SIEMENS

White Paper

Cybersecurity for Automation Systems

Abstract

Cyber-attacks on the automation infrastructure of facilities in the United States are real. Securing the automation infrastructures can be a difficult task and is more difficult on aging infrastructures that have no cybersecurity features and those that are running with operating systems that have become obsolete. Some customers believe that their IT departments can adequately protect these automation infrastructures. But what happens when the IT protection fails or the saboteur is able to bypass the surrounding network and connect directly to the automation system? At that point it is the responsibility of the automation system to protect itself against unauthorized access, against malware, against theft of critical software algorithms, and against unauthorized modification. Additionally, the automation system must be able to detect that it has been manipulated, detect intrusion, and report cyber activity.

Modern automation products have implemented cyber protection features for automation. These features, when properly configured, provide additional protection for aging infrastructures. This paper describes the implementation of these protection techniques and how they apply to new and aging automation infrastructures.

Author
Wayne Cantrell
Senior Principal Systems Engineer
Siemens Industry, Inc.

Introduction

From the time that man has been on earth, there has been conflict and warfare. Over the centuries, man has developed and continues to develop security mechanisms for protection. Until the advent of overwhelming force, one of the most successful protection mechanisms was the castle. The reason for success of the castle was the use of multiple protection mechanisms designed to confront many forms of attack. Some of the more useful castle defenses included.

- a building site where an enemy can be spotted from a great distance so the castle occupants would have adequate time to enable their defenses
- thick inner and outer walls to provide double difficulty for the enemy and provide a space between the walls where the enemy would be vulnerable to attack
- a moat to create difficulty assaulting a wall
- a drawbridge to provide a single point of entry
- round towers to prevent undermining corners
- small attack slits in the wall to protect the castle defenders
- passageways to dead ends
- variable size stairways to prevent rapid advancement by the enemy

These are just a few of the innovative techniques that were used to protect the occupants of the castle. Even with these protections, the castle was still at risk with one of the major concerns being the enemy within. This was the case until the invention of a super weapon, the catapult, that could destroy the castle defenses with overwhelming force. The castle concept provided good protection for hundreds of years.

One may wonder why we mention the castle in a modern cybersecurity paper. The reason is that there is similarity to defending both a castle and an automation system in the fact that in order to be successful multiple defense mechanisms are required. Additionally, downfalls to each include an insider with bad intentions or an overwhelming breach were the last element of defense is the individual; albeit an individual occupant or the cyber protection capability of the automation equipment itself.

This paper is dedicated to the ability of the automation equipment to protect itself.

Defense In-Depth Strategy

Defense In-Depth is a common term used today in cybersecurity discussions. In a nutshell, it means deploying multiple mechanisms of cyber defenses.

In a production plant environment or a military installation, including facilities, ships, weapon systems, etc., there are three areas that need protection. The three include the perimeter (plant security in a production facility), the integration or interconnecting elements (networking connections), and the system itself (devices or control components). Figure 1 is a depiction for a production plant.

Figure 1: Plant Defense In-Depth

Network Security

In modern automation systems, most of the access is through remote or local network connections.

A real-world example for a production plant is when a customer purchases a machine from a supplier and needs fast service such as in the case of a malfunction in the machine. Rather than wait for someone to travel to the plant, the production management prefers a remote connection for troubleshooting. However, this remote connection needs to ensure that an authorized person is connecting, the person does not introduce malware during the connection, and that the person only accesses the machine that needs support, not any machine in the plant.

The accepted design approach for modern automated plants is to create production cells and apply security to each cell and a cross cell security approach that protects all cells and forms a barrier between the information network (IT) and the operations or production network (OT). Industrial networking products provide these capabilities.

First, industrial security devices exist that are used to establish a VPN connection. The VPN provides authentication and encryption for the person connecting remotely. Since the person will need credentials for access, they must be given the authorization certificate for the data encryption.

For IT/OT barrier protection and cross cell protection, networking products exist that protect against malware introduction, detect intruders, prevent intruders, and provide additional advanced firewall protections. These capabilities can be achieved using industrial networking components or security software running on industrial PCs.

RADIUS servers have been used for years as an additional authentication method for users. Modern industrial automation hardware supports RADIUS authentication, so an added level of security is provided in addition to the VPN.

Depending on the RADIUS server being used, it may have a configuration screen that allows a security officer to block or allow access by simply checking a box which provides a third level of security.

Finally, a RADIUS server will allow access to an IP address or a range of IP addresses which can provide access only to the equipment authorized for the user.

A White Paper issued by: Siemens.

In addition to a VPN and RADIUS servers, other products exist that combine VPN management and specific device access in a single access server.

When combined, these solutions provide multiple levels of security for remote access thus creating a Defense In-Depth strategy. Figure 2 is an overview diagram of a remote connection with Defense In-Depth features.

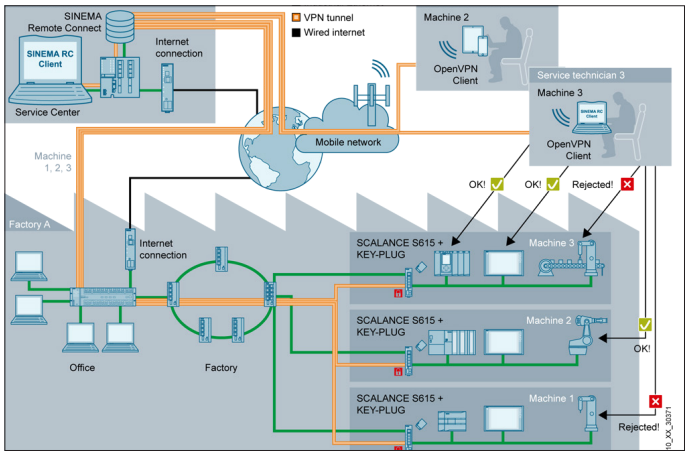

Figure 2: Remote Connectivity

As automation enters the Industry 4.0 era, requirements to connect automation systems to enterprise systems are a must. This connectivity creates new concerns for the once isolated automation systems. OT networking systems have more stringent requirements than IT networking systems. Differences include protected interfaces with the IT infrastructure, secure remote access, redundancy, performance determinism, wireless infrastructures for control, mobile applications, and hardware built for industrial environments.

Until recently, secure networking components have been produced mainly for the IT environment, but industrial networking components have begun to catchup. Industrial network switches are being produced with the following features:

- Integrated VPN
- Integrated IP and MAC firewalls
- Stateful inspection firewalls
- Ability to host threat prevention features and Malware protection
- Protection against known and unknown threats
- Ring or duplicate hardware redundancy
- Dual power sources
- Deterministic performance with Quality of Service or “cut-through” technology
- Failsafe systems utilizing wireless infrastructures
- Operating temperatures ranges of -40 up to +85 degrees C
- Diagnostics by the automation controller

Network protection is a requirement for modern automation systems.

System Integrity

Plant and network protection are extremely important for protecting an automation system, but they fall short in the quest for total protection. Additional protection in the event of physical access to the control system is also necessary and available. Examples include when an employee with bad intentions has access to the automation system, or a service technician has temporary access, or someone breaks into the control room of a remote site, or someone breaks into the electrical cabinet of a traffic control system, or an automation controller is accidentally connected to the internet. These are just a few possibilities. Security standards have recognized this, such as NIST 800-82 Revision 2 section 6.2.11. (Reference 1)

If physical access to the control system has been attained, the control system must have some capabilities to protect itself. Some of the areas of concern are:

- connectivity to components of the automation system
- protection against unauthorized access
- protection against unauthorized modification
- protection against manipulation
- intrusion detection
- authentication support
- security reporting

Connectivity Protection

Previously in this document, methods were mentioned for controlling access to an automation system, but these were features of networking infrastructure components. Modern control components, such as Programmable Logic Controllers (PLCs) have recently added protection mechanisms of their own.

PLCs protect themselves from unauthorized connectivity by utilizing network separation between their control networks in the plant and IT networks which is used for programming or connectivity with enterprise level systems. Some PLCs can support more than ten subnets. Figure 3 is an example of PLC network separation.

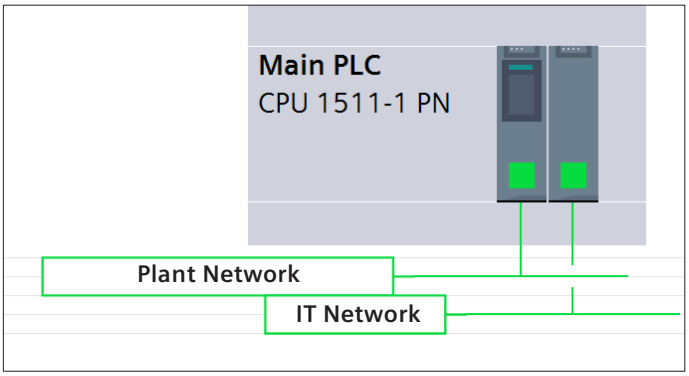

Figure 3: Separation of PLC Networks

A second connectivity protection method is to provide IP and MAC address firewalls in the PLC networking components. Figure 4 depicts the firewall rules table of Communications Processor module used in conjunction with a PLC.

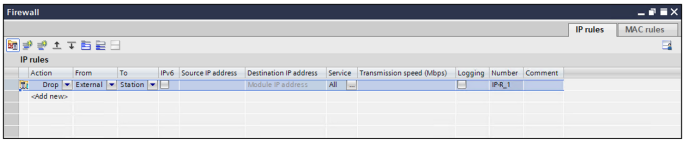

Figure 4: PLC Firewall

A third method is to include VPN connectivity directly into the PLC. Figure 5 shows an integrated VPN connection that has been setup for programming access.

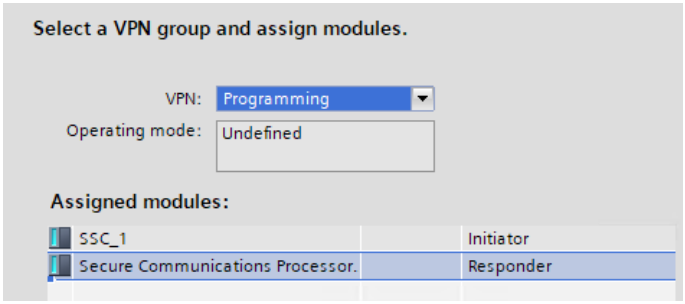

Figure 5: A PLC VPN

An additional method, that is less sophisticated, is to disable open network ports on the PLC's networking components (the PLC itself, Communication Processors, integrated network switches, distributed I/O racks, etc.). The hardware configuration of the PLC allows these unused ports to be deactivated, as shown in Figure 6. When the port is deactivated, it will not establish a communication link with a connected device.

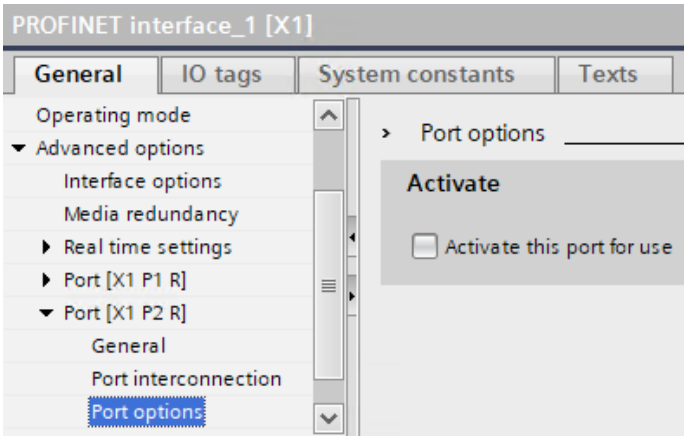

Figure 6: A Deactivated Network Port

Unauthorized Access Protection

After meeting all the authentication requirements to access the PLC, a programmer or maintenance person must still have the usability credentials of the PLC itself. Modern PLCs have role-based protection mechanisms. The roles typically include read-only access, read/write access, failsafe program access, and HMI/SCADA access. Each role has its own password and depending on the capability of the PLC, these passwords can be up to 30 characters or more. Figure 7 shows a typical role-based access control configuration screen.

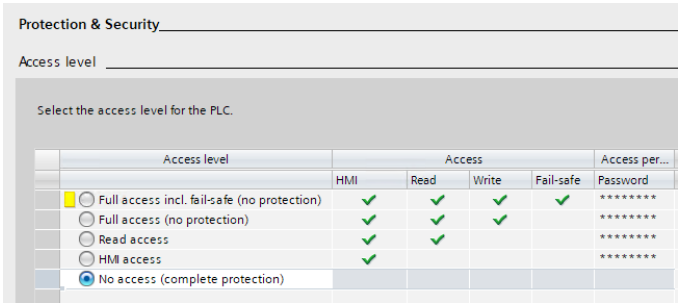

Figure 7: Role-based Access Configuration

Figure 8 shows examples of complex passwords for the roles mentioned above.

Read-Write Password(+ safety):	#t%H(i+S- @t%H-e* !F(u%L&I) !F(a%I*I^S&a$I#f@E _A=c-C*e@S's` ~P#a!S^sW%o$R^d+
Read-Write Password:	#t%H(i+S- @t%H-e* !F(u%L&I) _A=c-C*e@S's` ~P#a!S^sW%o$R^d+
Read-Only Password:	6!T@h-I=s+ &i$S, @a^ #R(e)A~d-O$n$L!y` *P&a$`S=s+W.o?R/d`0
HMI Access Password:	1>t<H#i~S`$i@S)-I%H+e-&H&m#^&*

Figure 8: Role-based Passwords

In some instances, there might be a need to lockdown the PLC either partially or completely. A good example would be the detection of an intruder on the PLC's control network. In this case, the PLC provides a logic instruction that can deactivate the roles shown in Figure 7 even though the user may have valid credentials (the passwords from figure 8). Figure 9 is an example.

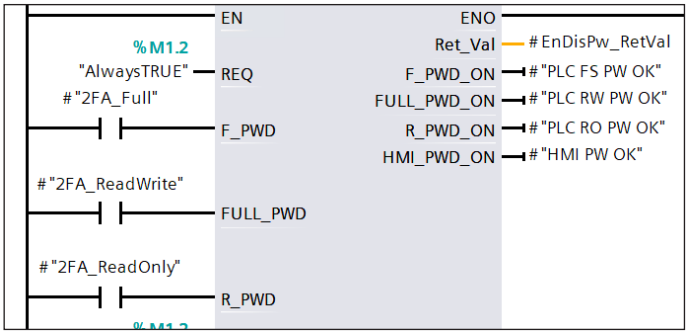

Figure 9: PLC Lockdown Instruction

Unauthorized Modification Protection

Even though a user has network access credentials and PLC usage credentials, it still doesn't mean that they should have the ability to view all the internal program logic of the PLC program. An example is the role of a maintenance person. A maintenance person can view and troubleshoot at a high level but does not need the ability to view specific algorithms that may be the intellectual property of the engineer's company that created the program or manipulate the program in such a way to cause it to malfunction. Mechanisms for this type of protection in a PLC include encryption and copy protection. Figure 10 shows the properties of a PLC subroutine with selections for Know-How Protection (encryption) and Copy protection. In both cases, the protection password can be

A White Paper issued by: Siemens.

up to thirty characters and can include upper and lower case letters, numbers, and special characters. This means the number of password combinations is approximately 2.596 e+57.

For copy protection, the PLC's program execution is bound to either a CPU with a specific serial number or a memory card with a specific serial number. In both cases, if the program is copied and an attempt is made to run this code on different hardware components, the PLC program code will not execute. This prevents reverse engineering of the PLC's program operation.

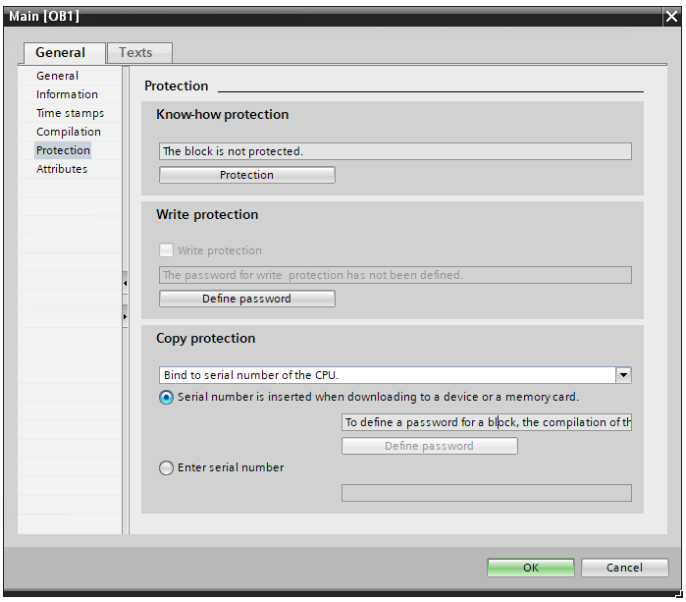

Figure 10: PLC Program Protection

In the example just mentioned regarding a maintenance person, the maintenance person will need access to certain portions of the program. To allow this, the ability to lock individual program objects and data objects is needed. Figure 11 shows several different program logic objects with an individual password for each. This prevents a single password from providing access to all the program objects.

OB1 Password:	,93T^h?!$s* *!:s; %T>h[E; ~c`OB1{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
OB30 Password:	,56T^h?!$s* *!:s; %T>h[E; ~c`OB30{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
OB31 Password:	,78T^h?!$s* *!:s; %T>h[E; ~c`OB31{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
FB1 Password:	,62T^h?!$s* *!:s; %T>h[E; ~c`FB1{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
FB2 Password:	,77T^h?!$s* *!:s; %T>h[E; ~c`FB2{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
DB1 Password:	,31T^h?!$s* *!:s; %T>h[E; ~c`DB1{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
DB4 Password:	,88T^h?!$s* *!:s; %T>h[E; ~c`DB4{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
DB7 Password:	,@@T^h?!$s* *!:s; %T>h[E; ~c`DB2{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
FB10027 Password:	,93T^h?!$s* *!:s; %T>h[E; ~c`FB10027{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&
Binding to memory card password:	,$%^^h?!$s* *!:s; %T>h[E; ~c`O+d{E# !s8E|c(U^r}!.t'Y? }p5A@s`-S_w7O2r@D&

Figure 11: PLC Program Object Protection

Figure 11 also shows that the data repository elements (DBs) can also be protected from modification via passwords. Additionally, some data elements may need to be write protected. A good example would be the overspeed setpoint values for a gas turbine engine. The ability to write protect data also exists. Figure 12 shows the configuration screen.

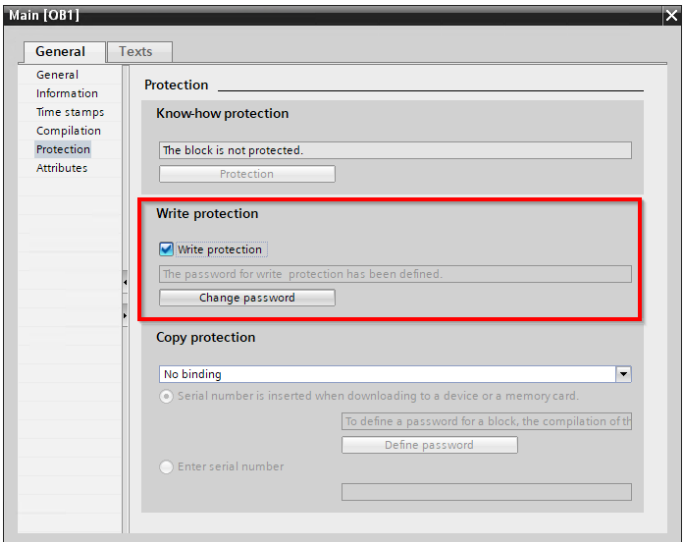

Figure 12: PLC Data Write Protection

Manipulation Protection

With all the protections mentioned thus far, a break down in security policies could still result in a situation where the PLC is vulnerable. Unauthorized manipulation of the PLC's logic program needs to be detected. This detection needs to not only include the PLC's program logic, but data constants used for personnel and machinery safety. Additionally, if the PLC manages the status and alarm messages that go to HMI/SCADA systems, modifications to these messages need to be detected to prevent false status values and the masking of alarm situations. To detect these types of modifications, the PLC has logic instructions that can compare the checksum of the program logic, the alarm text, and status messages to known values in real-time. These instructions should be placed in encrypted logic objects and for additional protection, called from multiple encrypted program objects. In the event one of these objects is compromised, its partner objects will detect the modification. Figure 13 shows the logic instruction.

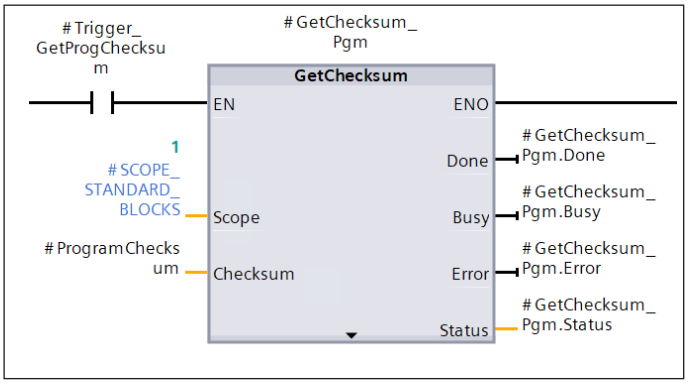

Figure 13: Program Modification Detection

A PLC program can be compromised without changing its logic. One method is to make unauthorized data changes via an HMI/SCADA device. To protect against this, the ability to exclude data from these devices or even the PLCs OPC UA server is provided. Figures 14 and 15 show this ability.

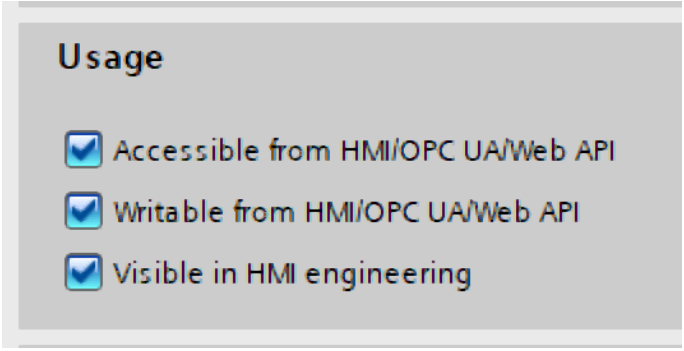

Figure 14: PLC Data Segmentation

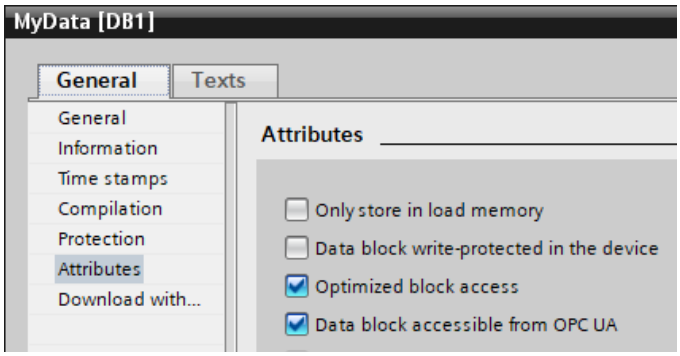

Figure 15: PLC Data Inclusion/Exclusion

Cybersecurity practitioners often refer to a "man in the middle" attack as a technique used for intercepting and manipulating communications. In this type of attack, communication data can be recorded, modified, used to reverse engineer the automation, and potentially retransmitted back to the PLC to cause harm. To reduce the risk of these types of attacks, PLC and HMI communication protocol now support cryptographic integrity protections and secure authentication. The selection and use of a robust password is part of the secure authentication process. Figure 16 shows a connection to an HMI/SCADA device where the HMI password is used to support the secure authentication.

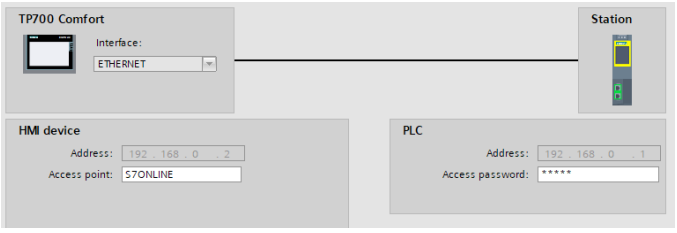

Figure 16: Protected PLC – HMI/SCADA Communications

PLCs communicate with more than HMI/SCADA devices. There are requirements to create complex automation systems where PLCs communicate between themselves and to other equipment. PLCs support industry standard protocols to meet these requirements but these protocols must be secured as well. Over recent years, the OPC protocol has moved away from its roots in Microsoft's COM and DCOM models to a TCP/IP model for communications plus added protection mechanisms. OPC UA is the new standard for the protocol. OPC UA communications supports up to 256-bit encryption. Since modern PLCs have OPC UA servers integrated, they must support these encryption mechanisms which means they must support security certificates. The engineering tools for the PLCs must be able to import and download certificates from partner devices and generate certificates for the partner devices in order to secure communications. Figures 17 and 18 show certificate management and the encryption settings for a PLC's OPC UA server.

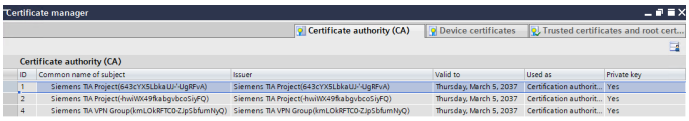

Figure 17: PLC Security Certificate Management

Figure 18: PLC OPC UA Server Security Settings

OPC UA is not the only protocol supported by a PLC. TCP/IP communication is widely used so the ability to encrypt those communications is also necessary. Transport Layer Security is needed. Figure 19 shows an example of secure communications between two PLCs.

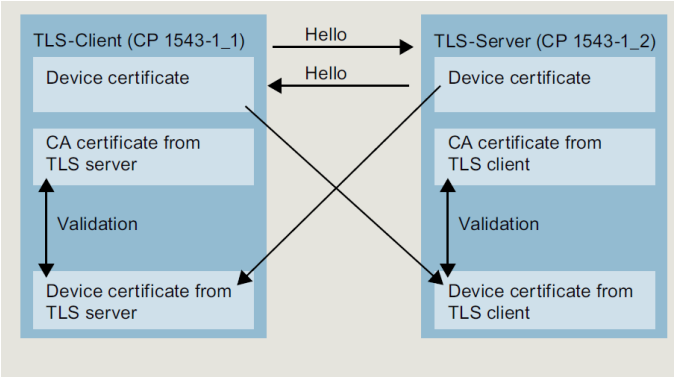

Figure 19: Secure PLC-PLC Communications

Intrusion Detection

One normally expects intrusion detection to be at the network layer instead of in the PLC. However, with some application creativity and certain features of the PLC's fieldbus protocol (used to communicate to the PLC's I/O system), intrusion detection functionality can be realized. In order to accomplish this, the features of the fieldbus protocol must be able to provide network information about the devices that are

connected to the communications ports of the PLC. In this example, the PROFINET protocol is used to provide the network name and network configuration of connected devices. This provides the PLC with a form of "whitelisting" where it can monitor and compare the devices attached to the same network as its network ports. If a "rogue" device is present, an alarm can be generated. If a sophisticated attacker attempts to spoof a device, instructions exist that can read additional device information. This includes the manufacturer, the serial number, the hardware revision, the firmware revision, etc. These elements can be used to further qualify a node on the network. Finally, PROFINET devices have a user configurable Identification and Maintenance data area that is typically used for asset management at a site. This data is customer specific, not manufacturer specific. This data can be used as another qualifier of the node on the network. These features combined make a very effective intrusion detection system. Figures 20 and 21 are examples of the logic calls and the data structures.

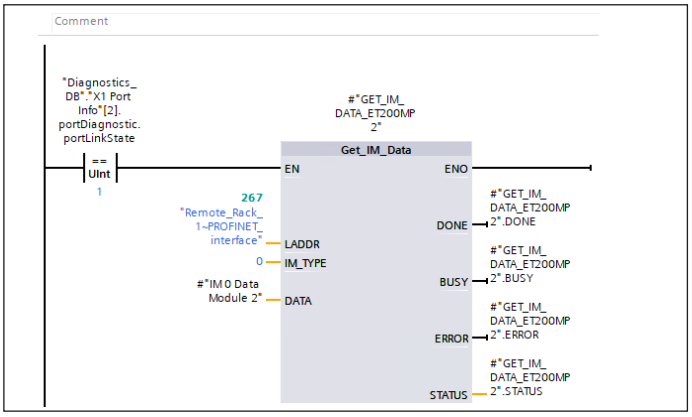

Figure 20: PLC Node Data Instruction

IM 0 Data Module 2	IM0_Data
Manufacturer_ID	UInt
Order_ID	String[20]
Serial_Number	String[16]
Hardware_Revision	UInt
Software_Revision	IM0_Version
Revision_Counter	UInt
Profile_ID	UInt
Profile_Specific_Ty...	UInt
IM_Version	Word
IM_Supported	Word
IM 2 Serial Number	String[16]
X1 Interface Info	"LPNDR_typeInterfaceInformation"
X1 Port Info	Array[1..8] of "LPNDR_typePortInformation"
X1 Link State	Array[1..8] of "LPNDR_typePortLinkState"

Figure 21: PLC Node Data Structure

Authentication Support

In the network section of this document, a RADIUS server was mentioned as a method for authenticating communications. Support for RADIUS servers has also been moved into the PLC's security components. Radius support is achieved by simply configuring the network credentials of the RADIUS server and then selecting it from a list for the security device. Figure 22 shows this.

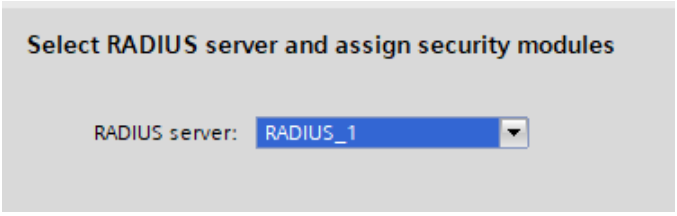

Figure 22: PLC Radius Server Selection

Security Logging

A requirement for the security of a PLC is that it must be able to report that it is under attack, has been attacked, or has been compromised. It must do this reporting without affecting its operation. One common method of causing a denial of service of a PLC is to cause so many errors that its processing of those errors prevents it from its normal automation processing. To protect against this, the PLC has configuration parameters that allow it to summarize like error messaging into a single message at a specific time interval. For example, if a PLC were under an automated attack where a program was attempting to break its 30-character password, the PLC would report only one error message every X seconds where X is a preset time interval. This provides the necessary reporting but doesn't consume all the PLC's processing capability. Figure 23 shows the configuration screen.

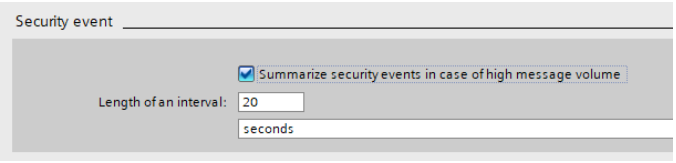

Figure 23: PLC Security Error Management

A PLC can provide two types of security logs. If used, its security communications processor can provide data to a SYSLOG server. In addition, it also logs messages to an internal diagnostics buffer. These security events can be captured by the PLC program which then can make them available to an HMI/SCADA device or perform some action based on the type of event.

The following list is an example of the types of security messages that the PLC will report in its security log.

- Going online with the correct or incorrect password
- Manipulated communications data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password lockout
- Timeout when an existing online connection is inactive

- Logging in to the Web server with the correct or incorrect password
- Creating a backup of the CPU
- Restoring the CPU configuration
- During startup:
  - Project on the memory card has changed (the memory card remains the same)
  - The memory card was replaced

Protecting Aging Infrastructures

Programmable Logic Controllers have been used since the late 1960s albeit they have changed considerably over the years. However, it is still commonplace to find PLCs being used that were manufactured more than 30 years ago. Security for PLCs in their early years consisted of a key. A key that fit all models of the same product family. The need for security, as we see it in today's world, was not imagined. There is a need to protect these legacy automation systems.

No one expects that modern security features will be added to these "ancient" devices because some of the company's that produced them are no longer in business. The recommended solution for these systems is to physically and logically isolate them using security appliances. A security appliance is a stand-alone network device that will provide cyber protection features. Figure 24 is an example of a security appliance that can be used.

Figure 24: SCALANCE S industrial security appliances offer protection of devices and networks in discrete manufacturing and in the process industry by protecting industrial communication with mechanisms such as stateful inspection firewalls as well as virtual private networks (VPNs)

HMI/SCADA

Automation systems consist of more than a Programmable Logic Controller. In this document, we have mentioned briefly HMI/SCADA devices (commonly called HMI or SCADA systems). These devices typically operate under non-real-time operating systems such as Microsoft embedded operating systems, various Microsoft operating systems up to and including Server, or LINUX operating systems. An additional document is required to present the security capabilities of these automation products.

Conclusion

This document has presented multiple security features for automation systems starting with plant security down to the automation controlling device. It has presented a feature suite, that when combined with plant and network security, can be used to create a very secure automation solution using Defense In-Depth practices. A secure automation architecture is only part of a holistic security solution though. Security standards must be used that include physical protections, security policies, security audits, continuous improvement strategies, and other recommendations in accordance with accepted security standards.

References

1. National Institute of Standards and Technology Document 800-82 Revision 2

Biography

Wayne Cantrell is a Senior Principal Systems Engineer with the Factory Automation and Government Technology divisions of Siemens Industry Inc. He has 37 years of experience in the factory automation industry including manufacturing, system test management, systems integration, and automation architecture design. He has a Bachelor of Science degree in Computer Science from East Tennessee State University.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. For more information about industrial security, please visit:
https://www.siemens.com/industrialsecurity

Published by
Siemens Industry, Inc. 2021

Siemens Industry, Inc.
100 Technology Dr.
Alpharetta, GA 30005

usa.siemens.com