Mitigating Cybersecurity Threats to Industrial Control Systems

This page is intentionally left blank.

Introduction

A modern plant cannot operate safely and efficiently without fully functional process automation systems and, in some cases, cannot operate at all. Therefore, it is vital to ensure the integrity of all automation systems and to protect them from malicious attacks, accidental corruption, and data breaches that may jeopardize safety or production or may compromise the end user's competitive advantage in the marketplace.

This paper describes the philosophy and best practices for keeping your process automation systems secure from cyberattacks.

Control systems have come a long way from the days of panel boards and pneumatic instrumentation. Most customers work with the latest computer technology on a daily basis through their personal electronic devices and expect similar features and capabilities from their Industrial Automation and Control Systems (IACS).

Modern automation systems are like the central nervous system of a plant. They provide for process and personnel safety using sophisticated safety systems, interlocks, and alarm systems. They provide for efficient plant operation through high performance Human Machine Interfaces, recipe and batch management, and equipment control. Furthermore, typical automation and manufacturing execution systems store vast amounts of proprietary information such as product recipes, process steps, graphics, historical data, alarm history, design documents, help documentation, etc.

Risk Analysis

Although most end users consider their actual automation platforms secure, well-publicized attacks on personal, business, and industrial control systems should serve as a warning for all computer system managers. Each control system should be evaluated for possible risks from external and internal sources and measures introduced to counteract those risks as part of a comprehensive cybersecurity risk management program. Whether accidental or intentional, human interaction by operators, managers, engineers, technicians, IT staff members, contractors, and other outside parties has the potential to cause significant damage to automation system operation and data integrity. *

To identify potential vulnerabilities, perform an industrial automation and control system cybersecurity risk analysis, similar to a Process Safety Management (PSM) analysis. This study should list all possible threats, quantify their impact, and identify risk mitigation actions for each threat. This risk analysis should be conducted and updated periodically. Risk analysis tools such as the ICS-CERT Cyber Security Evaluation Tool (CSET) can help with performing a comprehensive industrial control and IT risk analysis. A sample Security Maintenance Checklist included later in this document provides suggestions for the scope of the analysis.

Physical Security

The most obvious method of protecting critical computer resources is to physically secure the equipment. The plant may already have a method of limiting physical access but, once someone is in the plant, can they access data, computers, network gear, controllers, or I/O? Each physical component of the process automation system should be in a locked cabinet or placed in a limited access area and provided backup power. This includes, but is not limited to, all process automation system network components, process controllers, servers, and operator consoles. New generations of I/O communicate directly through gateways to the process automation system. Users should perform an audit to ensure that these gateways are physically secured as well. In addition to limiting physical access control system equipment, limiting or eliminating any other means of introducing external software to your systems and networks should be completed, such as disabling or limiting network switch ports and removing or disabling USB and CD/DVD devices.

The system administrators and their backups should keep a list of all personnel with key access to these areas and cabinets to control and manage key distribution. Periodic checks of the system components' physical security should be part of an overall control system cybersecurity maintenance program.

Network Design and System Configuration

Even after physical access to the equipment is properly restricted, it is usually still possible to access the process automation system from other company business (IT) systems or even from the Internet. The networks that connect the process automation systems to external systems should be analyzed for vulnerabilities.

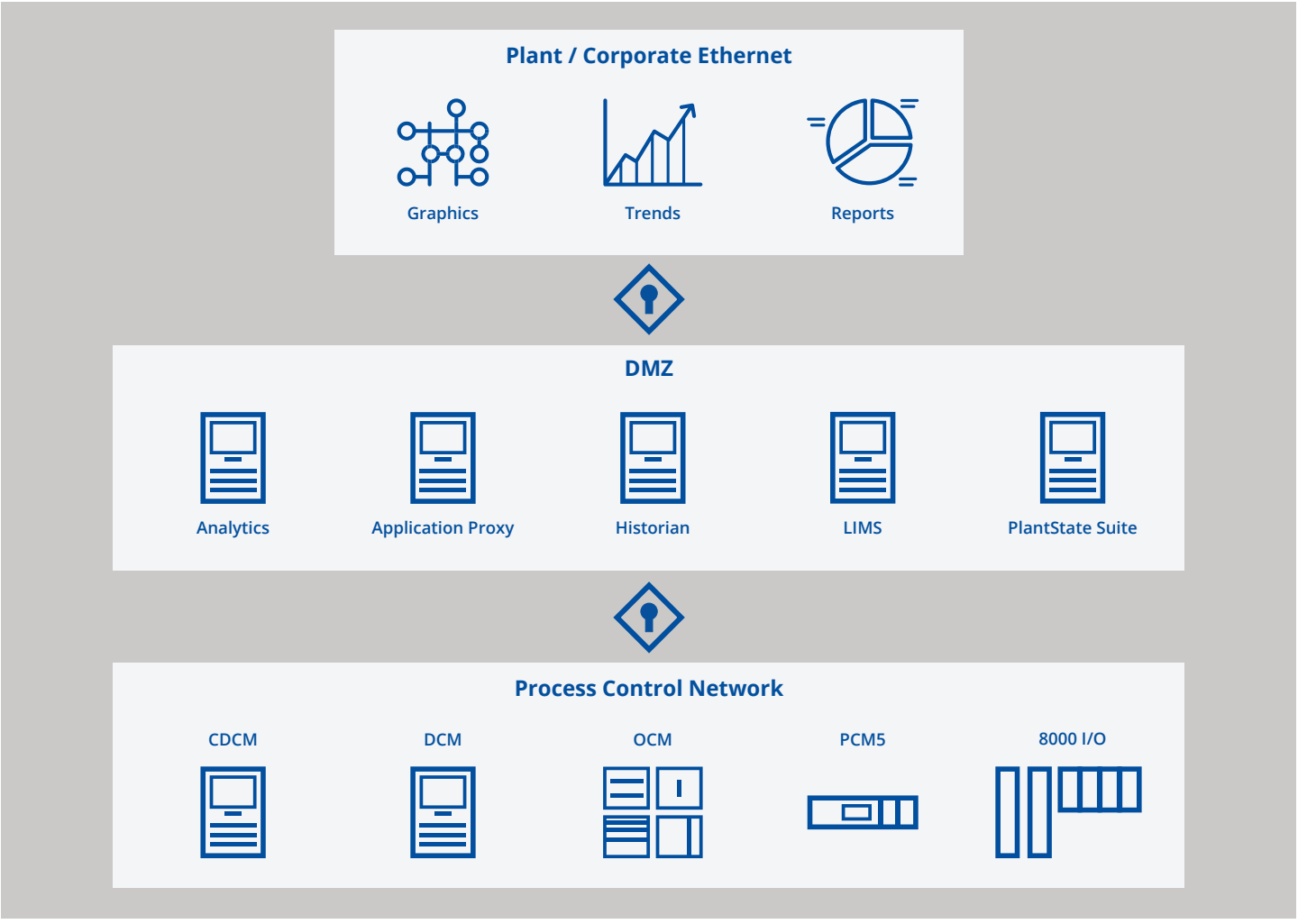
Network Designs

The most obvious way to prevent external threats to the control system through the network is to ensure the entire system is air-gapped. Although this is done in some very secure environments, it is not practical in many of today's modern plants where the enterprise requires access to control system data. In these cases, implementation of a network buffer zone with firewalls between the control system and any other systems will help reduce the risk of an external threat while providing inter-system communication. Such a buffer is commonly referred to as a demilitarized zone or DMZ.

*To help implement best practices in network design, access control, and countermeasures, review cybersecurity industry standards and sample frameworks such as NIST SP 800 series and ISA/IEC 62443 family of standards.

As a best practice, there should be no direct communication between enterprise systems and IACS systems; all data is exchanged through the DMZ. To support critical control applications, the DMZ and IACS layers together must provide critical services for the IACS environment that may otherwise be considered enterprise functions. Typical functions of DMZ servers include mirrored enterprise services, remote access services, patch and malware update management, and (in some cases) historians. Below the DMZ, the core IACS network should provide services such as historians, domain controllers, and time synchronization / master clock management. For example, NovaTech D/3 DCS provides an integrated interface to OSIsoft PI Systems. This feature allows the PI System server(s) to be installed in the DMZ and act as an intermediary between the other control systems, the D/3 DCS, and business systems requiring access to control system data.

Firewalls should be implemented in all layers of a plant including the industrial automation and control networks and on automation system computers. Specialized IACS firewall devices can be installed between the servers, controllers, and I/O sub systems to help eliminate or at least limit intrusions from unknown computers or programs. These industrial firewalls are designed to perform both protocol and deep packet inspection to control and limit communications to and from the various process automation system components. Process control vendors can also build these features into their hardware. For example, the D/3 PCM5 process controller uses an automatically configured Linux-based IPTables firewall. This basically prevents any non-D/3 node from communicating with or remotely logging into the PCM5.



NovaTech AUTOMATION

The network addresses assigned to the nodes of a process automation system should be non-routable static addresses. Dynamic Host Configuration Protocol (DHCP) on a process automation system is highly discouraged as it could provide an avenue into the control network. Additionally, by assigning only static IP addresses, each computer's network activity can be monitored and tracked. Users may also consider reassigning all standard ports used by common applications, such as 8081 (web servers) and 1433 (SQL servers), and configure other ports to communicate with these applications.

Companies commonly want to provide remote access to control systems to support engineering, troubleshooting, and monitoring requirements. Remote access from untrusted or home networks into critical production networks requires careful consideration and design to ensure remote workforce requirements are not providing a wide-open path for adversary groups.

- Engineering and IT should evaluate what systems should leverage remote access.

- Remote access requirements should be determined, including what IP addresses, communication types, and processes can be monitored. All others should be disabled by default.

- Validate your external exposure of IT and OT systems using networking tools.

- User-initiated access should require multi-factor authentication from the Internet to a DMZ through a dedicated jump host for ICS-specific communications. This system should leverage its own identity and access management system.

- From the DMZ, after authentication, user-initiated remote access should follow a trusted path to the OT system—where the user will authenticate again, this time using the local identity and access management solution.

- All remote access communications should be centrally logged and monitored. Various detection techniques should be implemented on remote access systems, such as looking for brute force attempts or specific exploits for known vulnerabilities.

System Configuration

Security features have improved with each new Windows operating system. Modern control systems should allow you to take advantage of built-in Windows security features like Windows Defender anti-malware, Windows Firewall, User Account Control (UAC). Proper system configuration will ensure security features are protecting the process automation system.

An industrial automation and control system security plan should include an antivirus application with regularly updated signatures that can be protect against malware without negatively impacting the memory or performance of the IACS computers. Most antimalware software uses blocklisting – scanning systems against a known list of threats which must not be allowed to run (blocked). The software signatures and blocklists must be kept updated to provide effective protection.

Along with an up-to-date antimalware service, we recommend using a proactive application control and allowlisting approach implemented with software like VMWare Carbon Black. Because most IACS computers have a relatively static software installation, they are ideal candidates for protecting with allowlisting software. This type of application allows the user to list all applications allowed to run on a computer (allowlist). Any other application that is introduced, whether malicious (e.g. a zero-day attack) or not, will not be allowed to run on the computer. Instead, the allowlist software produces alarms and records the execution attempt in a log for later review. In addition to implementing basic allowlisting, administrators can implement custom user profiles and group policies to further control application execution. Some users (administrators, system engineers) require more access to the system for enhancements, troubleshooting, and repair while others only require access to certain system functions. Industrial control system vendors should be able to provide detailed information to help configure an allowlist for their software to function properly.

Antimalware and allowlisting operations can put additional load on the IACS computers. The IACS vendor will help you verify that any antimalware or other software

added to the system does not diminish the real time operation of the control system. Benchmark testing is recommended before and after any additional software is installed to verify that time-critical automation functions are not affected.

Identity and Access Management

It is very important to manage and maintain individual user accounts for anyone accessing or using the process automation system. All unused standard user accounts such as Administrator, Guest, and standard accounts created by the process control system installation should be disabled and all generic passwords removed. Keep a record of system administrator user credentials in a safe and secure location to allow access to privileged accounts in the event of personnel changes. Most modern industrial automation and control systems support the use of local Groups or Active Directory groups for both Windows system access control and for controlling access to IACS-specific privileges. Individual user accounts should be added to the appropriate group based on their role in the organization. Note that a different set of privileges can be assigned to each user or user group. Example user groups are as follows:

System Administrators
IACS Administrators
IACS Engineers
IACS Operators
Boiler Room Operators
Line 1 Operators
Instrument Technicians
Supervisors

In the D/3 DCS, operators' span of control, the actions they are permitted to take on certain equipment or process units, is controlled by their username and Windows group membership. This is a very convenient way to set up privileges for certain classes of users and then assign each individual user to those groups. The D/3 DCS also features extensive logging of operator actions and engineering configuration changes, including the username, computer name, and timestamps. These features support security auditing as well as regulatory record-keeping compliance (e.g. 21 CFR Part 11 and GAMP 5). Log files are easily searched for all activities performed by a certain user.

Once policy settings are defined, proper control and management of user access credentials and privileges must be a regular high-priority activity. Immediately remove accounts for users who should no longer access the system. Require users to change passwords periodically. Control system user credentials should not be the same as the user's corporate / business system credentials. Shared credential management between IT (Information Technology) and OT (Operations Technology) networks such as connected Domain Controllers is a proven mechanism for the distribution of ransomware software inside the network. Multi-factor user authentication, which requires both something the user knows (password) and something the user has (token), is another important security enhancement to consider for mitigating compromised user credentials and passwords.

Control System Configuration Management

With the industrial automation and control system equipment physically secured and external threats addressed, it is time to consider internal threats. Physical security and system configuration hardening provide tools for guarding against internal threats. Disabling AutoPlay and USB ports and requiring login password complexity and password reset are just some of the policy settings designed to increase security. NovaTech Automation can assist customers with these and other policy settings to ensure secure operations of their D/3 DCS.

A Configuration Management system is a fundamental tool to prevent unauthorized control application editing or erroneous / malicious control system configuration changes. Configuration Management tools can also provide a means of backing out / recovering from these changes. The D/3 DCS includes the ability to integrate several of the most common source control configuration management tools on the market.

Where possible, a separate development control system with a medium-fidelity process simulation should be employed. Separating the development system allows engineers to develop and test application and system configuration modifications without jeopardizing the integrity of the actual process automation system. The Configuration Management tool can be used to ensure only specific changes are implemented. Remote access to a development system via VPN would provide secure access for development and troubleshooting without compromising production system integrity. NovaTech Automation has installed several development and test systems on virtualized platforms to provide a cost effective, reliable solution.

Plant managers and system administrators should consider a role-based approach to limiting functionality within the industrial automation and control system. For example, utilities operators should be able to manage and control boiler equipment but not production line equipment. Likewise, production operators should not be able to control utilities area equipment. Access to control loop tuning parameters, alarm suppression tools, or I/O address changes can be restricted to authorized maintenance technicians. The D/3 DCS provides multiple methods for granular span-of-control adjustment which can be configured by user and also by console (workstation), thereby restricting access to an operator's respective area of responsibility. By specifying (and possibly even dynamically adjusting) the security parameters of a process unit or specific device tag, system engineers can prevent inadvertent operation of equipment outside of an operator's area of responsibility.

Recovery Planning

Disaster recovery is an essential component in the overall cybersecurity plan. In a distributed control system like D/3 DCS, functionality is distributed across the various nodes of the system and virtually every component can have a redundant backup. Therefore, no single point of failure should significantly impact plant operations. In the event of a complete disaster such as a fire, hurricane, flood, or severe cyberattack, a comprehensive disaster recovery plan can help the plant resume operations as quickly as possible. A fundamental part of this plan must be a data backup plan. Daily incremental backups as well as weekly full backups should be automatically scheduled and both onsite and offsite storage locations should be established. Plant managers and system administrators should also consider how all network switch, gateway, PLC, and even field device settings critical to the IACS are documented and backed up and include these in the overall data backup plan. With the backup process in place, it is vital to test the backed-up data on a regular basis and ensure it can be recovered. Backups are useless if the data cannot be retrieved properly and efficiently.

Critical spare and replacement components for the IACS are an important part of the disaster recovery plan. Using a development or training system as a hardware backup location (including replacement servers, operator stations, controllers, switches, and gateways) provides the plant with a robust and responsive backup source that is already proven and ready to install.

Create and maintain a disaster recovery plan including:

- Designated personnel and action plans
- Backup hardware, including servers, switches, and other critical spares
- Software and data backups (onsite, offsite) and recovery testing
- Safe and secure location of system administrator user credentials
- Safe and secure location of physical media
- Separation of physical equipment (servers, operator workstations, network gear)

Security Maintenance Checklist

With the best security measures in place, there is still no substitute for due diligence. Threats will continue to evolve and even the best countermeasures of today will not be the best countermeasures of tomorrow. Regular (weekly) review of Windows application, Windows security, and Windows system logs should be performed. Periodic (twice daily) review of control system alarms should also be performed. Additional logs associated with networking traffic and control system performance should be included in a regular (weekly) review.

Even if the process automation system is isolated, software updates should be done on a regular basis to address enhancements or patches to existing the operating system and support software. Regular scanning of the system for any previously unidentified issues is also encouraged. If antivirus software is employed on the process automation system, malware signatures must be updated on a regular basis. All major antivirus software managers have a mechanism for updating the definitions offline. Regular checks should be made of hardware vendors' security bulletins to ensure firmware, BIOS, OS, etc. issues are addressed. These checks can be made manually or by using automated tools. NovaTech Automation regularly tests and validates Microsoft OS patches for compatibility with D/3 DCS and makes these results available to customers.

Plant managers and administrators should also consider working with their control system vendors to create a checklist and action plan to ensure that their IACS is configured properly, stays updated, and in top operational condition. NovaTech Automation offers several cost-effective support and maintenance plans to assist customers with designing and maintaining a secure automation system.

Conclusion

Industrial control systems are a potential target for different entities with varying motivations. Threats range from accidental corruption, deletion, or distribution of sensitive data to industrial espionage or even terrorism. While the job of the automation professional has always been demanding, today's world requires added attention to risk management with respect to cybersecurity. Process control engineers should take a proactive approach to cybersecurity, perform a comprehensive risk analysis, and develop a plan to minimize and manage cybersecurity threats on their process automation systems.

In summary, please consider the following steps to improve D/3 System cybersecurity:

- Identify, evaluate, and remediate risks to increase cybersecurity
- Ensure physical protection
- Follow good network design and configuration practices
- Manage user access
- Manage control system configuration
- Prepare for disaster recovery
- Be vigilant - create a checklist and perform periodic maintenance and evaluation

NovaTech AUTOMATION

Sample Security Checklist

Control System Engineering and Configuration

- Review configuration to ensure cybersecurity and recommended system settings (monthly)
- Review system alarms (twice per day)
- Review spare capacity of hardware, I/O, system con figuration (tags), controller memory, etc. (quarterly)
- Ensure critical monitoring applications within the IACS are running properly and up to date (daily / weekly)
- Develop plans for next scheduled plant outage (weekly / monthly)
- Review and plan for IACS vendor patches (monthly / quarterly)

Process Controllers

- Physical access
- Network configuration, access
- Power & power supply analysis
- Memory and CPU usage
- Spare capacity analysis
- Recovery plan for failed controller

Servers

- Microsoft patches
- IACS vendor patches
- Review access logs
- Antimalware is functioning and updated
- Allowlist configuration and error/alarm logs
- RAID disk status and spare disk space
- Memory analysis
- Physical ports locked down
- Unnecessary applications locked down/eliminated
- User account and credential management
- Backups made
- Daily backup made on engineering stations
- Disk cleanup
- Physical inspection of fans, keyboard, mouse, monitor, keyboard
- Spare parts/spare server
- Recovery plan for failed server

Workstations / Consoles

- Microsoft patches
- IACS vendor patches
- Antimalware is functioning and updated
- Allowlist configuration and error/alarm logs
- Disk space/disk cleanup

NovaTech AUTOMATION

Workstations / Consoles (continued)

- Memory
- Physical ports locked down
- Physical inspection of fans, keyboard, mouse, monitor, D/3 keyboard
- Spare parts/spare computer
- Recovery plan for failed computer

User Account Management

- Review user credential management
- Review user groups
- Review users within groups
- Review user and group privileges

Network

- Network switch analysis
- Firewall analysis
- Port usage
- Spares (switches, fiber transceivers, fiber, cables, wireless components)
- Documentation/backup of configuration for all network components

Physical

- Rooms
- Cabinets
- Fans in all cabinets
- AC in computer rooms
- Grounding
- Access control list

Disaster Recovery

- Risk analysis
- Disaster recovery plan in place
- Onsite/offsite backup media

Spares Analysis

- Spares in place for all critical system components

NovaTech AUTOMATION

Resources

ICS-CERT Home	https://us-cert.cisa.gov/ics
CERT CSET	https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET
NIST Cybersecurity Framework	https://www.nist.gov/cyberframework
SANS Vulnerability Management Maturity Model	https://www.sans.org/blog/vulnerability-management-maturity-model/
MITRE ATT&CK Framework Guide	https://attack.mitre.org/
Dragos ICS CYBERSECURITY YEAR IN REVIEW	https://www.dragos.com/year-in-review/
FireEye Cyber Threat Map	https://www.fireeye.com/cyber-map/threat-map.html

CISA	The US Cybersecurity and Infrastructure Security Agency
ICS-CERT	Industrial Control Systems Computer Emergency Response Team, a group within CISA dedicated to industrial control system security