Life Is On | Foxboro by Schneider Electric

Foxboro Evo Process Automation System — The security perspective

by Gary Williams

Table of contents

Introduction . . . 3
Best practices, policies, and procedures . . . 3
The threat . . . 3
Foxboro Evo System is designed to protect . . . 4
Services . . . 6
Conclusion . . . 7
Foxboro Evo features . . . 8

Introduction

For over 100 years, Foxboro™ has been innovating for and servicing the process industries. Its success is based on the ability to incorporate new technologies to ever-changing client needs. It has continuously adapted to all aspects of our industry from new protocols to new operating systems.

Today, one of the biggest threats to all process automation systems (PAS) comes from Information Technology. Ten years ago these threats were based on viruses; today these threats come from viruses, malware, and even one-off exploits written for personal, financial, or political gain.

Instead of hackers putting themselves at risk of being caught, there is a new trend of gaining fame and notoriety by analyzing software and systems to identify vulnerabilities and reporting them to the public.

Best practices, policies, and procedures

To mitigate cybersecurity threats, the importance of adopting and adhering to best practices, policies, and procedures cannot be emphasized enough. Failure to do so will render any control and safety system security vulnerable.

At the very least, all companies should adopt and practice an information security management system, such as outlined in ISO27001. ISO27001 is a solid foundation to build upon and ideal for those wishing to become compliant with the latest standards, such as ISASecure, IEC62443, NIST, etc.

The threat

The most successful attacks in recent years have actually been initiated from within by internal employees or contractors through the use of removable media or connectivity of an exploited engineering laptop. Protecting a PAS is no longer a case of simply building firewalls to mitigate external threats. Due diligence and effective action have to be applied at every level of the system.

So where does one start? Mitigation and protection are based on a clear understanding of the threats. The Foxboro Evo system has continuously evolved with protection from these threats in mind, based on sound risk and threat assessments.

Let's start with external threats. Gone are the days of autonomous automation systems. The pressure to respond to ever-changing customer demand and financial markets is huge. In order to respond in a timely fashion, the corporate decision makers need real-time information from the shop floor. This requires connectivity between the PAS and the corporate IT systems.

IT departments, responsible for protecting corporate systems, have a wide experience with network design and implementation, and cybersecurity. They are bombarded on a daily basis with information on potential corporate threats, unlike the engineers responsible for the PAS. The IT department configures their firewalls and switches, applies OS patches, and updates anti-virus software on a daily basis to protect their corporate information systems. Often these systems are redundant, so in the event of a successful attack they can quickly switch the systems from primary to secondary, identify the attack, and mitigate accordingly.

An attack on a PAS, however, poses a much bigger threat. Not only could an attack stop production, resulting in million-dollar losses, but because of the harsh environments controlled by these systems, it could result in loss of equipment availability, equipment damage, and even loss of life.

In order to meet the demand of providing real-time information to corporate bodies, but at the same time protecting the PAS from threats experienced on the corporate networks, intricate network design is required.

Foxboro Evo System is designed to protect

The Foxboro Evo System is designed to protect the operational integrity of your plant. The system is architected in layers. Within each layer, the portions of the system that must interact in real-time are grouped. These groups are lightly coupled with each other such that only necessary information is transmitted between groups. When designed in this manner, the plant has increased reliability, is hardened against fault propagation, and supports the security protection approach described below.

This protection starts with a demilitarized zone (DMZ). An external attacker can only get access to the network connected to the Internet or an available external connection. The DMZ acts as a gatekeeper that prevents any external threat connectivity to an internal isolated network. Its purpose is to protect the internal network from external attacks.

The internal network also requires operating system patches and antivirus signatures to be updated on a regular basis in order to protect it from threats originating from other vectors (i.e., internally). It is not always possible to patch or update a PAS in real time without interruption to production, thereby causing delays in updating and increasing the risk.

An example of another threat is identity protection: for example, a disgruntled engineer using another engineer's login credentials in order to access the system. To protect against this, the Foxboro Evo System utilizes Microsoft® Active Directory (AD). AD domain controllers manage the access rights of each user and computer in a Windows® domain. It is configured to both grant and restrict access to those activities that are required for an individual to carry out his/her duties.

AD will report any unusual activity, such as failed attempts to log in or changes to a directory structure, giving the administrator an early indication of something amiss. It is possible, through AD, to mandate only certain programs can be utilized by certain users. It can restrict one machine from talking to another. Although AD has a multitude of capabilities to protect a system, its users, and machines, it is quite complex and requires a detailed understanding of the control system in order to be configured correctly.

The Foxboro Evo System implementation of AD uses a single domain for the entire control network with multiple organizational units (OUs), group policies, and security groups:

Organizational unit (OU)	Group policy	Security group
Foxboro Evo computers	Default domain	
Foxboro Evo users	Default domain	Domain users
Plant maintenance	Plant maintenance	Plant maintenance
Plant engineers	Plant engineers	Plant engineers
Plant engineers	Plant operators	Plant operators

Note: Plant maintenance, plant engineers, and plant operator OUs are contained in the Foxboro Evo users OU. There are two additional security groups, Foxboro Evo installer and Foxboro Evo services, created for the purpose of installing software and running specific services.

What if the threat was to come from external media, such as a CD-ROM or a USB device? The Foxboro Evo System uses McAfee Enterprise Policy Orchestrator (ePO), a suite of products that facilitates the control of hardware. Through the use of this suite, the Foxboro Evo System is configured to allow only authorized users to access such devices as the USB ports or the CD-ROM drive. For all intents and purpose, to any unauthorized user, these devices are switched off.

ePO also offers other facilities utilized by the Foxboro Evo System for protection, such as Host Intrusion Prevention Systems (HIPS), a Policy Auditing facility, and rogue system detection. All of these facilities and more are used to protect the Foxboro Evo System. It also enables clients to centrally manage their systems through the provision of:

- Logging
- Reporting
- Software distribution
- Package updates
- Scheduled scanning
- Monitoring and alerting

A list of Foxboro Evo features and definitions can be found at the end of this document.

Migration/upgrade

Foxboro Evo builds on the continuously current philosophy of I/A Series — providing a futureproof platform for customers to cost-effectively take advantage of new technology while preserving their investment.

Hardware compliance

Foxboro Evo hardware is evolving with an emphasis on security from concept to delivery, ensuring new products follow international standards, such as ISASecure and IEC 62443. Embedded devices undergo a communication robustness test following Wurldtech Achilles certification and ISASecure/IEC 62443 EDSA (Embedded Device Security Assurance) certification procedures. Devices such as control processors, communication modules, and field devices are all designed with security considered from concept to delivery.

Services

Operating systems and antivirus signatures must be current to be effective. Schneider Electric tests these updates on the current and three previous iterations of its systems and informs clients of updates that are approved and pertinent to their system(s).

Through our Customer FIRST support program, these updates can be delivered directly to site, saving time and resources traditionally spent on identification and acquisition of updates pertinent to the client's systems.

In addition to the Foxboro Evo System, Schneider Electric offers network/system design and implementation services. Through our Cybersecurity Services team we offer a number of services:

- Network and systems engineering
- Vulnerability assessments
- Network and system audits
- Gap analysis and mitigation planning
- Network and system hardening
- Infrastructure evaluations
- Security program review/development
- Incident/emergency response services
- Information security training
- Backup and disaster recovery
- Endpoint protection

Conclusion

The Foxboro Evo System provides a significant, evolutionary step toward protecting your plant's operational integrity. It is backward compatible with multiple generations of I/A Series, offering new capabilities that provide operational insight to every worker to perform his or her role faster, better, and with more ease of use.

The Foxboro Evo System evolves with the environment, not just to threats, but also in compliance with international standards and new engineering trends.

With the end of life of Windows XP® in April 2014, new exploits being publicized for field devices, SCADA systems, and PLCs, cybersecurity represents one of the most critical threats, and the biggest investment clients will make in the near future. That investment will likely be made to fix, not replace, the current installations. Where a fix is not possible, it is likely that the investment will be in compensating controls, such as firewall isolation.

Historically, compensating control manufacturers are smaller entities than the PAS vendors. The adoption of these products often presents disparity in support agreements. Furthermore, it is feasible that any future update or patch would have to be tested both against the compensating control and the PAS. Although this investment and action is necessary, the more compensating controls, the more diversity in vendors, and subsequently the greater the increase in support cost. Ideally clients should pressure their process control vendors to provide these compensating controls and insist that they test and support them in line with their products. This is one of the strengths of the Foxboro Evo System. The Foxboro Evo System evolves around the same issues as experienced by our clients, thus providing an all-encompassing system to meet clients' needs.

Foxboro Evo provides the ability to control, operate, and maintain your processes in a safe and continuously resilient manner by evolving in line with the latest threats. With proper adherence to best practices, policies, and procedures, your system will protect you not just today, but tomorrow and well into the future.

Foxboro Evo features

ePolicy Orchestrator (ePO)

A unifying security management open platform by McAfee. ePO makes risk and compliance management simpler, enabling clients to connect security solutions to their enterprise infrastructure to increase visibility, gain efficiencies, and strengthen protection.

Anti-malware

Virus scans prevent, detect, and remove malware, including, but not limited to, system viruses, computer viruses, computer worms, Trojan horses, spyware, and adware.

Host Intrusion Detection System (HIDS)

HIDSs monitor and analyze the internals of a computing system. A host-based IDS monitors all or part of the dynamic behavior and the state of a computer system.

Data Loss Prevention (DLP)

DLP systems enable organizations to reduce the corporate risk of the unintentional disclosure of confidential information.

Active Directory (AD)

AD provides a central location for network administration and security. It authenticates and authorizes all users and computers in a Windows domain type network — assigning and enforcing security policies for all computers including the installation or updating of software.

Harden OS

Factory hardening is a procedure that updates patches and antivirus software and disables unused ports and services. System hardening is necessary because the default operating system installation focuses more on ease of use over security.

Whitelisting

Whitelisting contains rules that discriminate who or what can utilize programs. The use of whitelisting ensures that no rogue program or unauthorized user executes unauthorized programs.

Backup Exec System Recover

Centrally manage backup and recovery tasks for multiple desktops across the network. Schedule backups to run automatically, including event-triggered backups, without disrupting the network.

Foxboro Evo Station Assessment Tool (SAT)

A Windows-based Foxboro application automatically installed on all Foxboro Evo workstations and servers with Windows operating systems on the MESH network. It supports full functionality on all stations.

About the author

(Gary Williams) Sr. Director Technology, Cybersecurity and Communications
Schneider Electric