Whitepaper

The Best Approach to Zones and Conduits: IT Cybersecurity Lessons for Industrial Applications

While modern industrial enterprises work hard to prioritize security, the game has recently grown tougher. Industrial equipment and PLCs are now more frequent targets of cyberattacks, adding pressure and urgency to the task. At the same time, controls engineers are in the early stages of familiarizing themselves with cybersecurity risks and solutions, and how to address these quickly in the OT environment.

The good news is that as industrial automation control systems become smarter and digitized, they benefit from years of Information Technology (IT) experience in cybersecurity best practices.

The IEC 62443 standard is a consensus-based cybersecurity standard for industrial automation and control system (IACS) applications. It consolidates global IT cybersecurity best practices and translates it into security standards for industrial applications. The result is a solid roadmap for industrial enterprises and equipment owners seeking to shield data and systems from breach or damage and to strengthen their overall security posture.

The standard defines how networks and connections should be configured and secured for the entire lifecycle of industrial applications – from design through to decommissioning. It drives a crucial point home, one learned and borrowed from IT: Security is not just implemented, but needs to be continuously improved.

STRENGTH THROUGH SEGMENTATION: ZONES AND CONDUITS

In industrial automation, that means adopting a layered security approach. At the level of network connectivity, the IEC 62443 standard establishes requirements for dividing systems into segments as a key security measure to fortify industrial systems.

Consider a factory automation facility with separate assembly lines (Lines A, B, C, D), each of which encompasses several processes and multiple input/output (I/O) devices, Programmable Logic Controllers (PLCs), and Variable Frequency Drives (VFDs). Many organizations maintain flat networks with no divisions between different lines. The problem is that a device plugged in anywhere can access every other part of the system.

This ease of connectivity is a major security risk and can lead to intentional or unintentional compromise. An employee laptop infected with malware, for example, could damage the rest of the system. A hacker with malicious intent could infiltrate one network and gain easy access to the others.

A safer approach is to segment the factory floor into multiple smaller containers, called zones. Since each zone has its own network, any device plugged into that zone can only access the processes and devices in that area. Zones create a layered security boundary with process control and help maintain the same security level for all devices within that zone.

Zones aren't isolated from one another, however. Communication between devices in different zones can be enabled through conduits that control and monitor traffic in and out of individual segments.

For example, if our imaginary facility's Line A had a PLC that needed to communicate to a PLC in Line C, a conduit would be set up to connect Line A to Line B, and a second conduit would connect Line B to Line C. Those conduits would block or allow traffic. Done right, they would also provide visibility into what's happening at each boundary.

THE RISKS OF TRADITIONAL VLAN

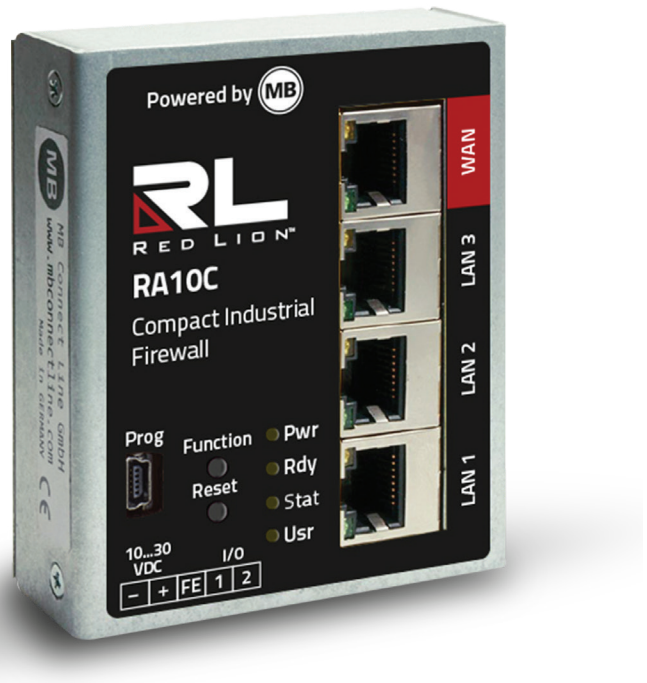
A conventional approach to zone segmentation would use VLAN technology. For that, you need to configure multiple VLAN subnets – one for each zone – each with its own unique IP address, subnet mask, and default gateway. For devices to communicate properly within and between zones, every single device in those VLAN subnets – PLCs, VFDs, and I/O devices – would need to be updated with new parameters reflecting those new IP addresses.

You'd have to set up routers for those subnets. You'd also need firewalls to block traffic ingress and egress at transport and network layers and effectively allow or disallow communication through segment boundaries.

Getting VLAN, router, and firewall technology to work effectively together can be a challenging process. Every piece adds a layer of complexity, and a single change introduced to one part of the solution requires adjustments to every other device.

When an industrial process has been running reliably for 5 to 10 years or more, any change to that process is daunting. The concern with VLAN technology is that what begins with a little downtime could end up jeopardizing the whole process.

Solving network segmentation using VLANs requires a significant time and labor investment. On top of the work involved, the number of configuration changes required introduces significant risk. IP addresses of hundreds or even thousands of devices may need updating. A simple typing error could bring operations to a halt and necessitate a lengthy troubleshooting process to identify the error and restore the system. Key Performance Indicators (KPIs) including Overall Equipment Effectiveness (OEE), productivity, and quality could decline during the ensuing shutdown.



MEETING CYBERSECURITY STANDARDS OUT-OF-THE-BOX

A better and easier method is possible with Red Lion's RA10C compact industrial firewall. You simply install the RA10C in your panel as the conduit between two zones (e.g. Line A and Line B). Rather than having a cable that runs between Lines A and B, cables from Line A and Line B both plug into the RA10C, acting as the conduit and providing the necessary segmentation between zones.

The unit provides firewall protection, along with traffic control and monitoring, and eliminates the need for VLANs and routers. In contrast to the VLAN approach, the Red Lion unit supports zone and conduits capability and preserves network communication without requiring any time-consuming and risky changes to network devices.

With the RA10C operating in Bridge Mode, users can control, visualize, and monitor network traffic with a single piece of software. No special expertise is expected in either networking or firewall functionality. A setup wizard launches during setup, asks users a few questions, and guides them through the installation process.

The RA10C comes installed with configuration software that enables the automatic creation of a host list of devices trying to communicate with the RA10C. The user only needs to know which hosts should be connected to each other and which connections should be blocked. Those decisions are easily and securely managed through a graphical user interface. Arrows indicate which communication pathways are open and closed, and users can direct, redirect, and block traffic with a few simple clicks.

Among the system controls is a Syslog that logs and stores network events on the RA10C unit. In the case of a cyber incident or attack, those network events can be collected and used to alert the IT department that something has occurred.

BRIDGING OT AND IT FOR CYBERSECURITY RESILIENCE

Given the mounting threat of cyberattack on critical infrastructure and supply chains, industrial enterprises around the world are seeking new ways to increase the resiliency and security of their Operational Technology (OT).

When safer, stricter access control is a priority, large, flat networks are no longer viable options for automated industrial applications. A zones and conduits approach to network communication meets modern standards and provides more robust security and the necessary traffic control.

Experienced controls engineers sometimes feel wet behind the ears when it comes to cybersecurity. Fortunately, industrial cybersecurity standards have their best interests in mind: high uptime and compliance. The tools that deliver those priorities best are those that support IT cybersecurity principles by design.

Adopting a layered security approach doesn't just make engineers look good. It strengthens the security posture of the organization, protects upstream and downstream partners, and enhances the security of the industrial sector overall.

To discover how Red Lion solutions can help you access, connect, and visualize your data, visit www.redlion.net.

About Red Lion

Red Lion is focused on being THE Industrial Data Company™. We empower industrial organizations around the world to unlock the value of data by developing and manufacturing innovative products and solutions to access, connect and visualize their information. Red Lion's global manufacturing and support facilities serve customers in factory automation, alternative energy, oil and gas, power and utilities, transportation, water and wastewater industry segments. We provide scalable solutions for cloud connectivity, edge intelligence and asset management, industrial Ethernet switches and industryleading panel meters and operator panels, to make it easy for companies to gain real-time data visibility that drives productivity. Red Lion is part of Spectris plc, the experts in providing insight through precision measurement.

www.redlion.net

RED LION®