



Securing your PlantPAx system in The Connected Enterprise

Alignment with IEC 62443-3-3 prioritizes availability – and addresses risk.

Introduction

Integrating Industrial Automation and Control Systems (IACS) with enterprise-level systems enables better visibility and collaboration, which help improve efficiency, production and profitability. But greater connectivity also exposes control systems to additional cybersecurity risks.

No doubt, cybersecurity is critical for every industrial operation. However, there is a marked difference in priorities between a standard IT system and an IACS. Availability is the most crucial aspect of a secure IACS. Conversely, data confidentiality and integrity take precedence in a standard IT environment. Therefore, using security standards from IT will not fully suit most plant's requirements.

To meet the needs of industrial environments, Rockwell Automation aligns systems developed on our technology with international standard ISA-99/IEC 62443-3-3. This standard is designed specifically for Industrial Automation and Control Systems and defines procedures to implement an electronically secure system.

This paper demonstrates how Rockwell Automation PlantPax®, a modern distributed control system (DCS), addresses cybersecurity based on the IEC 62443-3-3 standard.

Why IEC 62443-3-3?

By aligning PlantPax with IEC 62443-3-3, Rockwell Automation has committed to following global cybersecurity best practices based on defense-in-depth. The National Institute of Standards and Technology (NIST) and the US Department of Homeland Security¹ also recommend a defense-in-depth approach.

As the term implies, a defense-in-depth strategy is based on the notion that any one point of protection will likely be defeated. Cybersecurity systems based on this strategy establish multiple layers of protection through a combination of physical, electronic and procedural safeguards.

The IEC standard directly supports the defense-in-depth approach through its seven Foundational Requirements (FR) for securing an IACS:

FR1: Identification and authentication control (IAC)

FR2: Use control (UC)

FR3: System integrity (SI)

FR4: Data confidentiality (DC)

FR5: Restricted data flow (RDF)

FR6: Timely response to events (TRE)

FR7: Resource availability (RA)

These Foundational Requirements are the cornerstone for the IEC standard and compliance – and will be referenced and defined throughout this document.

The first step to securing your system

Cybersecurity is an ongoing process, not a product or policy. And the first step in that process is evaluating the specific security risks at each site within your organization. IEC 62433-3-2 provides guidance on how to identify your risk tolerances and vulnerabilities.

Keep in mind, you may find that different areas in your system have different security needs. For instance, a computer in a demilitarized zone getting patch updates may have less security risk than the primary processor running a turbine program.

To meet diverse requirements, IEC 62443 has established security levels SL0 to SL4. The security levels are suited to scenarios ranging from systems that do not require specific security measures to those that require protection against intentional, sophisticated threats. The IEC 62443-3-3 standard outlines cyber features that must be included to meet each system security level.

For more information on risk assessments, logical zones and security levels, see the Rockwell Automation [System Security Design Guidelines](#) reference manual.

Following the foundational requirements

To establish a secure PlantPAX system, Rockwell Automation uses IEC 62443-3-3 Foundational Requirements (FR) as a reference. Rockwell Automation also adheres to industrial cybersecurity best practices – and follows additional standards to address specific application requirements.

Where to begin? Although system availability is critical to any IACS, a secure system must first limit access to intended and qualified users.

In line with defense-in-depth, access is controlled through both physical and operational layers of security.

A word about physical security

In any system, the first layer of protection is achieved through multiple physical means.

- **Passive physical security devices**

Passive physical security devices include fences, walls, concertina wire (barbed wire, razor wire, and so on), anti-vehicle ditches, concrete barriers, earthen walls or mounds, and other access-limiting devices. They are used to either help protect physical entities or help prevent access to specific locations. Passive security devices are active *at all times*. These devices require no manual intervention to either engage or disengage.

- **Active physical security devices**

Active physical security devices engage or disengage based on time intervals, autonomous control or specific interventions from outside sources. These devices include doors, locks of various types, gates and retractable road obstructions.

- **Identification and monitoring devices**

This category includes still and video cameras, motion sensors, vibration sensors, heat sensors, biometric authentication or recording devices and a variety of other devices. These devices do not specifically control or limit access to a physical location or system by themselves. Their design and intended use is to detect, identify or record physical entities.

Operational access controls

Expanding on a defense-in-depth approach, IEC 62443-3-3 includes sections specifically dedicated to operational access controls. The IEC 62443-3-3 framework begins with FR1: Identification and authentication control and FR2: Use control. Below are the actual IEC 62443-3-3 requirements related to this topic:

IEC 62443 – FR1: Identification and authentication control (IAC)	IEC 62443 – FR2: Use control (UC)
Human user identification and authentication	Authorization enforcement
Unique identification and authentication	Authorization enforcement for all users
Software process and device identification and authentication	Permission mapping to roles
Account management	Wireless use control
Identifier management	Use control for portable and mobile devices
Authenticator management	Mobile code
Wireless access management	Session lock
Unique identification and authentication	Remote session termination
Strength of password-based authentication	Auditable events
Public key infrastructure certificates	Audit storage capacity
Strength of public key authentication	Response to audit processing failures
Authenticator feedback	Time stamps

PlantPax DCS response to FR1 and FR2

HUMAN USERS AND NON-HUMAN USERS

Authentication and identification apply to more than just human users. PlantPax can address both human and non-human interactions with operational access controls.

User access

Proper consideration must be given to any human interaction into a system. Security based on predefined roles and operation interfaces should be established. Listed below are typical human-machine interfaces:

System operation role	Operation interface
Operators	Operator workstation (OWS)
Operating supervisors	Operator workstation (OWS)
Maintenance	Engineering workstation (EWS)
Maintenance supervisors	Engineering workstation (EWS)
Engineering	Engineering workstation (EWS)
Managers	External access (process reports)
Administrators	Internal IT infrastructure

Each user should have a unique system account and assigned system role. This account is used to provide several levels of permissions, from general computer resources usage to detailed system operation and configuration. All users receive an interactive logon message describing the restricted system access and the implications of disobeying this direction.

The PlantPAX system integrates Microsoft® Active Directory™ technology within the Rockwell Automation FactoryTalk® platform to provide full system access control. The PlantPAX system also provides operation access control by process area or zone, achieving operation segmentation via FactoryTalk® Security.

Password-based authentication strength and unsuccessful login attempts are fully configurable in the system, including multi-factor authentication as an option.

The PlantPAX system integrates Active Directory Certificate Services (AD CS) to create a Certification Authority (CA) with Microsoft Network Policy and Access Services (NPAS). NPAS provides the Network Policy Server (NPS) responsible for the Remote Authentication Dial-In User Services (RADIUS). RADIUS integrates the operation of the wireless and external access infrastructure (802.1X wireless or wired connections).

PlantPAX takes advantage of services like Active Directory, FactoryTalk Security and Public Key Infrastructure (PKI) to implement identification and authentication.

Least privilege

Least privilege means allowing applications and users to access only the bare minimum number of processes required to operate correctly. Managed services accounts are created in the system to provide least privilege to execute the desired functions.

The PlantPAX system can enforce access authorizations supporting segregation of duties and least privilege for humans, software processes and devices (including wireless technology) within predefined roles.

Keep in mind, a modern DCS offers support and delivery flexibility. Therefore, at multiple points during the system lifecycle, various authorized parties will need limited access. Creating and managing least privileged accounts for these service providers is a best practice that adds a level of security – and helps maintain secure access for the right people at the right time.

Time sync

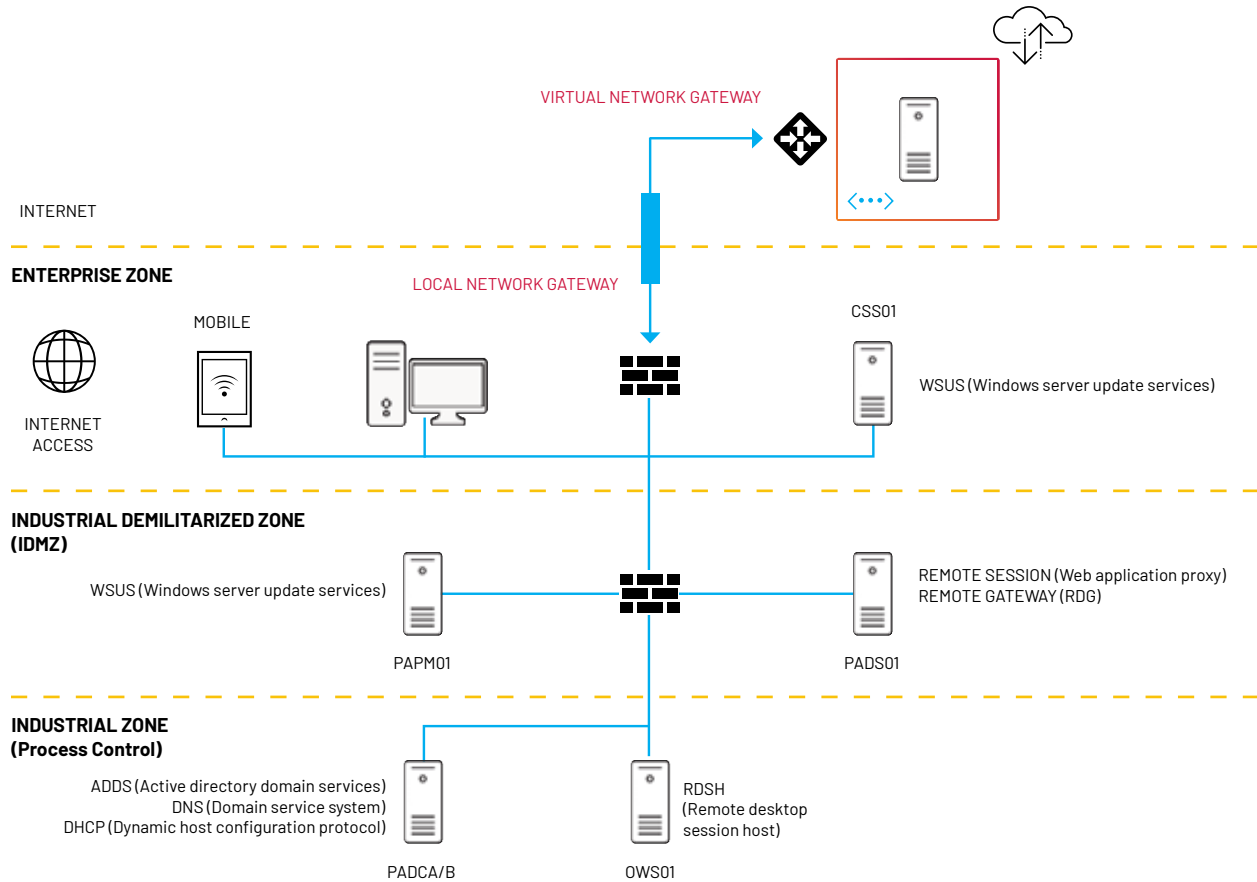
The PlantPax system provides time synchronization strategies for (1) Network Time Protocol (NTP) between computers and network infrastructure devices and (2) Precision Time Protocol (PTP) to automation devices. The PlantPax system also provides guidelines to external NTP sources where it is possible to choose Global Positioning System (GPS) and other strategies. Trusted time stamps are required for quality audit events.

Session lock

The PlantPax system can be configured to lock or terminate a remote session after a period of time. This can be accomplished with both Rockwell Automation ThinManager® controls and through the FactoryTalk Idle Detect utility.

Restricted data flow – zoning

Since distributed control systems span multiple plant areas and equipment types, layered topologies and network integration are common. Furthermore, since these systems generally have long lifecycles, the supported network integrations will likely see multiple infrastructure updates and modifications over a typical deployment. Therefore, designing proper topologies and workflows at the outset will help mitigate loopholes and potential security risks that could be introduced by future modifications.



Listed below is the IEC 62443-3-3 Foundational Requirement related to restricted data flow:

IEC 62443 – FR5: Restricted data flow (RDF)
Network segmentation
Physical network segmentation
Zone boundary protection
Deny by default, allow by exception
General-purpose person-to-person communication restrictions
Application partitioning

PlantPax DCS response to FR5

Network segmentation

The PlantPax network infrastructure uses virtual local area networks (VLANs) to create **logical segmentation**. VLANs decrease network exposure, reduce the broadcast domain and maintain critical control data in the same subnet. When required, routing enables access from different subnets, such as those normally used to maintain the control system.

Physical network segmentation is used when isolation is desired by design. For example, typically a safety instrumented system (SIS) will use physical network segmentation. This architecture decision should be discussed during the risk analysis phase, which will determine if any part of the control system must be decoupled from the rest of the network.

PlantPax DCS provides segmentation flexibility by allowing a control system to be physically or logically decoupled. System components can be shared or isolated depending on requirements.

The PlantPax system maintains typical reference architectures, which can scale according to application requirements. Critical system services are provided with a redundancy option from Dynamic Host Configuration Protocol (DHCP), Dynamic Name Server (DNS) or application servers, such as the HMI server, data server, alarms and historian server.

Zone boundaries and monitoring

In situations where untrusted networks are part of the system, PlantPax creates a zone boundary by implementing industrial-level firewalls. Typically, this is accomplished by using the Allen-Bradley® Stratix® 5950 security appliance and firewall.

The problem with air gaps

Creating an “air gap” between network connections is one popular way to physically isolate a system. In theory, an air gap is designed to keep network connections physically separated from the outside world. In reality, creating the barrier and maintaining it over time is challenging.

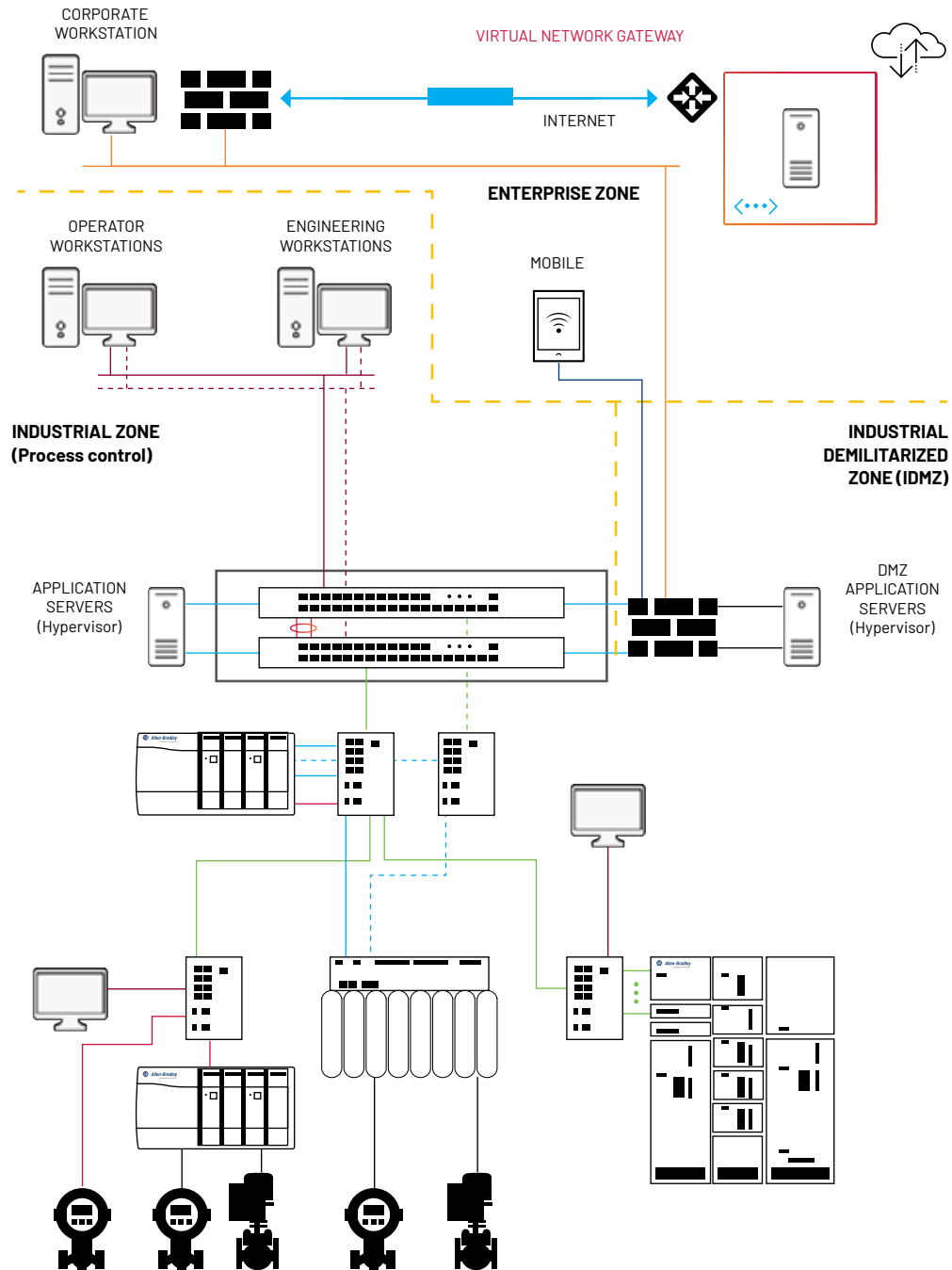
In other words, a system that is “air gapped” is not necessarily secure.

Why? Isolation methods based on air gaps require the continual maintenance of patches, firmware and potentially, even wireless network adapters. At a minimum, an isolated system forces creative workarounds by the very staff meant to maintain and use it. Ultimately, the result is greater risk.

For a far more manageable solution, choose alternatives – such as data diodes or physical port blocks controlled by physical keys on ICAS elements.

Wireless and external communication connections are monitored and controlled through the Industrial DMZ firewall. The firewall is configured to allow access by exception according to PlantPax guidelines.

The PlantPax system can be configured to not allow email services, social media or any messaging system that permits transmission of any type of executable file.



System integrity and data confidentiality

Data integrity is the assurance that the delivered data comes from a trusted source in a trusted way. Confidentiality is a key component of data integrity. This means that data cannot be read by prying eyes, and only by those who specifically know how to decrypt the data. System integrity is also critical. Despite physical safeguards and logical segmentation, a breach could still occur.

The requirements listed below are designed to help maintain both system integrity and data confidentiality – and the secure transfer of data from one system to another:

IEC 62443 – FR3: System integrity (SI)
Communication integrity
Malicious code protection
Malicious code protection on entry and exit points
Security functionality verification
Software and information integrity
Input validation
Deterministic output
Error handling
Session integrity
Protection of audit information

IEC 62443 – FR4: Data confidentiality (DC)
Information confidentiality
Protection of confidentiality at rest or in transit via untrusted networks
Information persistence
Use of cryptography

PlantPax DCS response to FR3 and FR4

Monitor and report vital changes via FactoryTalk AssetCentre

FactoryTalk® AssetCentre monitors and reports any changes in source code across the control system, including devices. FactoryTalk AssetCentre delivers the following features to assist in security management:

1. Provides secure access to the system.
2. Tracks detailed user actions.
3. Automatically tracks firmware versions.
4. Manages historical versioning of any electronic file.
5. Provides automatic backup and compares operations on supported devices.
6. Adds backup and compares plug-ins for third-party vendor devices.
7. Configures process instrumentation.
8. Manages instrumentation calibration schedules and certificates.
9. Shows the latest asset lifecycle status via the Asset Inventory Agent, which can connect with the Product Compatibility and Download Center.

FactoryTalk AssetCentre leverages FactoryTalkSecurity to administrate access – and to create policies outlining who can access which FactoryTalk AssetCentre tools and features.

FactoryTalk AssetCentre allows scheduled searches of audits, events, diagnostics, and more – including specific times that staff may implement unsafe programming practices (for instance, at the end of shifts). It also allows unscheduled searches, which may be used when a system goes down unexpectedly.

Prevention of non-authorized software

To prevent usage of non-authorized software tools, the PlantPAX system allows the blocking of external storage devices. All PlantPAX computers have predefined, built-in, firewall rules that provide the “least functionality” required to operate along with a “least privilege” design. As a result, every module only has access to information for a legitimate purpose.

Along with firewalls, PlantPAX systems include Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) functionality, which is built into the Stratix 5950 security appliance. FactoryTalk AssetCentre monitors code for any changes.

Antivirus software or similar technology is also expected to be part of the system deployment and management.

Input and output validation

Rockwell Software products provide input validation as part of intrinsic quality control. The control system application is responsible for input validation, which is an out-of-box feature when using the Rockwell Automation library of process objects.

Deterministic output is included in select Rockwell Automation products. These products can operate in safe mode when the system process controller is unavailable due to a system fault or loss of communication.

Data at rest

As noted throughout this paper, protecting data integrity when data is moving between systems is critical. But it is also important to keep data confidential when at rest. Encrypted drives are the recommended way to achieve this goal. Disabling smart card usage in controllers is also recommended to help maintain data confidentiality.

In a PlantPAX system, critical data is stored in Microsoft® SQL Server. The asset management tool must query and store data, and users must have no direct access to the database.

PlantPAX reference manuals include instructions on how to configure data access using Active Directory. In a PlantPAX DCS, data access is protected by Active Directory domain groups, and policies are integrated with the asset management tool. The asset management tool provides granular access restrictions.

Auditing capabilities and event management

A detailed operation audit capability is part of the FactoryTalk platform. The audit reporting capability is available to authorized user groups in read-only mode. Listed below is the Foundational Requirement that applies to auditing capabilities and event management:

IEC 62443 – FR6: Timely response to events (TRE)
Audit log accessibility
Continuous monitoring

PlantPax DCS Response to FR6

Audit data retention follows the application requirement – and does not allow a user to change or delete any system event in a pre-defined time period.

System audit policy services run continuously and cannot be disabled during system operation.

System management

System management begins with taking a defense-in-depth approach. In particular, building a system that is robust enough to maintain operation despite resource limitations is critical. In addition, resource availability is a primary concern and must be included in system design considerations. Listed below is the related IEC 62443-3-3 requirement:

IEC 62443 – FR7: Resource availability (RA)
Denial-of-service protection
Manage communication loads
Resource management
Control system backup
Backup verification
Control system recovery and reconstitution
Emergency power
Network and security configuration settings
Least functionality
Control system component inventory

PlantPAx DCS response to FR7

Critical operation and availability

A PlantPAx system can operate in a degraded mode during a denial-of-service (DoS) event. If this functionality is required, the system will need additional control hardware and software to provide the emergency mode of operation. Depending on requirements, firewalls and switch configurations can throttle network access.

PlantPAx network infrastructure also enables storm control. General network guidelines are provided in the PlantPAx user manual to help users choose an appropriate setup that will not interfere with the application.

During design, users must consider the implications of power loss or power failure. Emergency power alternatives may be required, such as redundant power supplies for infrastructure and control devices.

Resource management

The PlantPAx user manual outlines resource management techniques for the following topics:

1. Virtualization
2. Application Servers
3. Process Control

Patch management

- **Operational system**

The PlantPAx system integrates Windows Server Update Services (WSUS) and the active directory group policy manager – and supports patch management deployment. Windows Patch Management Strategies should be part of end-user policies and procedures. The WSUS service shall run in the Industrial DMZ. The patch deployment model should be synchronized with production and operated under supervision.

- **Rockwell Automation security updates**

Rockwell Automation security updates are available through security advisories. Users are highly encouraged to sign up for the Industrial Security Advisory Index or Product Notice Email Notifications (Knowledgebase Tech Note: KB 58870).

Users are also encouraged to create a Rockwell Automation Software Update file server location as a repository in the Industrial DMZ. The software update deployment model should be synchronized with production and always manually executed.

Firmware management

- **Rockwell Automation devices**

Security-related firmware updates for Rockwell Automation devices are available through the security advisories noted above – the Industrial Security Advisory Index or Product Notice Email Notifications.

The Rockwell Automation® ControlFLASH™ tool is used to update device firmware. Firmware update deployment should be synchronized with production and always manually executed.





Conclusion

Taking advantage of innovations created by The Connected Enterprise is vital to the future of a Modern DCS. Improvements in production and profitability are quickly giving advantage to the early adopters of more connected production environments. As you move toward a Connected Enterprise, you must seriously consider how best to protect your system.

Unfortunately, security is not just an off-the-shelf product and a Defense in Depth approach is needed. To execute properly, a secure system requires active intervention, thoughtful design, and maintenance.

The techniques presented in this paper provide only the introductory framework required to implement a secure system. Additional details are available in various documents created for PlantPax DCS. Know that Rockwell Automation domain experts are also available to provide insight – and help you adopt a security policy as part of your system’s lifecycle.

¹The following publications address defense-in-depth: [NIST Special Publication 800-82](#) and the US Department of Homeland Security/[Idaho National Laboratory Report INL/EXT-06-11478](#).

Connect with us.    

rockwellautomation.com ————— **expanding human possibility™**

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Allen-Bradley, ControlFLASH, Expanding human possibility, FactoryTalk AssetCentre, FactoryTalk Security, PlantPax, Rockwell Automation, Stratix and ThinManager are trademarks of Rockwell Automation, Inc. Microsoft, SQL Server and Active Directory are trademarks of Microsoft, Inc. Trademarks not belonging to Rockwell Automation are the property of their respective companies.

Publication PROCES-WP024A-EN-P - August 2019

Copyright © 2019 Rockwell Automation, Inc. All Rights Reserved. Printed in USA.