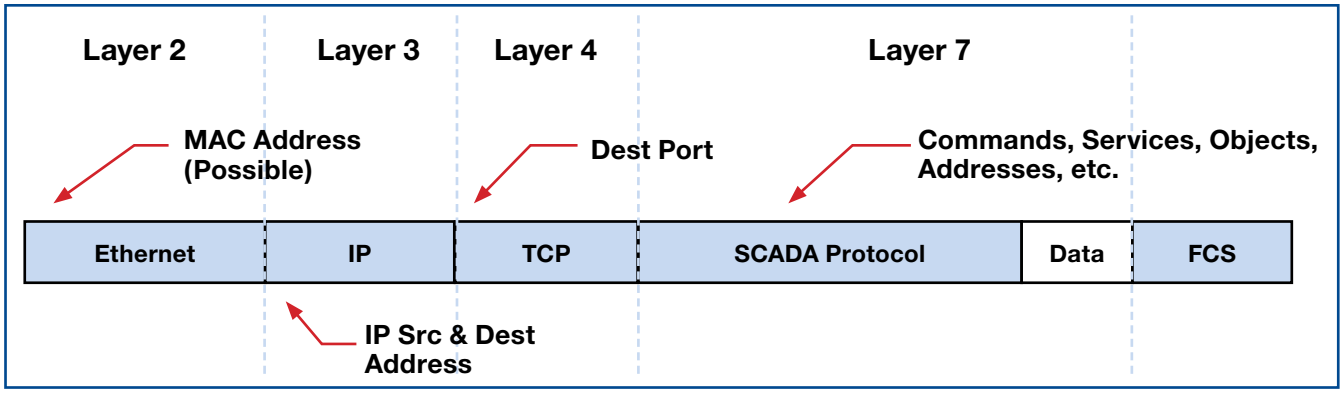


Figure 4: Security devices can inspect the different fields in the Ethernet frame – from the Layer 2 header fields to the Layer 7 payload.

"Cyber security will be the difference in future-proofing networks. Our customers are conscious of the risks they can avoid by having a comprehensive security policy. Our application engineers are experts in designing networks to meet the highest security standards."

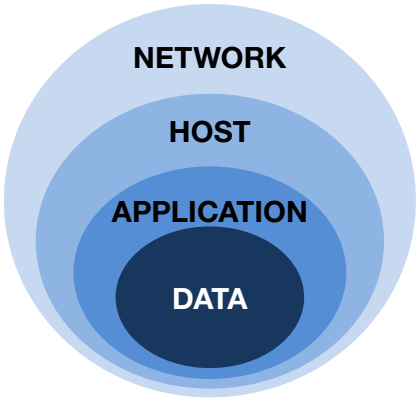
– Carlos Prada,
Belden Competence Center Director

How to Implement Cyber Security in a Substation

Single point of defense security solutions are a thing of the past. The electrical grid – including its substations and feeders – is an increasingly easy target for hackers and, given its critical importance, any internal errors that bring down the network would be detrimental as well.

A carefully constructed and strategically designed security strategy, such as following the Defense in Depth model[6], is the practical solution. Defense in Depth involves using multiple, overlapping layers of protection to secure critical infrastructure. This can include looking at policies and procedures, as well as physical, network, computer and device security.

Defense in Depth is built on three core concepts:



Defense in Depth: when one layer of security is breached, the next layer defends the system

1. **Multiple layers of defense.** Layering multiple security solutions so that if one is bypassed, another layer will provide the defense. Systems cannot rely completely on a single point of security, no matter how good it is.
2. **Differentiated layers of defense.** Sound security strategy, whether military, physical or cyber security, makes sure that each of the security layers is slightly different. If an attacker finds a way past the first layer, they don't automatically have the capabilities for getting past all the subsequent defenses.
3. **Threat-specific layers of defense.** Each of the defenses should be designed to be context and threat specific. In essence, design for the threat. The electric power system can be exposed to a variety of different security threats, ranging from computer malware and angry employees, to DoS attacks and information theft. Each needs to be considered and defended against. For example, in the substation, sophisticated supervisory control and data acquisition (SCADA) aware firewalls are now available that can observe the network traffic right down to specific types of commands. This allows defenses based on the behavior and context of the systems using these protocols.

The industry needs to accept the idea that complete prevention of all attacks or issues isn't possible. The best way to manage hostile

entities or internal errors is to quickly detect, isolate and control them, and ultimately limit impact on other areas of the network.

A few security measures that utility operators can implement include:

- **Prioritize.** Make sure your mission-critical systems are secure first.
- **Create a culture of security.** Keep teams informed and educated on security best practices.
- **Update your existing risk assessments regularly,** including both physical and virtual checks.
- **Do not apply a one-size-fits-all solution** across the entire IT and SCADA system. The threats, risks and goals of these systems are different, so the solutions should be as well.

Physical and cyber security can be used together to create more robust layering. For example, layers of physical security can include card readers installed on control room doors and transformer cabinets; and security cameras that monitor substation access and guard important areas against unauthorized infiltration, copper theft and other attacks. If these are matched with layers of network security to create a coordinated monitoring system, then both cyber and physical security can benefit.

In a typical substation network, a systematic approach for cyber security procedures includes the following elements:

- Installing routers and firewalls between the corporate backbone and the substation network.
- Implementing stateful inspection, or Deep Packet Inspection (DPI)[7], to ensure that only authorized packets travel between both networks. Tunneling, router redundancy and encryption are valid features to secure access to the substation.
- Segmenting between the operational network and telecom network, by creating demilitarized zones (DMZs) for servers and computers in the operational network with external access. Security zones can be defined by physical location or common functions.

Several standards, such as North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), Institute of Electrical and Electronics Engineers (IEEE)'s 1686[8] and the International Electrotechnical Commission (IEC)'s 62351[9], are working to address cyber security for substation control systems. Each covers or focuses on different areas and parts of the overall system, but some gaps still remain.

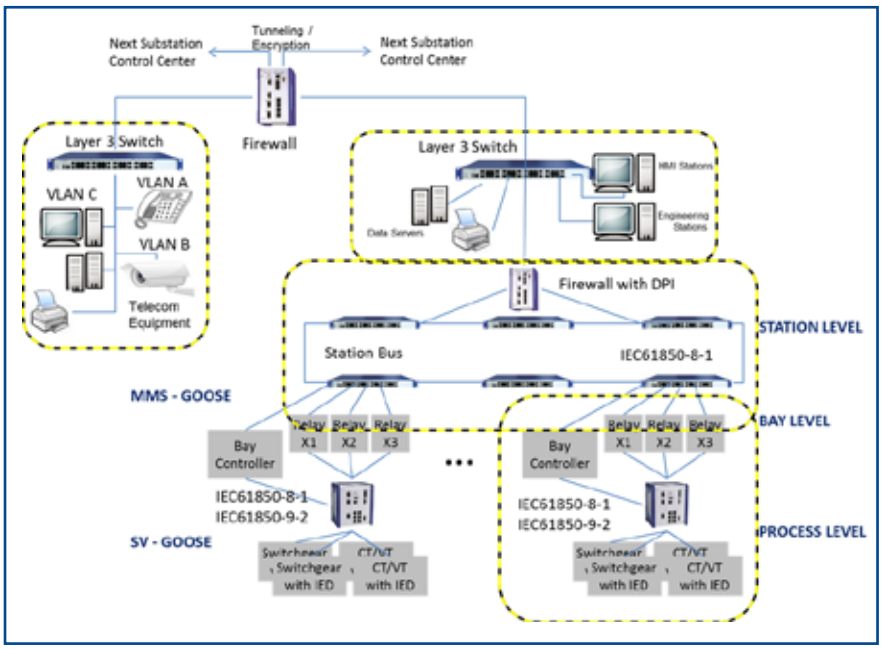


Figure 5: Establish security zones to limit access points to different areas of the industrial network.

True Security Requires Vigilance

Precise knowledge of the network topology, protocols and type of traffic is absolutely essential for a reliable design of security policies and countermeasures. The network administrator must know how and where components are connected in order to allow the necessary conduits and establish the security zones.

Even electrical substation networks evolve over time, and documentation can easily become outdated. A good set of preventive countermeasures will force any new device connected to the network to be validated by an administrator and trigger a documentation process review.

Throughout a network's operational lifetime, it is necessary to carry out repetitive, but essential, maintenance tasks. For example, the threat of cyber attacks means that responsible network administrators should change device passwords regularly, implement upgrades to fix bugs and maintain regular antivirus updates. An active Corrective Security plan is also needed to maintain the robustness of a network.

Conclusion

Substation cyber security requires vigilance against both accidental and intentional threats. An entire network can be protected by segmenting the network into smaller virtual local areas networks (VLANs) with limited access points[10].

Following a Defense in Depth model allows for building in multiple layers of security protocols, so any system failure or breach results in limited damage, which can be controlled or managed more efficiently. Meanwhile, the large portion of the system remains protected and up-and-running.

Rely on Belden's experience and expertise in designing and implementing complete and secure network architecture.

HIRSCHMANN
A BELDEN BRAND

The Belden Solution

Belden can assist customers by helping to choose the network architecture, security policies and best devices for each type of protection and for specific applications. Belden experts remain aware of the latest trends in substation automation networks by constantly reviewing customer applications.

By sharing other customers' experience and the best practices in the industry, Belden brings invaluable worth to any project.

The Belden portfolio of active network components is designed to meet the most demanding cyber security standards. Belden participates in many standardization bodies, including IEC, ISA and IEEE.

Protection and control level in a digital substation. Ethernet switches are inside the cabinets and allow communication among the different intelligent electronic devices (IEDs) in the station bus.

Protection and control cabinet with Hirschmann switch.

In North America, Belden offers assistance through a free Industrial Ethernet Infrastructure Design Check-Up that includes security. This process evaluates networks based on best practices. To arrange a Design Check-Up, call 1-855-400-9071 or email inetsalesops@belden.com.

In Europe and other parts of the world, the Belden Competence Center is a facility where network design engineers work with customers' technical teams to design the most cost-effective solution for high-performance networks, including aspects, such as cyber security, wireless and network design best practices. To learn more about this service, visit http://www.beldensolutions.com/en/Contact/index.phtml.

Belden Product Range

As a specialist in automation and networking technology, Belden and its Hirschmann brand develop innovative solutions that are tailored to its customers' requirements in terms of performance, efficiency and investment reliability.

Together, Belden and Hirschmann not only offer a complete range of products for company-wide data networks, but also a broad support package direct from the product manufacturer. Customers receive support while their tailor-made communications solutions are being designed, and also throughout the subsequent planning, process, commissioning and maintenance of their networks.

Comprehensive seminars and workshop offerings, in which trends are evaluated and technical subjects are put into practice, complete the vast range of available services.

Product Details

TOFINO Xeno

Thanks to its conformance with numerous approvals, Tofino Xenon offers maximum flexibility in its protection of industrial plants, oil rigs, substations and transportation systems.

Benefits at a glance:

- Stateful firewall with Layer 2, 3 and 4 filtering for all Ethernet-based protocols
- Additional application layer filtering for SCADA and ICS protocols using flexible loadable security modules (LSMs)
- Prevention of DoS attacks with rate limit controls
- Simple configuration over the network or with ACA21-USB using the Tofino Configurator software
- Simultaneous event logging to remote syslog servers and local nonvolatile memory
- Audit capabilities for tracking configuration changes

EAGLE One

Industrial firewall and security router with extensive Layer 2 and Layer 3 redundancy features.

Benefits at a glance:

- Redundant backbone connections for production cells
- Firewall Learning Mode for easy and smooth commissioning
- Router redundancy plus stateful firewall and 1:1 NAT in Layer 3 mode
- Text-based configuration file for automated pre-configuration
- Transparent Layer 2 bridge or routing operation mode
- Wide range of transmission and encryption standards (PPPoE, PPP, IKEv1/v2, IPsec, NAT)
- A variety of security mechanisms (stateful packet inspection firewall, VPN)
- Digital input for controlling VPN connections

Hirschmann Operating System (HiOS) Software

HiOS software provides maximum network availability and data security for efficient production processes.

Benefits at a glance:

- Supports various security mechanisms, comprehensive management and diagnostic methods, precise time synchronization, and redundancy protocols
- Works with switches in the Rail Switch Power (RSP), RSP-Expandable, RSP-Lite, RSP-Smart, and Embedded Ethernet Switch (EES) families, as well as the modular MICE Switch Power (MSP) system, to implement fail-safe networks

HIRSCHMANN
A BELDEN BRAND

DataTuff Industrial Ethernet Cables and Connectivity

Belden DataTuff encompasses a portfolio of industrial Ethernet cable and connectivity products.

Benefits at a glance:

- Industrial-grade jackets that withstand exposure to oil, chemicals, rough handling, abrasion, UV and temperature variations
- Product consistency for ease of termination and assembly
- Comprehensive range of products, including Cat 7 and Cat 5e, PVC, FRNC, TPE and PUR jackets

References

1. "SCADA Security Basics: Integrity Trumps Availability," Belden blog, November 6, 2012.
2. "ICS-CERT Vulnerability Analysis," 2013.
3. "7 Steps to ICS and SCADA Security," Belden white paper, February 16, 2012.
4. "Improving Control System Security with ANSI/ISA-99 Standards," Belden blog, May 17, 2012.
5. "Understanding Deep Packet Inspection for SCADA Security," Belden technical briefing kit, 2014.
6. "Defense in Depth Cyber Security for Substation Communications," Belden blog, February 4, 2015.
7. "Why SCADA Firewalls Need to be Stateful," Belden blog, April 11, 2012.
8. "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities," IEEE webpage.
9. "Core IEC Standards," IEC webpage.
10. "Substation Communications Design Legacy to IEC 61850 Best Practices," Belden white paper, 2014.

Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge play a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world's first certification program for industrial networks. Up-to-date manufacturer's expertise, an international service network and access to external specialists guarantee you the best possible support for products from Belden, GarrettCom, Hirschmann, Lumberg Automation and Tofino Security. Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.