Cybersecurity Guidebook for Process Control

A practical guide to what you should start, stop, and continue doing to protect your assets from cybersecurity threats.

EMERSON

Take the Next Steps with Cybersecurity Together

Over the past decades, process industry manufacturers and suppliers have accomplished incredible scientific and technological advancements in the products and services our industries provide. Process industry operations comprise critical pieces of the global economy and infrastructure, like the energy needed to power our world, vital therapies and medications for patients in need, and agricultural products for food-insecure nations. As the demands of our industries have become more sophisticated, so has the complexity of operations–necessitating that legacy self-contained control systems are now connected to business networks and therefore, however indirectly, to the internet.

By leveraging the connectivity of the broader business network, manufacturers have revolutionized interconnected processes, but also encountered new risks to the safety, profitability and reliability of plant operations. Cybersecurity needs to be in every operational conversation not just today, but every day going forward.

An important factor in implementing a cybersecurity program is change management. Emerson's cybersecurity leaders for the DeltaV™ distributed control and safety instrumented systems have compiled this brief guide based on the Start-Stop-Continue Change Management model to help you lead organizational change and take immediate steps to make your operations more secure. Every organization is at a different point in the cybersecurity journey. While not all points will reflect where you are in your journey, take this guide as a reminder to continue that evolution to a cybersecurity-aware organization.

The IEC 62443 family of cybersecurity standards

The IEC 62443 is a family of standards that defines requirements for how a distributed control system (DCS) should be developed, deployed, and maintained to dramatically enhance the cybersecurity of the installed system. Cybersecurity is as important in today's climate as safety. And, in many ways, this standard is similar to what is currently required for Safety Instrumented Systems for safety certification.

Following the requirements defined in the IEC 62443 standards, Emerson has trained its DeltaV developers to create new secure products. We continue to harden the individual components of the automation system and have created system-wide capabilities, both internally and with partners, to better secure the automation system as a whole.

In addition to protection that is integral with the system, it is imperative the end user has an active role to ensure security best practices are enforced in the DCS deployment at their site. This can be accomplished through, among other things, work processes, behaviors, lifecycle management, and training. The combination of all the above will result in a state-of-the-art cybersecure installation.

Adopt a Risk-based Approach to Cybersecurity

Organizations regularly evaluate the risks to their business and operations. Cybersecurity is an organizational risk that affects strategic, compliance, operational, financial and reputational risks. A risk-based approach to cybersecurity is not to protect against all threats to your control system, but to identify potential vulnerabilities and make a strategic decision based on the likelihood and impact of each vulnerability.

- **START** Quantifying the extent of cyber risk. It pays to know where things could go wrong. While you can't identify every eventuality, you can easily identify where the particularly vulnerable points exist. By becoming knowledgeable about the types of events, understanding the likelihood those events will happen, and the impact of those events, you can make more economical decisions on how to protect your control system, your business, and your people.
- **STOP** Attacks before they start. Cybersecurity is not just about making sure that bad things don't happen; it's about ensuring your control system works as it should, 24 hours a day, 365 days a year. By employing physical, software-based, and administrative controls you can better ensure your system's availability, integrity, and confidentiality. View cybersecurity as an opportunity to ensure that you keep your operations running smoothly, without costly, unintended shutdowns.
- **CONTINUE** Using your current risk management process as you do for other aspects of your operations, like safety. Work within your organization and with experts to examine your networks and control system setup to identify risk areas. Generally, some of the easiest changes can go a long way toward making your system more secure and reducing your organizational risk.

Having a backup and recovery solution with onsite and offsite storage of the backup will reduce risk to your control system. Remember to regularly update your OT team's cyber incident response plan. While not preventative, these plans help get operations back up and running faster.

Tighten System Access

Security measures can be cumbersome and may make limited security tempting, but attackers are counting on it. In many cases, massive shutdowns are caused by small malware infections on unsupported operating systems. Companies must be conscientious about their security policies to ensure they are raising strong cyber barriers.

- **START** Simplifying and strengthening user access to critical systems. Consider deploying multi-factor authentication for user logons. Two-factor authentication systems can often be simpler for users than a complex single password, and are far more secure. Also, longer, easier to remember passwords (e.g. a group of short words or a passphrase) can be superior to shorter, more complex passwords since users will find them easier to type, remember, and not write down.
- **STOP** Opportunities for intrusion. Limit single sign-on and group logons wherever possible. If single sign-on is a requirement in your industry, look for methods to implement it so that the bare minimum is exposed. Finding ways to eliminate shared accounts and elevated user access can mean sacrificing some flexibility, but these changes are worthwhile; shared accounts are prone to password theft - a more serious risk than many organizations anticipate.
- **CONTINUE** Evaluating and monitoring privileged permissions. Remain vigilant and periodically evaluate the level of user-access granted to highly privileged users. Ensure they only have access to the minimum permissions they need to complete their job. It might be effective to enforce two-person rules for highly sensitive operations or decisions as well.

Today's convenience shouldn't become tomorrow's crisis. Building a culture of security by creating and enforcing security best practices will help your employees realize they are a crucial part of keeping your operations safe and secure.

Establish Strong Policies

Even the most sophisticated, secure measures can be rendered useless in the face of simple, human error or lack of knowledge. Many devastating attacks are achieved through social engineering and phishing that enable corporate and control system networks to be infected. This is preventable with knowledgeable employees and strong administrative policies.

- **START** Making it a point to arm your employees with knowledge. Education and training will help your employees understand the basics of cybersecurity, identify potential threats, and realize when they are being targeted. Emphasizing and enforcing strong password creation and management are critical to keeping your networks safe, as is following authentication policies for customers and employees.
- **STOP** Peripheral-based exploits. USB ports left enabled create the possibility for human error when an unsuspecting employee plugs in a phone to charge or attaches a compromised thumb drive picked up from a vendor event. By disabling these ports and establishing and enforcing organizational policies, you can help limit your exposure.
- **CONTINUE** Maintaining vigilance on physical security by locking down control system workstations and servers within dedicated rooms and cabinets. Companies must stay on top of maintaining their physical security systems. Access management controls help protect assets from unauthorized direct access.

Defense wins championships. By establishing and enforcing these administrative policies, you can prevent your control system from falling victim to unauthorized physical access or exposure to compromised media devices.

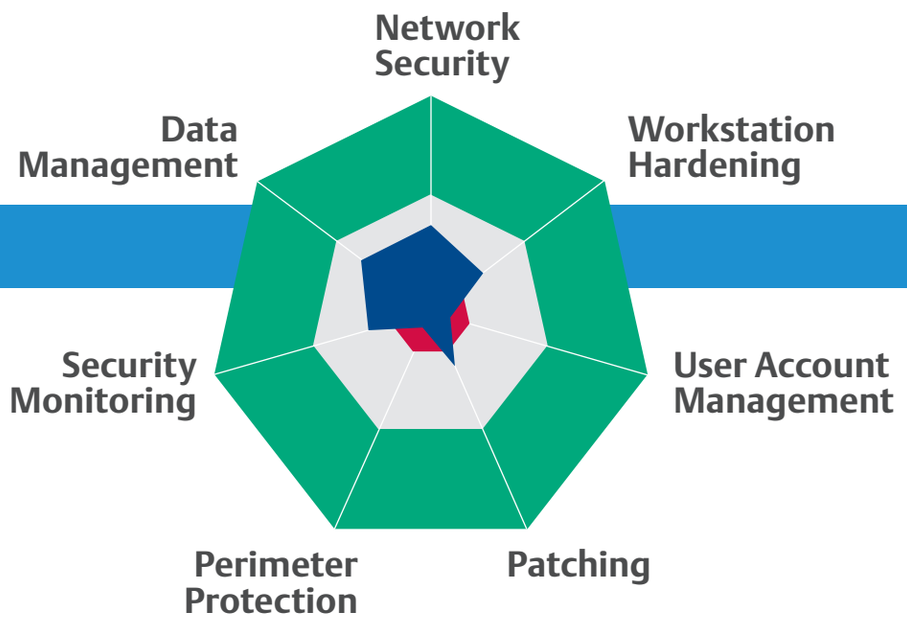
Protect yourself: Building the Right Cybersecurity Coverage

Start with an Assessment

Making your plant and control system cybersecure is an evolution and one that can be overwhelming. By conducting a plant risk assessment and leveraging that assessment, you can prioritize your cybersecurity implementation to strategically mitigate many risks upfront.

An assessment determines the readiness in each of seven key elements of cybersecurity, as shown by a radar plot. The closer the blue plot areas are to the outside edges the better the results of the assessment and the strength of a system's overall security posture.

Basic Cybersecurity Assessment Results



Improve Your Cybersecurity Posture

Adopt a Risk-based Approach to Cybersecurity

- Risk assessments
- Backup and recovery
- Incident response plan

Tighten System Access

- Two-factor authentication
- User accounts management

Establish Strong Policies

- Training
- Cybersecurity posture
- Physical security
- Policies and procedures

Upgrade to a More Secure Control System

- Request cybersecurity solutions
- Patch management
- Workstation hardening
- Endpoint protection

Go Beyond Perimeter Protection

- Network segmentation
- Perimeter protection monitoring
- Network firewall with IPD

Keep Remote Access in the Right Hands

- Remote access management

Know Your Control System

- SIEM
- Network security monitoring

Upgrade to a More Secure Control System

We all know that downtime is costly, and we must make hard decisions to avoid it as much as possible. Timely patches and upgrades are a critical element of cyber defense. Recent malware and ransomware attacks around the globe have proven just how costly unprotected and outdated systems can be. Protecting your control system can help avoid putting your operations at risk.

- **START** Requesting that vendors provide cybersecurity solutions as part of the bid specification for the control system. All modern control systems require cybersecurity measures beyond the basic process control system "Request to Quote" language. Have an assessment of your current cybersecurity practices and control system and learn how you can greatly improve your cybersecurity posture.
- **STOP** Latent software vulnerabilities. Upgrading old control systems builds strong cyber barriers. Unsupported operating systems and older control systems may have inherent security vulnerabilities that have been designed out of modern automation systems. Demand that new system releases have cyber hardening features to provide additional defense-in-depth.
- **CONTINUE** Applying patches, system updates, and new anti-virus signature files. While patching can be disruptive, it is a critical aspect of your operation and ensures that your control system is operating with the latest software updates. Those updates and patches include fixes and shore up vulnerable areas of the applications and operating system. Anti-virus is another critical aspect of protection that must be maintained so it can identify the latest system threats.

Most cybersecurity threats are avoidable. Look to the many options for automated patching and lifecycle cybersecurity services to eliminate the risk of having unprotected servers and workstations.

Go Beyond Perimeter Protection

Workstations and servers are potential entry points to the control system, especially if they are connected to the corporate business network. Targeted attacks assume that perimeter protection is in place and therefore use common protocols and known service ports to compromise control system components. How you connect your control systems to the corporate network matters.

- **START** Using firewalls and network segmentation. A controller firewall further segments and protects your most critical control assets from Denial of Service attacks (among other things). Define clear security zones and DMZs. Start holding contractors and suppliers to the same security standards you expect from your own employees. Enforce your methodology for any connections to your internal systems.
- **STOP** Hackers scanning for security gaps. Ensure firewall bypasses are opened only long enough for active testing and then immediately closed. Avoid providing direct Internet and email access on control system workstations and servers; all data coming from or going to the Internet should be made available through segmented networks with intermediate servers in demilitarized networks, and should be monitored at all times.
- **CONTINUE** Deploying customizable, adaptable firewalls at the control system perimeter. Check firewall event logs and adjust rules accordingly. Continue defining and hardening network segmentation to protect and limit access to the very highest layers—particularly the control system. Constantly define and enforce security procedures for data flow at every network layer.

Hackers count on organizations forgetting the backdoors they've left open. Using the tools at your disposal, you can shut those doors and lock them tight, leaving hackers out in the cold.

Keep Remote Access in the Right Hands

Almost all control systems are deployed with some type of remote connectivity. But just because something is the norm, doesn't mean it is a safe practice. Poorly controlled remote access is like leaving the keys in the lock of your front door. On systems where remote access is a must, make sure it is monitored and secure.

- **START** Considering a dedicated remote access strategy incorporating mobile devices. Remote access should start with view-only permissions, and any commands that are required should be provided temporarily and only by exception in strategic instances. Write access (if needed) should only be allowed temporarily, and only under supervision of a local user. A remote engineer might be allowed to change the configuration, but it should require a local engineer to download and apply the change to the system.
- **STOP** Easy remote access by intruders. When users require remote access to control systems, you can improve security by detailing policies and procedures for each deployment. Control system administrative permission or safety-related user access should never be allowed through a remote connection. Strong remote access policies provide significantly more protection than air-gapping.
- **CONTINUE** Evaluating which users have the rights to remotely access your control system. Very few, if any, users should have permissions to log on remotely, and different accounts should be created for the same user—one for local highly privileged access and another for restricted remote access.

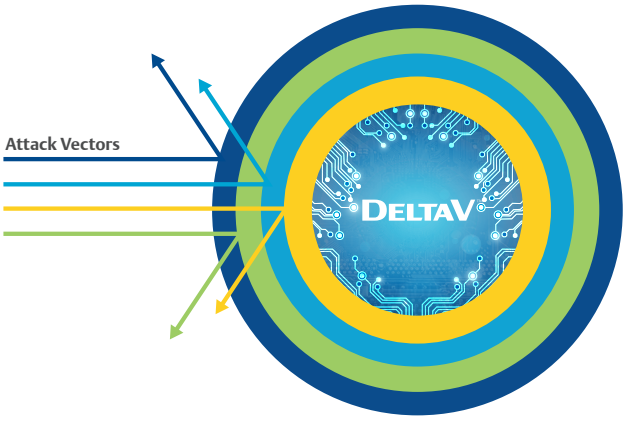
Knowing exactly when and how any mobile devices connect to your control system will put you in control. Remote access needs to be implemented securely, always requiring it to pass across the control system perimeter protection and jump servers traversing multiple layers of authentication for added security.

Know Your Control System

You have adopted a risk-based approach to cybersecurity, so you have a plan to prevent and deal with cyber incidents when they happen. But how will you know when to put those plans into action? By implementing comprehensive system monitoring, you will be able to identify threats or issues in their earliest stages as well as leverage that information for forensic purposes after an event.

- **START** Implementing security monitoring. Active, continuous monitoring is crucial for understanding your control system's baseline activity so you can identify anomalous events when they occur. Start with a Security Information and Event Monitoring (SIEM) solution that monitors syslog events from your firewalls, Windows events from your workstations, and SNMP monitoring of your switches. A SIEM is critical for intrusion detection, post-event forensics, and future threat prevention. Use the tools at your disposal to detect cyber-attacks as they start – before they can damage your control systems.
- **STOP** Previously undetected intrusions. You need to be able to detect and respond to threats as quickly as possible, and that means having the right tools, staff, and procedures at your disposal. Tactical defense information is available in security events and log data. Analyze it to identify unwanted activity. Despite some claims, security devices are not "set-and-forget". Intrusions go undiscovered if you are not monitoring – vigilance is essential to maintaining security.
- **CONTINUE** Gradually improving monitoring, response, and forensic strategies. Move toward more advanced Network Security Monitoring of your control system's network communications. If you already know what normal, expected activity looks like, then it is easier to know when something unexpected or malicious is happening.

After a breach, you need to react quickly and efficiently. To do that, it is critical to identify events as soon as possible. While events are not always malicious attacks, you want to prevent any abnormal activity that could result in downtime, accidents, or worse.



PLANT SECURITY
- Policies
- Procedures
- Training
- Physical Security

SERVICES AND SUPPORT
- Cybersecurity Assessments
- Automated Patch Management
- Upgrades
- Guardian Support

FEATURES AND SETUP
- System Hardening
- DeltaV Security Administration
- Network Device Command Center
- DeltaV Flex Lock
- DeltaV User Manager
- DeltaV and DeltaV SIS Lock Commands
- Authenticode File Signing

SECURITY PRODUCTS
- Endpoint Security
- Application Whitelisting
- SIEM
- Network Monitoring
- Emerson Smart Firewall
- DeltaV Firewall-IPD
- DeltaV Smart Switches
- Backup and Recovery

The Time for Cybersecurity is Now.

Cybersecurity threats are more prevalent than ever. Has your organization taken the necessary steps to ensure it is protected from the next malware or ransomware attack? Emerson has a comprehensive portfolio of cybersecurity solutions and strategies aimed at helping you assess and reduce your risk level. Begin building the foundation for a cybersecure future today.

Take the next step. Learn more at www.emerson.com/cybersecurity

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/deltavcybersecurity

DeltaV™

EMERSON™