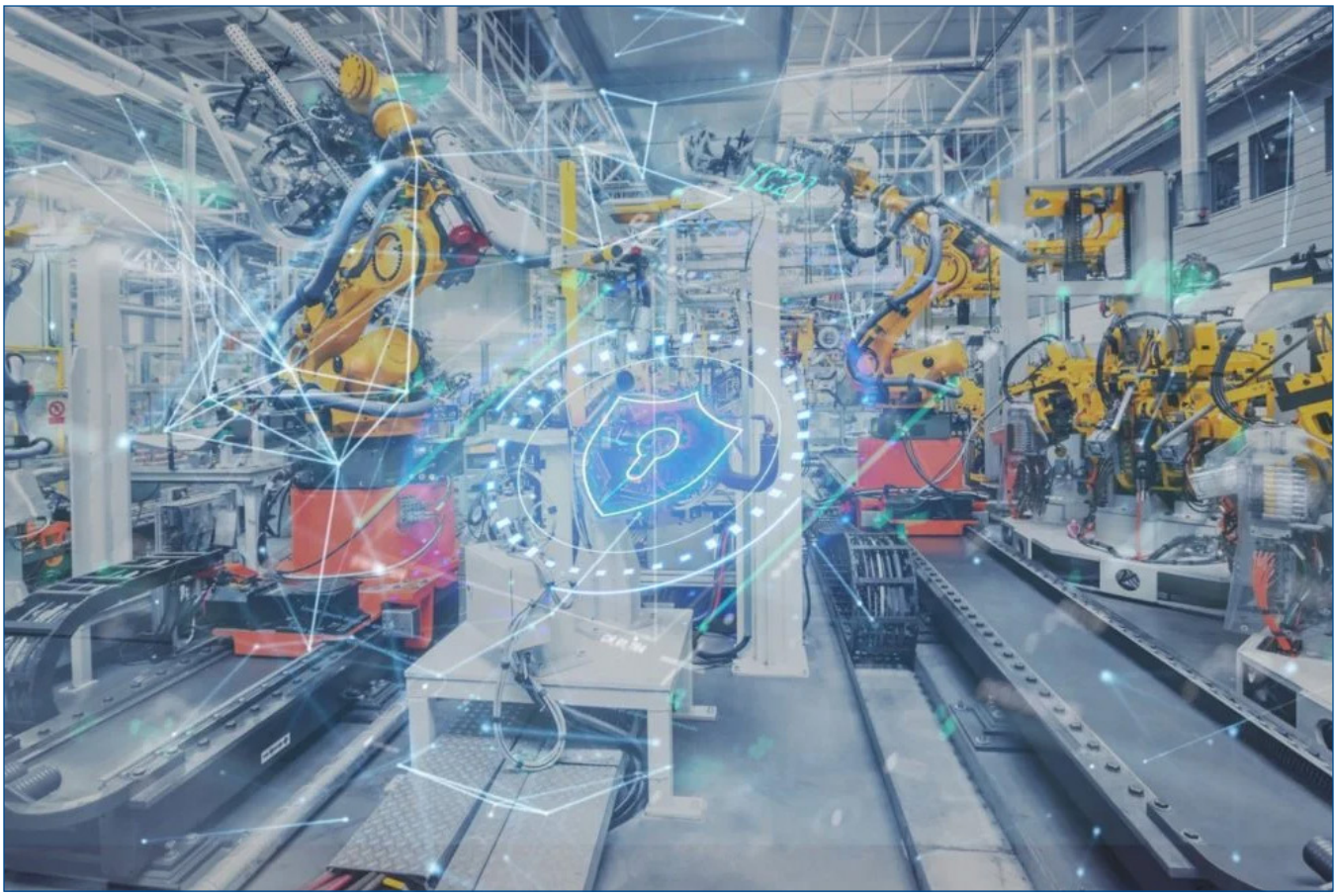
Industrial Security in SCADA Systems: IEC 62443-3-3 Certification



EMERSON

Table of Contents

List of Abbreviation

ACL	Access Control List
CR	Component Requirements
DCS	Distributed Control Systems
DMZ	Demilitarized Zone
ESD	Emergency Shutdown System
ES	Engineering Station
FR	Foundational Requirements
FTP	File Transfer Protocol
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ML	Maturity Level
OS	Operator Station
PDCA	Plan Do Check Act
PLC	Programmable Logic Controller
RE	Requirement Enhancement
SCADA	Supervisory Control and Data Acquisition
SR	System Requirements
SL	Security Level
TCP	Transmission Control Protocol
VPN	Virtual Private Network

Terms & Definitions

Asset Owner	An individual or a company owning a physical or logical object having either a perceived or actual value to the industrial automation control system.
Attack	Assault on a system that stems from a deliberate attempt to evade security services and violate the security policy of a system.
Authentication	Security measure designed to verify the identity of a user, process or device, often as a prerequisite to allowing access to resources of information.
Automation Systems	Control systems (e.g., DCS and SCADA) that are used to operate machines (e.g., boilers, turbines and instruments such as sensors and pressure transmitters) in a plant with minimum human effort.
Authorization	Right or a permission that is granted to a system entity to have access to a system.
Availability	Property of ensuring timely and reliable access and use of control system information and functionality.
Component Requirement	The requirements defined in the standard IEC 62443 that IACS components have to fulfill to attain the highest possible security.
Confidentiality	Protection of IACS data and information from an unauthorized access.
Demilitarized Zone	A perimeter network segment that is logically between internal and external networks for controlling data flow between the networks.
Firewall	Inter-network connection device that restricts data communication traffic between two connected networks.
Foundational Requirement	The requirements defined in the standard IEC 62443 that every IACS system or component must fulfill to attain security.
Host	Computer that attaches to a communication subnetwork or inter-network and can use services provided by the network to exchange data with the other attached systems.
Industrial Automation and Control System	Collection of personnel, hardware, software and policies involved in the operation of the industrial process that can affect or influence its safe, secure and reliable operation.
Integrity	Measure of assuring the accuracy, consistency and availability of information.
Information	An asset that is important for an organization's business. Information can be in digital form, paper form or in the knowledge of an organization's employees.
Maturity Level	The levels that define the benchmark of requirements defined in the standard IEC 62443.
Product Supplier	Manufacturer of a hardware and/or software product.
Security Gateway	A security relay mechanism that attaches two or more computer networks that have similar functions but dissimilar implementation, and enables host computers on one network to communicate with hosts on another network.
Security Level	Measure of confidence that IACS is free from vulnerabilities and functions in the intended manner.
Service Provider	Organization (internal or external, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement.
System Integrator	A person or a company that specializes in bringing together component subsystems into a whole and ensures that those subsystems perform in accordance with project specifications.
System Requirement	The requirements defined in the standard IEC 62443 that an IACS system has to fulfill to attain the highest possible security.
Vulnerability	Weakness in a system function, procedure, internal control or implementation that could be exploited or triggered by a threat source, intentionally designed into computer components or accidently inserted at any time during its lifecycle.

Purpose of this Document

- This white paper gives a brief explanation of the IEC 62443 standard and its procedures, and provides some suggestions and activities to make a Movicon.NExT SCADA/HMI platform-based project application compliant with the specifications defined in the IEC 62443 standard.
- This white paper was written to inform Movicon.NExT developers about the concepts and best usage of Movicon.NExT in applications subject to IEC 62443 validation.
- The Movicon.NExT platform has been audited and certified for IEC 62443-3-3 by Lloyd's Register. However, it must be noted that the product itself is not subject to IEC 62443 validation, but the context within which the project is created for may be. Notwithstanding this, Movicon.NExT, as a platform, has been specifically designed to support the IEC 62443-3-3 standard and thus simplifies the task of creating IEC 62443-ready projects.
- This white paper has no absolute value and is not in any way legally binding to Emerson. It is the customer's or the Movicon.NExT application designer's responsibility to make sure the developed application is compliant to IEC 62443 and any of its updated specifications. The purpose of this white paper is to suggest the best practices to interpret the standard for designing applications subject to IEC 62443 validation.

Movicon NExT Product Certification: IEC 62443-3-3

Movicon.NExT, the SCADA/HMI software platform, has been subjected to validation according to the IEC 62443-3-3 standard with the purpose of providing users, who need to operate safely in critical architectures subject to validation, a tool explicitly designed to guarantee the maximum level of security within SCADA environments.

Movicon.NExT was certified by Lloyd's Register Quality Assurance Srl, an authorized certification company, with validation audit conducted on the 20th, 23rd, and 24th of March 2020. LRC00001153 / 3547690 Rev 1 01/06/2020

Lloyd's Register

Assessment Statement

Lloyd's Register Quality Assurance Italy S.r.l. was commissioned by

Progea srl
Via G. D'Annunzio 295, Modena 41123, Italy

to assess the product features of

"Movicon.NExT™" version 3.4.270

according to the standard

IEC 62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.

Based on the evidence of the Assessment Visit conducted on 20, 23, and 24 March 2020 the product "Movicon.NExT™" version 3.4.270 has been found developed by taking into account the requirements of the mentioned IEC standard.
All detected issues were communicated to the Organization and documented in the audit report (LRC00001153 / 3547690 Rev 1 01/06/2020) to which reference is made for further details.

16/06/2020

Alberto Melis
Technical Manager

Introduction to the Concepts of Industrial Security

Critical infrastructures are becoming a potential target of cyberattacks as they increasingly connect with other networks. Manufacturers and operators of SCADA systems and industrial automation and control systems report increasing cases of cyberattacks on their systems. The reason behind this is the more popular a system is, the more lucrative the attack, as it can often be reused.

Interlinking of the enterprise and production networks and integrating the process control networks with web technologies such as Ethernet and TCP/IP have increased the need for security in the Industrial Automation Control System (IACS). This cross connection makes the critical system in the process control network open to the exploitation of these vulnerabilities (a cyberattack), which can cause the whole system to shut down and even affect the safety of the environment. There are several key differences with respect to the security between the traditional IT security environment and IACS security environment as shown in Table 1.

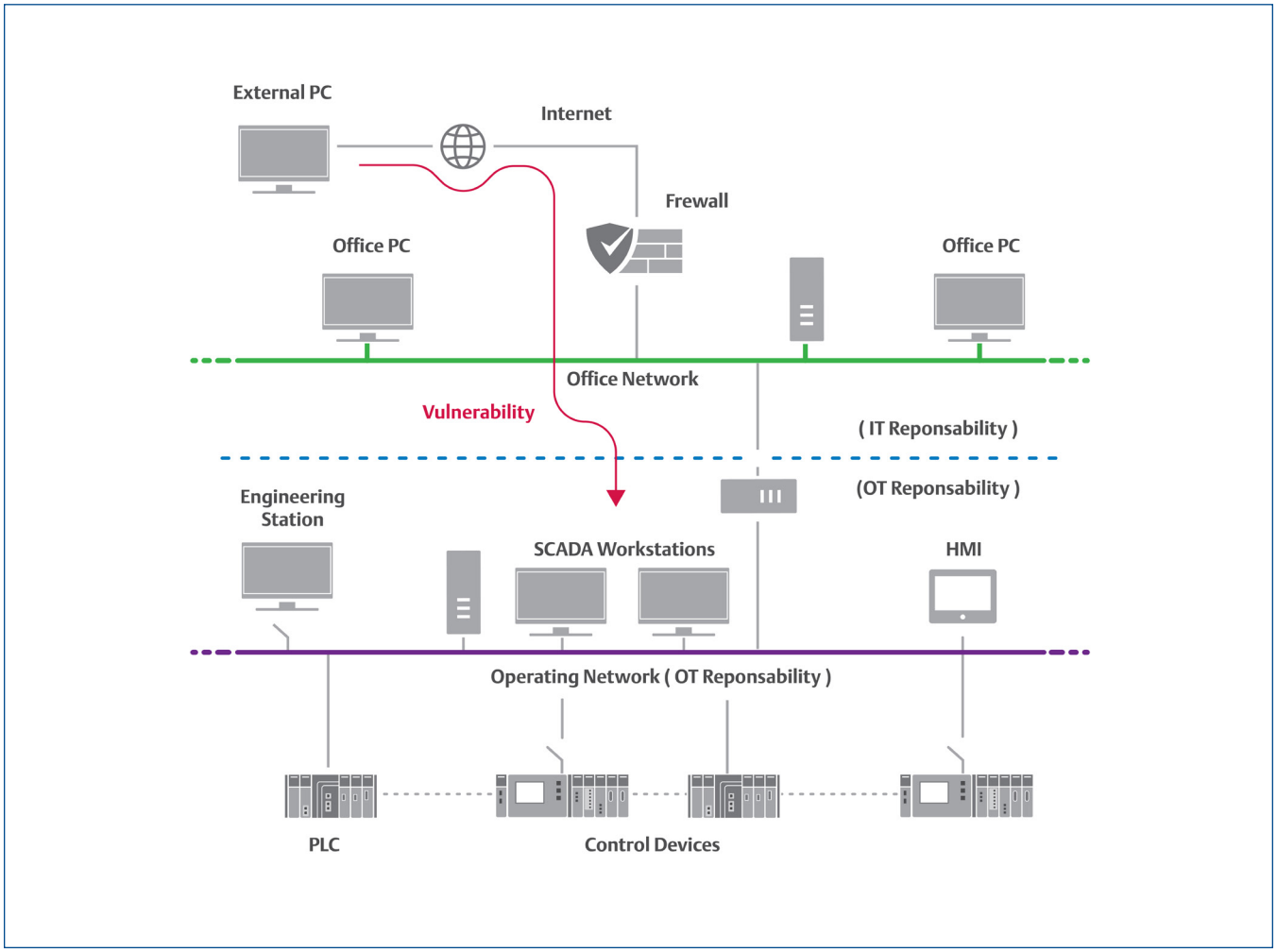
Security Topic	IT Systems	IACS Systems
Antivirus	Widely used and easily updated	Not always used, sometimes difficult to use
Life Cycle	3-5 years	5-20 years
Awareness	Good	Not good
Patch Management	Often	Rare, often approved by manufacturers
Change Management	Regular and scheduled	Rare
Evaluation of Log Files	Established practice	Unusual practice
Time Dependency	Delays accepted	Critical
Availability	Working hours, short failures accepted	24/7
IT Security Awareness	Good	Poor
Security Tests	Widespread	Rare and problematic
Test Enviroment	Available	Rarely available

Table 1: The Differences Between Traditional IT Security and IACS Security

Security Criteria

Due to the poor practice of different measures in IACS systems as compared with traditional IT systems, security in an IACS environment is challenging and important. The security in the IACS is considered to be securing the industrial plants from unauthorized physical and digital attack.

The attack in the IACS can be through the negligible or unintentional behavior from an employee; for example, when an employee tries to format the plant system during the production process and loses historical data. However, attacks are increasingly made off-site by hackers with the criminal intent to jeopardize the data integrity of the control system by stealing, changing, destroying or holding data at ransom by installing dangerous malware or injecting computer viruses.



The objective of industrial security is to fulfill three security criteria:

- Confidentiality
- Integrity
- Availability

In IACS, availability is given top priority to determine continuous system uptimes. This is followed by integrity and data consistency, and confidentiality.

Confidentiality is given less importance because data is often in raw form and needs to be analyzed within context before it has any value. Therefore, it is paramount that continuous running of production processes is guaranteed even in the event of, and independently from, a cyberattack or system failure.

The previous diagram shows the architecture of a typical IACS with a separate IT network (offices) and plant network (IACS). The interconnection between the office network and the IACS network shows how vulnerable the critical control systems are without any security measures implemented when connecting to the office network and the open world (internet).

In the information technology (IT) network, the standard procedure for protecting information against unauthorized access and unauthorized use is already a widely used and normal practice delegated under the supervision of IT managers, and also defined in the ISO 27000 standard.

However, at the operational level (operating technology), the same level of protection is lacking in the industrial networks that are increasingly more connected with the company IT systems. Often, inadequate security precautions are adopted without thoroughly taking into consideration the seriousness of the negative effects that a cyberattack can cause to production runs and plants, especially in the infrastructure industry.

The IEC 62443 standard concentrates on the protection of IACS information, devices and systems, typically used in industries and in infrastructure control systems.

The IEC 62443 Standard

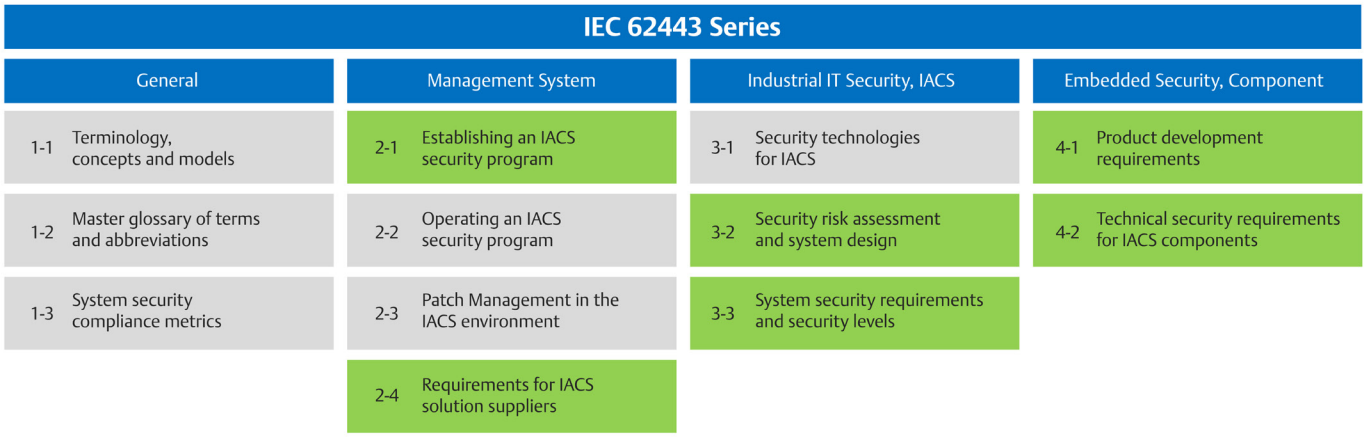
IEC 62443 deals with security of industrial control systems, commonly known as the “Industrial Automation and Control Systems.” The term IACS includes control systems used in the manufacturing and processing facilities, or in remote control systems – geographically distributed operations such as infrastructure plants for electricity, gas and water using automated, remote controlled or monitored assets.

The aim of the standard is to ensure that a product supplier, integrator or asset owner adopts efficient methods for secured processes with a focus on safety of the personnel and production, its availability, efficiency and quality of the IACS’s production, and safety of the environment.

How IEC 62443 is Structured

The IEC 62443 series is divided into four parts as listed below and shown in the diagram underneath:

- General
- Management System (policies and procedures)
- Industrial IT Security, IACS (system requirements)
- Embedded Security, Component



Basic Terminologies, Concepts and Abbreviations Used in the Standard

General:

Standard 62443-1-1 presents the concepts and models of the series.

- The technical report 62443-1-2 contains a glossary of terms and abbreviations used throughout the series.
- The standard 62443-1-3 describes a series of metrics derived from the basic requirements (FR) and system requirements (SR).

Management System (policies and procedures):

This describes the policies and procedures that are required and used to implement a cyber security management system.

- Standard 62443-2-1 describes what is required to define and implement an effective IACS cyber security management system. This standard is aligned with the ISO 27000 series.
- The standard 62443-2-2 provides specific guidance on what is required to operate an effective IACS cyber security management system.
- Technical Report 62443-2-3 provides guidance on the specific topic of patch management for IACS.
- Standard 62443-2-4 specifies requirements for suppliers of IACS.

Industrial IT Security, IACS (system requirements):

This describes the security requirements for a system in an IACS environment.

- The technical report 62443-3-1 describes the application for different safety technologies to an IACS environment.
- The standard 62443-3-2 addresses the risk assessment and the system design for IACS.
- Standard 62443-3-3 describes the basics of the security requirements and the security assurance level (SL).

Embedded Security, Component (component requirement):

This describes the security requirement of a component in an IACS environment.

- Standard 62443-4-1 describes requirements that apply to the development of physical products.
- The standard 62443-4-2 contains requirements that allow a detailed mapping of the system requirements (SR) to subsystems and components of the system under scope.

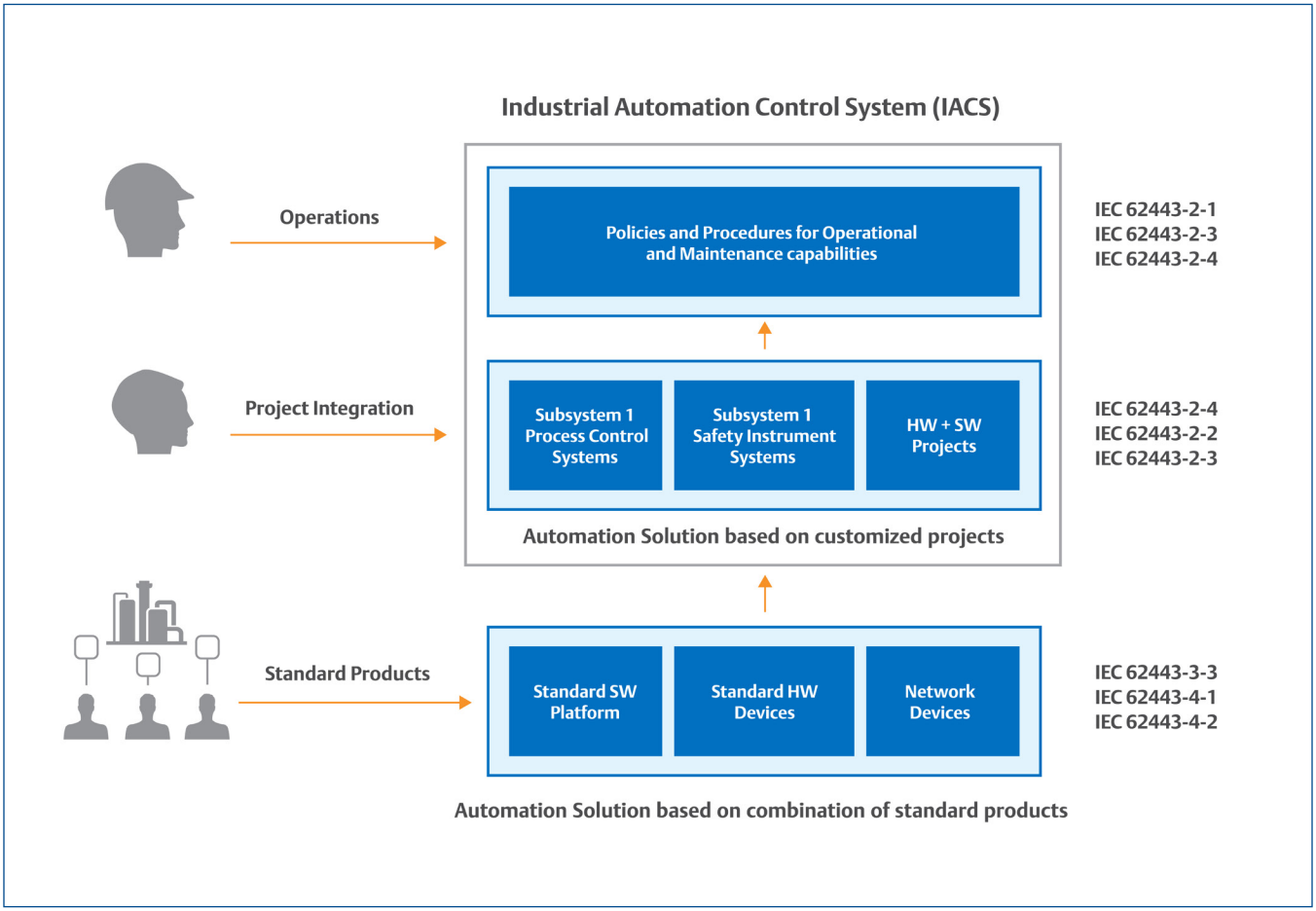
Roles and Scope of IEC 62443 in IACS

1. The product supplier

2. The system integrator

3. The asset owner

These roles are the basis for defining and connecting the different parts in the IEC 62443 series as illustrated in the diagram below:



This diagram illustrates how a product developed by the product supplier strictly relates to the configuration, installation and maintenance capability of the system integrator, while the overall system and its operation by the management of the asset owner (end user).

It also illustrates the role and relationship between the product supplier, system integrator and asset owner.

Responsibility of Roles

- The product supplier or manufacturer is responsible for the supply of a product – developed to be fully compatible with the requirements of the standard – by following the required levels of security (LS) and providing users with the appropriate instructions on correct product usage according to the security concepts defined in IEC 62443 3-3, IEC 62443 4-1, IEC 62443 4-2.
- System integrators are responsible for the integration and starting up an IACS automation solution of the product in conformance with the security levels (SL) required by the customer. They are responsible, unless otherwise indicated, for the development and testing of the control system, the control or supervision systems (SCADA, HMI), the engineering stations including the external security systems (antivirus, whitelisting, etc.), the security of devices connected in the field (PLC, DCS, etc.) and of network devices (firewall, router, switch etc.). They are also responsible for product integration and start-up by using processes compliant to IEC 62443 2-4, IEC 62443 3- 2, IEC 62443 3-3.
- Asset owners are responsible for operational and maintenance capabilities of their assets with the help of policies and the procedures defined in IEC 62443 2-1, IEC 62443 2-3 and IEC 62443 2-4 for the IACS developed and integrated by the automation solution provider and installed at a specific site.

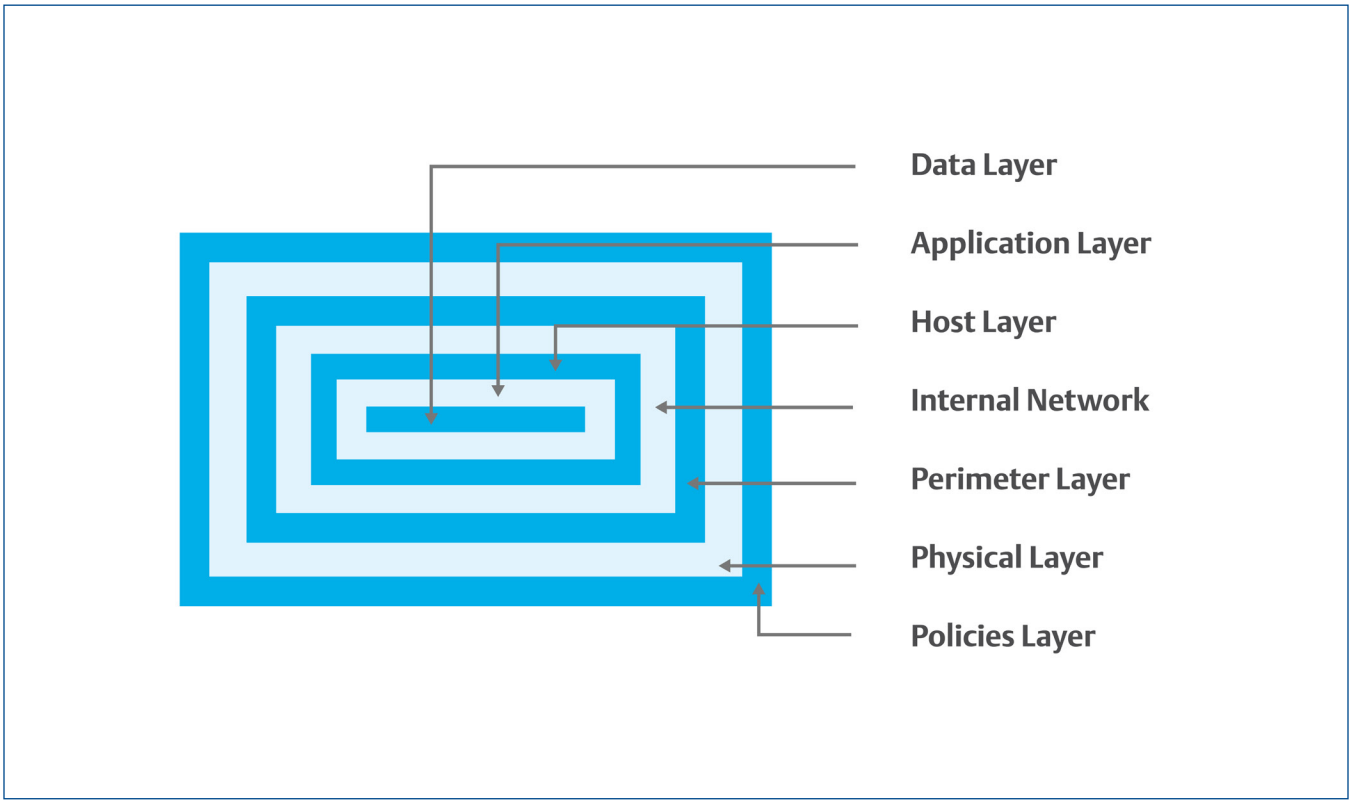
Concepts Used in IEC 62443

The general concepts used in the IEC 62443 standard are defined below.

Defense in Depth

Defense in depth is a layered security mechanism that enhances security of the whole system. The benefit of this mechanism is that during an attack, if one layer gets affected, other layers can keep assisting to protect against, detect and react to other attacks. The layers can be described as:

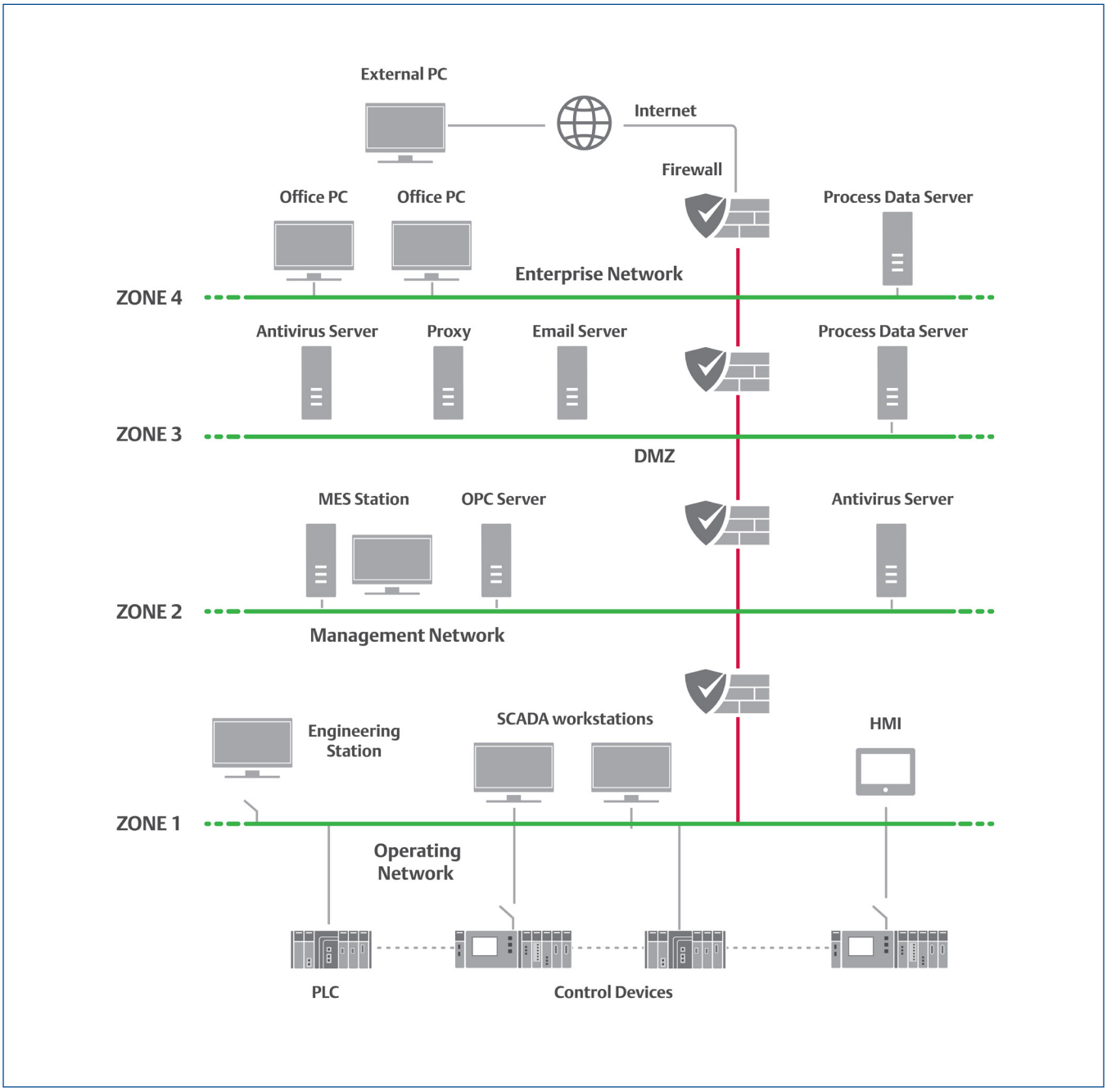
- Data Layer is the innermost layer and can be used for ACL and encryption of data.
- Application Layer is the next layer used for installing antivirus software and application hardening.
- Host Layer is used for the patch implementation of vulnerability detected and authentication of the users.
- Internal Network is used for IPsec (Internet Protocol Security) for IP communications, authentication and encryption of the packet that takes part in a communication system; IDS (Intrusion Detection System) detects the intrusion of every user (authorized or unauthorized).
- Perimeter Layer is used for implementing the firewalls and VPN quarantining.
- Physical Layer is the layer where the useful guards, switches, locks, ports and physical access are employed.
- Policies Layer is the outermost layer where the security policies and procedures for the IACS networks are defined.



Zones and Conduits

Security zones are physical or logical groupings of assets that share common security requirements and isolate the critical control systems components. A special type of security zone is the demilitarized zone (DMZ), which segments the external network with the internal (IACS) network with help of security components (e.g., firewall). This concept provides a layered security approach, with a “defense in depth” approach being taken into account.

“Conduits are the special type of security zone that groups communications that can be logically organized into information flows within and also external to a zone. It can be a single service (i.e., Ethernet network) or be a multiple data carrier.” [1-1]. Conduits control access to the zone by resisting several attacks like denial of service and malware attacks, and protects the integrity and confidentiality of the network traffic.



The previous figure illustrates the network architecture of an IACS network with zones and conduits. The network is segmented into four zones and each has a firewall or gateway protection. The zoning concept in an IACS network has to be in such a manner that the information transfer from the enterprise network should be a step wise (Zone 4 to Zone 3, Zone 3 to Zone 2, Zone 2 to Zone 1) process. The information can be antivirus pattern updates, patch updates, etc. The flow of information from Zone 1 to the other zones has to be restricted (read only function) and should be transferred only through a proper authentication method. For example, process data of the production network is only transferred to a process data server in the DMZ in Zone 3. Access to the process data server should be limited to authorized employees.

IEC 62443 3-3 and IEC 624434-2 Security Level Basis

The security level (SL) concept focuses on the zones of the IACS. SLs provide a frame of reference for making decisions on the use of countermeasures and devices with different inherent security capabilities. The concept can be used to select the IACS devices and countermeasures to be used within a zone and provides the ability to categorize risks for zone or conduits.

The SL may also be used to identify layered defense in depth strategy for a zone that includes hardware and software base technical countermeasures. The security levels defined for components are based on the four types of device categories in the standard (i.e., embedded device, host devices, network devices and application software). The security levels in the standard are defined as:

- SL1- Prevents the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL2- Prevents the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL3- Prevents the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL4 – Prevents the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No objective
SL2	Capability to protect against intentional violation using simple means with low resources, general skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL3	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical damage	Industrial specific	High	Aggressive

This table shows a summary of each security level with characterization of target, skills, motivation and means of attacks that can occur at each security level.

Maturity Levels on the Basis of IEC 62443 2-4 and IEC 62443 4-1

Maturity levels are based on the CMMI-SVC model. These levels define the benchmarks that are requirements defined by the standards IEC 62443 2-4 and IEC 62443 4-1. Each level is progressively more advanced than the previous level. The service providers and the asset owners are required to identify the maturity level associated with the implementation of each requirement.

Maturity Level	Category	Description
ML1	Initial	Capability of performing a service without a documented process that is poorly controlled
ML2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
ML3	Defined	Capability of performing ML2 level, including evidence of practicing the process (e.g., documented process) plus list of participants in the training of personnel
ML4	Improved	Capability of performing ML3 level, including demonstration of continuous improvement (e.g., internal audit report)

This table shows a summary of each security level with characterization of target, skills, motivation and means of attacks that can occur at each security level.

Project Process and Certification

An IACS project created in compliance with the IEC 62443 standard can be recognized as a project with an optimal level of cyber security.

Nevertheless, the IACS system can be subjected to certification by referring to a validation center approved and authorized by the certification agency for running tests according to IEC 62443.

The agency in charge will provide the appropriate tests to validate the whole IACS system according to the desired security level and the audit required by the validator, in compliance with the standards.

- Movicon.NExT is an IEC 62443-3-3 certified product and, therefore, facilitates the development of IACS systems ready for validation according to the standard.

The IEC-62443 Standard and Movicon NExT

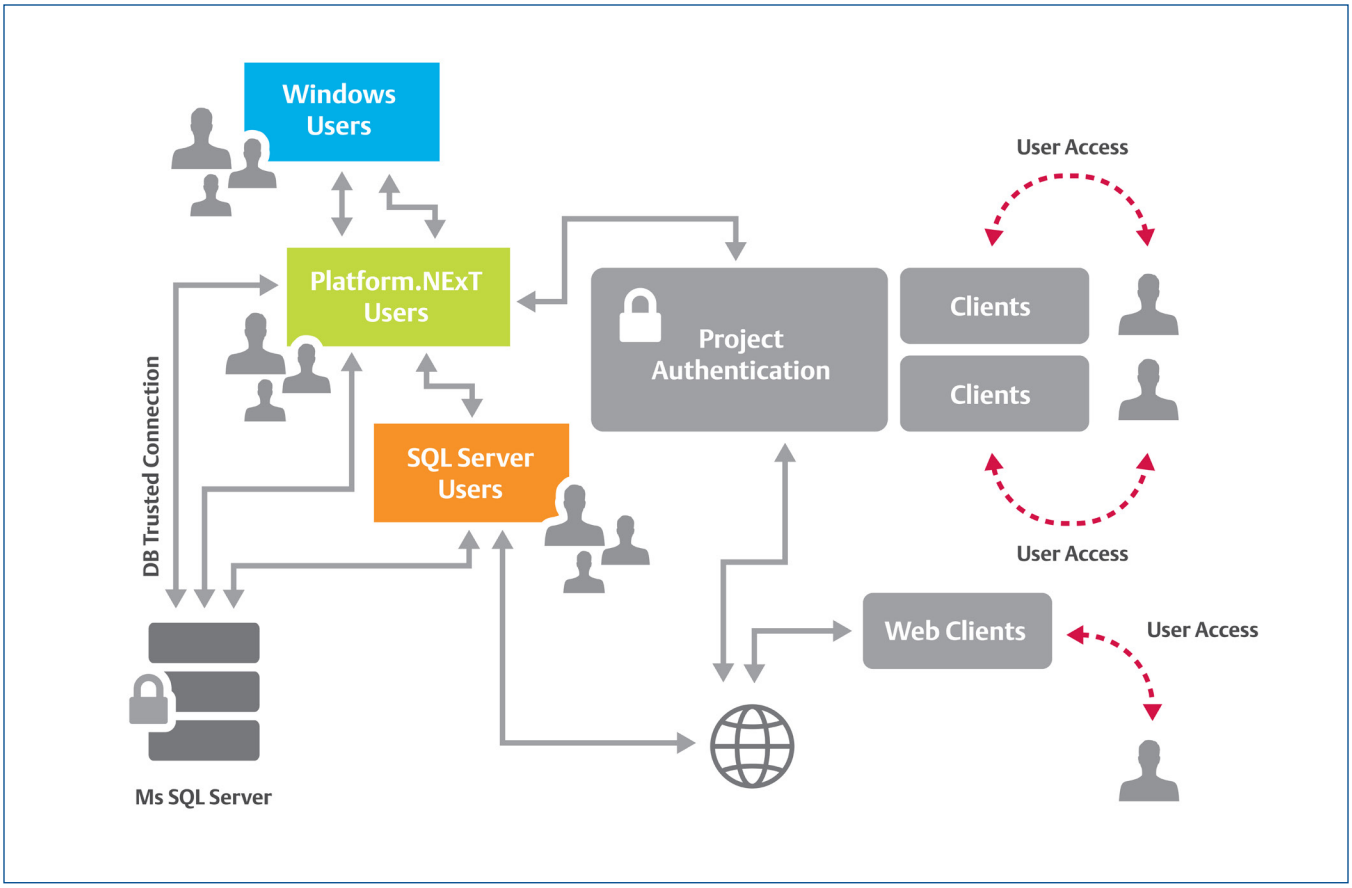
In compliance with the standard requirements, the designer should create a Movicon project that uses the features specifically provided by the Movicon.NExT software platform to guarantee security management in compliance with the standard's requirements.

The main concepts related to security management, intended as users management, system access and data integrity, are summarized in the functional concepts described in detail in the following chapters and in the product's documentation.

5.3 User Authentication and Identification

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the control system to support segregation of duties and privileges in accordance with applicable security policies and procedures.	Movicon.NExT securely manages the users' management and their authentication, allowing the designer to utilize user management to associate each applicable feature, such as a password level and user area. Movicon.NExT allows user authentication management in the client (front end) and the server security (back end) using the following connection concepts: – Local client/server (in case server and client run together) – Remote client/server (in circumstances where server and client run separately in a network). In such circumstances, the platform uses the OPC UA technology-based connectivity, and the data transport can be configured in the project. Maximum security can also be obtained by using cryptography and server and client authentication certificates. – Remote client/server on Windows Terminal Server (in circumstances where server and client run separately and connected through a terminal server or remote desktop). In this case, the connection security between the remote station and server/client is handled by the Windows OS and, therefore, delegated to the operating system's configuration. – Web client, for accessing the server using an HTML browser. The secure user authentication requires the web server configuration of Windows IIS using HTTPS and certificates. – Web client, for accessing the server using native APPs on Android or Apple iOS mobile devices. The native technology of the Movicon APPs allows the user access and authentication from mobile devices using HTTPS and WebSockets, with encrypted data.
	Memberships The Movicon user authentication process is managed by using the Windows membership technology to ensure it is extremely safe and independent from the system. The Movicon default provider is ASP.NET and uses an encrypted SQL Server database. The provider can also be set by the designer to support different authentication methods, such as biometric recognition.

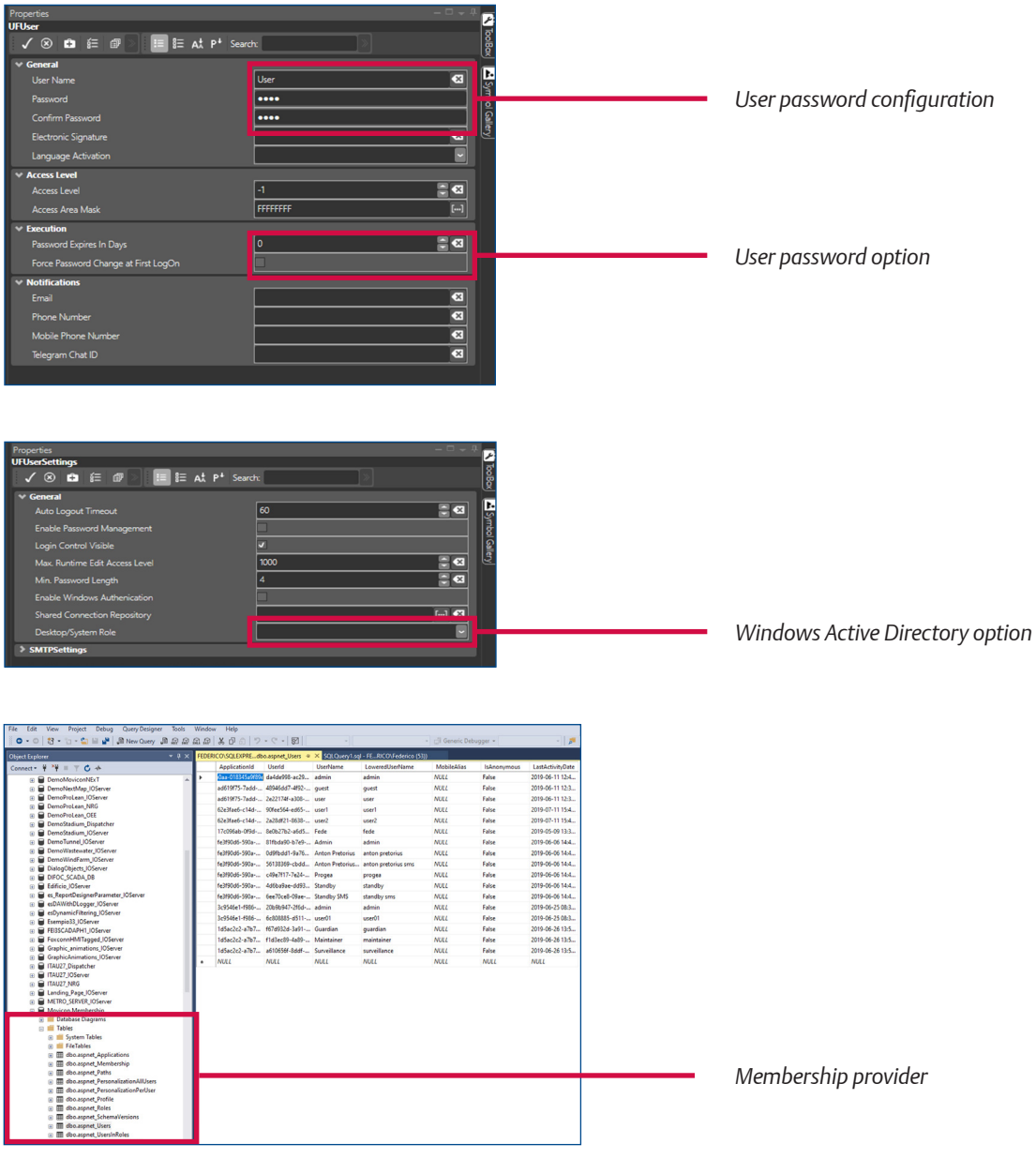
Users Management	**Movicon User Identification and Authentication** Movicon allows users to manage user authentication by defining the security properties of the project configured by the developer or system integrator. Movicon also allows all the relevant properties to be organized in a manner to offer complete and secure user identification and authorization. **User Data Repository** User data is managed according to which management type the developer intends to use as follows: – Non-centralized user data residing on a local project: in this case, passwords are encrypted locally and the entire project can also be encrypted. – Centralized user data: this is data that is centralized in the server project independently from the client, via Windows Membership management with a repository on a secure and encrypted SQL Server database. **User Access Level** Each project user is subject to authentication and receives one hierarchical privilege level. Each user can be assigned one hierarchical level in their properties. Movicon. NExT manages from 1 to 9999 user levels. **User Access Area** The “user access area” property of each user can be used to assign them a specific access area. Each access area has a specific set of controls that the user can interact with according to which hierarchical privilege level and user area they have been assigned. For example, when a control is set with an access level and enabled with Area 1, any user logging on with the same hierarchical level or higher, but not with the same Access Area 1, will not be able to use this control. Only users authorized with the same hierarchical level and Access Area 1 or higher will be able to interact with this control. The configurable access areas range from 1 to 31. ■ Non-centralized user data residing on a local project: in this case, passwords are encrypted locally and the entire project can also be encrypted.



An illustration of Movicon users management and user authentication

Windows Active Directory	**User Authentication with Windows** Movicon allows the Windows operating system to manage user authentication by using its domain users. The Windows domain users management can, therefore, be inherited and users will be managed according to the "Windows Active Directory" and the consequent Windows's authentication. **Examples:** Movicon.NExT supports the user authentication from operating system domain (external server). An authentication server can manage the password control for its own users and communicate the effective authentication to Movicon.NExT as a member of a Movicon.NExT user group. If you intend to use the authentication servers, you will have to first configure the servers then the Movicon.NExT users or user groups that require them. ■ Note: Please refer to the Movicon programmer's guide for how to set the Windows Active Directory users authentication.

Remote Access: Radius Server	The Remote Authentication and Dial-in User Service (RADIUS) is a Windows client-server protocol that provides centralized authentication and authorization functions for remote access. The RADIUS servers use UDP packets to communicate with the RADIUS clients on a network to authenticate users before allowing them access to the network and to authorize access to resources by the appropriate users. RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (accounting) and listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems. It is essential that the RADIUS server be configured in order to accept the Movicon.NExT unit as a client. Movicon.NExT units use the authentication and accounting functions of the RADIUS server.



Example of user management configuration properties

5.5 Accounts Management

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.	Please refer to section 5.3 – "User Authentication and Identification." ■ Note: Please refer to the Movicon programmer's guide for how to set the Windows Active Directory users authentication.

5.6 Identification Management

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.	Please refer to paragraph 5.3 – "User Authentication and Identification." ■ Note: Please refer to the Movicon programmer's guide for how to set the user authentication correctly.

5.7 Authentication Management

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to: h) initialize authenticator content; i) change all default authenticators upon control system installation; j) change/refresh all authenticators; and k) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	Movicon.NExT securely manages the users authentication based on the encrypted and secure Windows Memberships technology by using the user authentication procedures described above. In addition, standard users can be validated and identified using biometric devices. Movicon.NExT can be configured to support all the security procedures needed for managing users authentication. These include: ■ User password change at first login ■ Timeout for automatic logoff ■ Password validity period ■ Password min. and max. length ■ Mandatory password characters ■ Electronic signatures ■ Registration and notification of intrusion attempts

5.8 Wireless Access Management

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	The client or web client application can be run with Movicon.NExT in a location connected to the server application using a wireless communication method. The security criteria used by Movicon in a wireless connection between server and client are the same. However, the system integrator should consider two possible scenarios: 1. Wireless communication with server is allowed only in an internal network (i.e., Wi-Fi) and access from external networks is not allowed. In this case, the developer should not allow network access to any unauthorized third party. 2. Wireless communication with server is allowed from an external network, such as is the case with public networks or 3G - 4G technology. In this case, it is absolutely necessary that system developers use firewalls correctly and any other necessary means to prevent any unauthorized network access. In both these scenarios, Movicon should be configured to exchange data between server and client using the HTTPS protocol and data transport, as well as authentication certificates.

Sending Notifications to Users

Movicon.NExT offers the possibility to notify and send information by remote control using the Alarm Dispatcher module. This feature also allows process information to be sent to users using different notification methods, such as messages or alarms.

Requirements	Movicon Solution
Alarm Dispatcher Module	The customer should configure the plug-ins to be used by the Alarm Dispatcher for sending notifications. The available plug-ins are: ■ **Telegram** ■ **SMTP email** ■ **GSM SMS** ■ **Voice text-to-speech (VoIP)** Whatever plug-in is being used, communication will always be one way from Movicon to the user. It is not technically possible to reverse it for security reasons to prevent undesired access to system data.
Telegram Push Notifications	This plug-in allows communication between Movicon and the Telegram server. Notifications can only be sent to specific groups using the “Telegram Group ChatID” properties. In order to receive messages sent by the Alarm Dispatcher, a BOT must be created. Once the messages have been received, the BOT will forward them onto the recipient chats or groups defined in the project using the Telegram ChatID properties at the user or user group level. Communication is one way.
Email (SMTP)	The “SMTP Mail Sender” plug-in is used to send messages by email (electronic mail) using direct access to a server with SMTP protocol. This notification system requires internet access. The SSL option must be enabled to ensure that both the system and communications are safe. This parameter depends on the server that the client uses.

SMS (GSM)	The “GSM SMS Sender” plug-in sends messages using SMS technology based on GSM with any standard GSM modem. Messages are only sent one way.
VOIP (Voice Over IP)	The “VoIP Sender” plug-in vocally synthesizes the notification text and sends it as voice messages to individual recipients or recipient groups. The system adopts the voice messaging procedure as described in the product documentation, and only manages the telephone key # to allow all users to silence notifications to prevent data intrusion of vulnerability. Calls can be made using two different methods: ■ Direct IP call: The recipient is a VoIP client and can be reached by specifying their IP address. In this case, no account is required from a VoIP service provider (e.g., Skype). ■ Call with provider: The services of a provider are used, and communication is set up with the plug-in using a PSTN telephone and mobile phone network.
Telegram Push Notifications	This plug-in allows communication between Movicon and the Telegram server. Notifications can only be sent to specific groups using the “Telegram Group ChatID” properties. In order to receive messages sent by the Alarm Dispatcher, a BOT must be created. Once the messages have been received, the BOT will forward them onto the recipient chats or groups defined in the project using the Telegram ChatID properties at the user or user group level. Communication is one way.

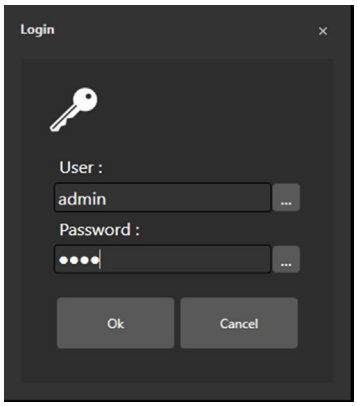
Example of Alarm Dispatcher configuration properties

5.9 Password Management

IEC 62443 Requirements	Movicon Solution
For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.	Movicon.NExT password management is complete and meets all the security requirements as demanded by the most stringent standards, such as the FDA CFR21 Part 11 regulations. Passwords are always encrypted and the repository is completely safe. Each password management feature allows the designer to configure the minimum and maximum number of characters (whether special characters are to be used or not), the expiration date and mandatory password change at first logon. In addition to Movicon password management, the designer can opt to delegate password security to the Windows Operating System by using “Windows Active Directory” to manage users. In this case, you will need to refer to the Windows documentation for managing users and passwords of the Windows domain. ■ Note: Please refer to the Movicon programmer’s guide for how to set the user authentication correctly.

5.12 Authentication Feedback

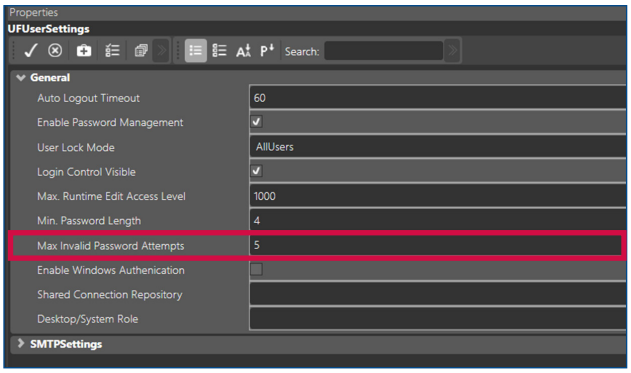
IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to obscure feedback of authentication information during the authentication process.	According to consolidated practice, the entering of passwords by the user, in any point or for whatever reason, will be obscured by replacing the entered characters with dots to ensure password entry confidentiality.



A Movicon user login window

5.13 Unsuccessful Logon Attempts

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts where critical services or servers are run, the control system shall provide the capability to disallow interactive logons.	Movicon.NExT user authentication management offers the possibility to set a maximum number of logon attempts for each user before blocking their access to the system. Any attempt to force access will be recorded in the system's historical log. The maximum number of attempts before blocking the user is to be set by the designer based on their security criteria by using an appropriate configuration as described in the product manual. A locked user can only be unlocked by the system administrator using a specific command. When the designer opts to use the Windows users authentication by means of the "Windows Active Directory," all logon attempts and accesses will be managed using the Windows Operating System security procedures.



A password property settings window

5.14 System Use Notifications

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	A Movicon.NExT project allows you to manage and display all the necessary information relating to system use. This information is managed by the designer and displayed in screens or historians on an as needed basis. For example, Movicon can display which user is logged on, the number of clients or web clients connected to the server, audits and data validators. Each piece of information to be displayed or recorded can be displayed to the end user in the language desired by the designer. In addition, if the application has to manage sensitive data, the designer can create the appropriate procedures to protect process information by using a popup window to inform the user about the sensitive data policy, or by protecting the hidden process data with the same password feedback criteria. Each sensitive data management procedure can be defined by the designer on an as needed basis. ■ **Note: please refer to the Movicon programmer's guide for how to set sensitive project data management.**

5.15 Access via Untrusted Networks

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.	The option to use untrusted or unsafe networks within the system architecture is entirely at the discretion of the designer or system integrator. However, Movicon.NExT provides the use of the procedures and protocols necessary for secure data exchange between the software platform's modules. It is the task and responsibility of the designer to use the security criteria provided by the platform, especially when using untrusted networks, by monitoring access and adopting the appropriate measures to avoid compromising data security.

6.3 Implementing Authorizations

IEC 62443 Requirements	Movicon Solution
On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and privileges.	Movicon.NExT allows properties to be assigned to each user interface control on the client side and all process data on the server side that relate to authorization based on user authentication and their assigned hierarchical- level privileges and access areas. The designer can, in any case, use the users and password management to enable interaction with the user interface's controls and functions.

6.4 Controlling Wireless Connectivity Usage

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.	Movicon.NExT provides the possibility to run client or web client applications in a workstation connected to the server application using the wireless communication method. The same security criteria used by Movicon are used in the wireless connections between server and client. However, the system integrator should take into consideration two different and possible scenarios: 1. Wireless communication with the server is allowed only in internal networks (e.g., Wi-Fi) and it is not physically possible to access from an external network. In this case, the designer should take care to impede access to the network by unauthorized third parties by configuring the Wi-Fi network appropriately. 2. Wireless communication is allowed from external networks (for example, when using public networks or 3G or 4G technology). In this case, it is absolutely crucial that system designers use firewalls and any other means necessary to prevent unauthorized access to the network. In both cases, Movicon should be configured to exchange data between server and client using the protocol and HTTPS data transport with authentication certificates.

6.5 Portable and Mobile Device User Control

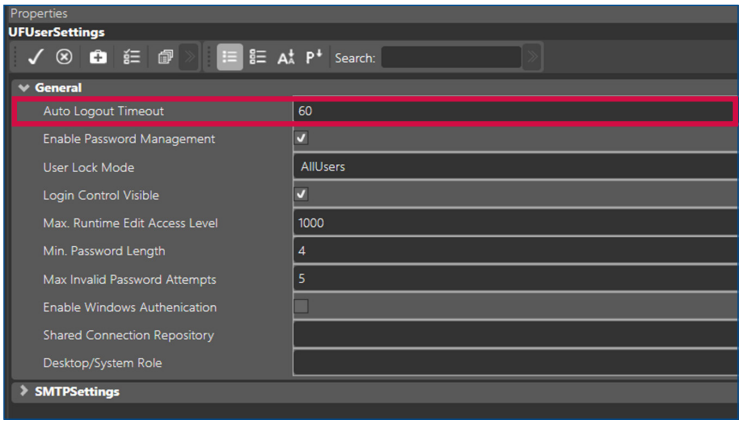
IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices b) requiring context-specific authorization c) restricting code and data transfer to/from portable and mobile devices	Access to Movicon.NExT from a mobile device can be managed in the project by means of appropriate configurations, as described in the product's documentation relating to the web client function. ■ This feature is optional and must be enabled on the product's user license. Access from remote or mobile devices can be disabled in the server project to impede any unauthorized access. When enabled, Movicon.NExT allows connection to mobile devices using secure protocols, in HTTPS and web sockets between server and client with data encryption. In addition, before being able to access the server application, the web client user of the mobile device must be authenticated by using an access mechanism with user name and password, as described above.

6.6 Mobile Code

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system, including: a) preventing the execution of mobile code b) requiring proper authentication and authorization for origin of the code c) restricting mobile code transfer to/from the control system d) monitoring the use of mobile code	Movicon.NExT uses an encryption key method to ensure the execution of the original code only. In addition, all the project files can be protected and encrypted with passwords. By doing this, it will not be possible to modify any of the project files or execute any other file types. The designer or system integrator is normally required to activate the security and congruency of files installed on the PC or server by protecting access to the entire Windows system and using data backup procedures.

6.7 Access Session Lock

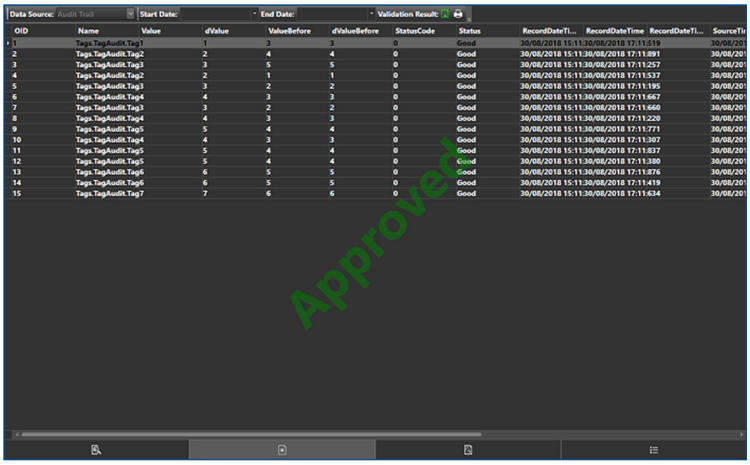
IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using approp¬riate identification and authentication procedures.	An inactivity timeout can be set by the designer in Movicon.NExT for user access sessions. After this period of time expires, the active user will automatically be disconnected and logged off from the system. Following this, the user or any other user will be able to log on again with the appropriate authentication procedures.



Screen shot of user settings property window

6.10 Event Audit

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	Audit management is configurable in Movicon.NExT and offers the possibility to track any type of event that occurs while executing the process, such as: 1. Command executions 2. Data value changes 3. Process data recording 4. Operations performed in system 5. Device communication notifications 6. Errors 7. Alarms Movicon.NExT records the events associated to users, variable value change events, communication events and system events. All this information is archived on the SQL Server database, with the security criteria and data encryption set in system properties. Each data point recorded may be subject to validation using an appropriate control and data validation command that the user can use to certify the integrity of historical data and prevent any attempts of tampering. The procedure to back up and restore historical data is required by the operating system or by the procedures defined by the developer.



6.11 Storage Capacity Control

IEC 62443 Requirements	Movicon Solution
The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	Movicon.NExT records and stores process data in files based on a relational database, where the data format can be configured by the user. The system uses the SQL Server format for default. The historical data storage period can be set by the designer in the properties of each historical log. The default period is 365 days, but the designer can change the data storage capacity by setting the engine properties of each historian or data logger in the project. The allocated capacity is, therefore, always kept under control and data is recycled to prevent exceeding the capacity of the physical space available.

Redundancy Management

Movicon.NExT also offers the designer the possibility to easily and automatically create redundant supervision and control systems, according to the “hot backup” techniques required by “mission critical” and “fault tolerant” processes.

In a redundant system, Movicon.NExT will automatically control the availability and backup of one or more servers by automatically activating secondary servers the moment in which the primary server goes out of use.

Once restored, the system will automatically synchronize all the archived data and restore the correct synchronized functioning of all the servers.

It is strongly advised to use redundant architectures for every critical process, according to the modalities provided by the product, as well as the configuration procedures described in the programmer’s manual.

6.12 Response to Process Failures

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Movicon.NExT allows the designer to manage errors and alarms in response to all the events involving a potential loss of process functionality, by notifying and clearly displaying the errors and corrective measures to take as established by the designer. All errors (alarms, messages, system errors, communication errors, notifications) can be displayed according to the modalities established by the designer in the user interface – in different languages and which can be recorded in safe and uneditable historical log archive files. In addition, Movicon.NExT allows developers to create custom procedures, using script code, to alert personnel when a special event occurs, providing them with the specific corrective actions to take or with specific support documentation.

7.3 Communication Integrity

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to protect the integrity of transmitted information.	Movicon.NExT is a modular software platform, and communication between the server and client modules takes place through encrypted communication protocols and certificates as defined in the IEC 62541 OPC UA standard specifications. This type of encrypted communication method is also used in Movicon.NExT to share information between the different modules that are available within the platform's framework. In addition, the Movicon.NExT server manages communications with field devices using the "legacy" protocols that are specific for connected devices or industrial field buses. Movicon will, nevertheless, control the integrity of communication data and notify the user of any errors by displaying and recording them in system error historical log files, as described above. The designer is, therefore, able to create and manage IEC62443-3-3 SL 1-ready applications.

7.4 Protection from Malicious Code

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.	Movicon.NExT provides an encryption method to ensure that the application's resources are not modified by unauthorized users or applications. All the project files can be protected and encrypted with passwords. This will ensure that they will remain unaltered, and that unsafe data or malicious and dangerous code content is not executed.

7.5 Security Function Verification

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	It is the responsibility of the designer to verify that the project is functioning correctly and all security requirements are applied to the correct configuration of the project. The correspondence between the operation of security functions and the security requirements must be verified in system testing. Movicon.NExT offers designers the possibility to record all system events and to customize reports, audits and verification procedures by using a script code.

7.7 Input Validation

IEC 62443 Requirements	Movicon Solution
The control system shall validate the syntax and content of any input that is used as an industrial process control input or input that directly impacts the action of the control system.	Movicon.NExT projects offer the possibility to validate operator input according to different configurable procedures. A very simple and much used method is to implement minimum and maximum value thresholds to prevent input errors made by the operator. Another method is to accept commands and value settings, according to procedural controls defined in the project, in order to control inputs and verify their congruity within the context they have been entered. In this case, the designer can enter control logic in the system to validate input and report any errors. Input validation is always established in the project by the designer on an as needed basis and according to security requirements.

7.8 Deterministic Output

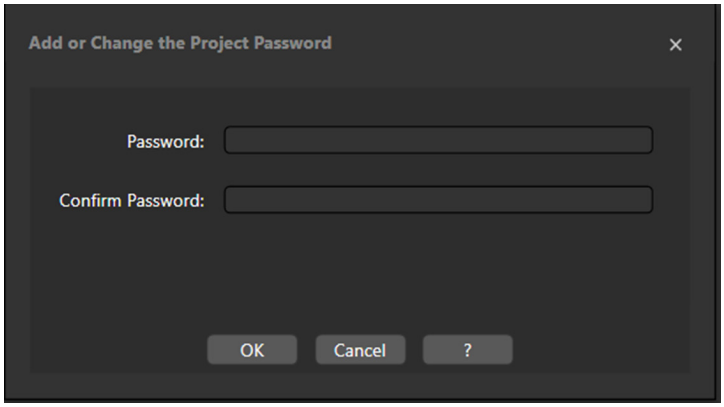
IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.	Movicon.NExT projects allow predetermined values to be set within commands based on a specific event. In addition, the designer can establish and pre-assign default values in the project's start-up procedure. However, it is the designer's responsibility to establish the control procedures and verification logics to assign predetermined values based on the situations of the process events.

8.3 Information Confidentiality

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.	The confidentiality of sensitive information and data managed by Movicon.NExT is ensured according to the different typologies used in the project. Data exchanged between clients and servers uses the OPC UA IEC 62541 standard, with data encryption and uses of certificates. Project data, users and passwords can be configured to be protected and confidential by using data protection and secure access to repositories.

8.5 Using Cryptography

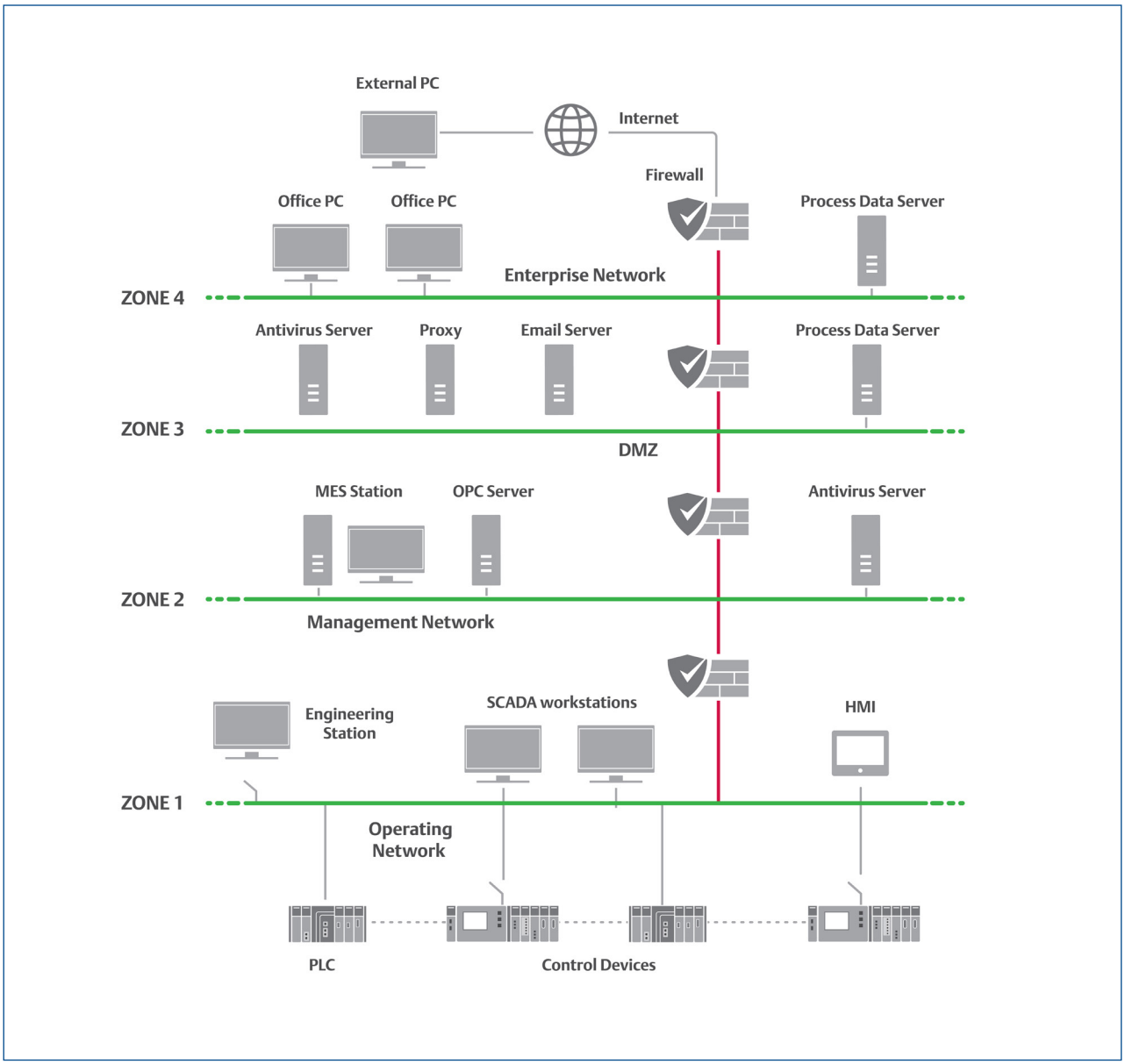
IEC 62443 Requirements	Movicon Solution
If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	Movicon.NExT offers designers the possibility to encrypt all project data and resources by using a specific function in the project's properties as indicated in the manual. This protection uses a password to protect the entire project and lock any unauthorized editing. The cryptographic algorithm used is symmetric CBC composed of two different keys. The private key length is 256 bits and the initialization key length is 128 bits.



Screen shot of a project cryptograph and access lock configuration

9.3 Network Segmentation

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	Movicon.NExT allows communications to be managed with different devices installed on different networks. The network architecture is defined based on the design choices made by the users (both the system integrator and client users) according to the project's implementation needs, as indicated in the diagram below. The network segmentation is established by the design choices based on the decisions that designers must make to create a secure infrastructure pursuant to the IEC62443 standard. The software of the project designed with Movicon.NExT will effectively adapt to the proposed architecture.



9.4 Zone Boundary Protection

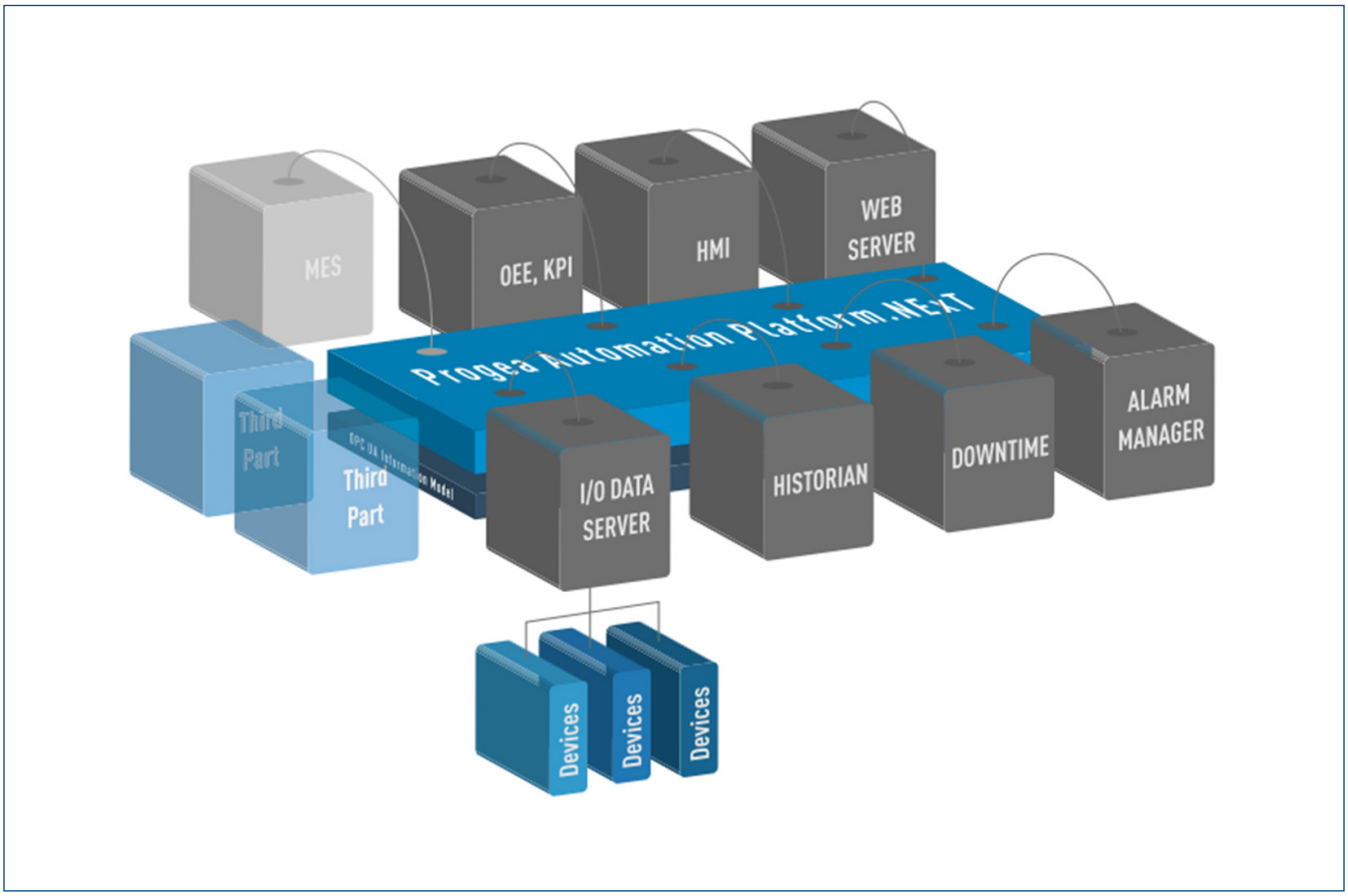
IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	Movicon.NExT allows communications to be managed with different systems in distributed architectures. This is accomplished by connecting to other server or client stations and all the field stations installed in the different networks based on the network architecture decided by the designers. Here are two possible scenarios where this may happen: ■ In cases where the network has a firewall, the client must manage the configuration to ensure access to Movicon.NExT. However, a protocol can be configured with secure transport to share information between the server and client application. ■ In cases with communications in external networks, Movicon.NExT allows the HTTPS port to be used, which does not usually need any additional configurations within the proxy. These requirements should be discussed and decided between the system integrators and the factory's IT department.

9.5 General Purpose Person-to-Person Communication Restrictions

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.	Person-to-person communications should be prevented based on secure architectures when using private messaging systems. Movicon.NExT allows notifications to be sent to personnel, as described in one of the chapters of this guide, concerning production process alarms or messages, by also using mobile devices and public networks. However, communications are unidirectional only, meaning that data can only be sent and not received. This prevents any malicious attachments to be sent to Movicon.

9.6 Application Partitioning

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.	As shown in the image below, all the functional modules belonging to the Movicon. NExT framework are independent, leaving it possible to decide to partition them by installing them on a different PC or server. All communications between the functional modules are managed by the Movicon.NExT framework using the OPC UA IEC 62541 standard information model, which ensures secure models and communication transports by using HTTPS and certificates.



This block diagram shows a Movicon NexT application partitioning

10.3 Historical Data and Audit Accessibility

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	All historical production process data recorded by Movicon.NExT is logged in archives based on the SQL Server database. The system designer will be able to ensure secure access to these data logs by using appropriate password protections. Historical data can be protected with the same method used to authenticate users to prevent data from being modified. For further security, Movicon provides an option to configure data protection for auditing purposes. When activating this option, data will be encrypted and cannot be edited, even by the system administrator. Archives subjected to data protection will ensure historical data validation to certify their authenticity without any tampering. The design can also manage how historical data is displayed in reports in PDF format for only the user to view and print. ■ **Note: Please refer to the Movicon programming guide to set the audit log security correctly.**

11.3 Protection in the Event of DoS (Denial of Service)

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to operate in a degraded mode during a DoS (denial of service) event.	In the field of IT security, a denial of service (DoS) indicates a malfunctioning due to a cyberattack in which the resources of a system are deliberately overwhelmed (for example, a server or a web server), making it incapable to provide the service to clients requesting it. Movicon ensures that its server functions by using a protocol with secure transport to its clients, with HTTPS and certificates. In fact, the server automatically discards any other requests by using certificates. In addition, if the operating system should function less effectively due to events linked to a malfunction or cyberattack, Movicon.NExT will continue as much as possible to ensure the basic functions needed are able to manage the production process. In such an event, Movicon.NExT can be run as a Windows Service, and not as a normal Windows application, to ensure the essential features are functioning independently from the operating system as much as possible.

11.4 Managing System Resources

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.	A secure system should manage its resources in a way that prevents their overuse, which leads to complete exhaustion. Movicon.NExT offers designers tools to ensure that the projects they create have the capability to correctly manage or monitor the system's resources: 1. Archive management: Each historical archive is recycled and allows physical memory to be allocated in such a way that it is not exhausted. 2. System information that allows designers to monitor the system's resources or access the operating system's information using script code. This detects any abnormal consumption of resources and, as a consequence, informs operators or reduces their functionality. 3. Use SNMP protocol for communications and to access and manage information for connected systems.

11.5 System Backup Control

IEC 62443 Requirements	Movicon Solution
The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.	Movicon.NExT offers the capacity to automatically back up all the control system's features and their functions by using and configuring the optional redundancy (hot backup) function. This will guarantee the functioning of all systems, including the archive backups, even if one of the servers should crash. The redundancy should be distributed among two or more servers in the application. In addition to redundancy, Movicon allows the scripting function to be used to create the appropriate backup procedures of data from the system's repository to other repositories, both locally or centralized, or in the cloud. In the latter case, the designer can create procedures in the project to schedule regular backup copies of sensitive data.

11.6 Recovery System

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	Movicon.NExT offers the capacity to automatically back up all the control system's features and their functions by using and configuring the optional redundancy (hot backup) function. This will guarantee the functioning of all systems, including the archive backups, even if one of the servers should crash. The redundancy should be distributed among two or more servers in the application. In addition, all settings used to define how the application functions are recorded and saved by Movicon in project files should be taken into consideration. These files are automatically backed up locally and can be saved as deemed appropriate by the designer to restore the application to its normal functioning state if a disruption or failure should occur.

11.7 Emergency Power

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	The choice of what energy management to adopt to for supply power of a control system based on Movicon is entirely left to the designer and end user. Whatever choice is made, the appropriate measures must be taken to ensure that the system is supplied emergency power in the event of a power failure without affecting its security state. For example, when using a system powered with UPS (power backup), the PC will remain with power for the time needed to restore electricity from the main power source. In any case, Movicon can be relied upon for restarting PCs in the event of a power failure when run as the operating system's 'service.'

11.8 Network Security Configurations

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to be set up according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.	A control system based on Movicon.NExT can adapt to the security policies of any communication network on which it is installed. Network administrator security configurations are independent from the Movicon functions, which guarantees support to the security policies adopted. In addition, Movicon.NExT supports the deployment of secure connections between its functional modules using cryptographed communications, HTTPS and certificates.

11.9 Function Restrictions

IEC 62443 Requirements	Movicon Solution
The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	Movicon.NExT allows the designer to configure the ports used and enable or disable all the project's unnecessary functions. Other functions, such as the use of ports, protocols and/or services (e.g., FTP), fall within the specific competence of the integrators who implement or deploy them according to project needs.

Compliance Table

FR 1 – Identification and Authentication Control (IAC)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 1.1 – Human user identification and authentication	5.3	YES			
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1				
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2				
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				
SR 1.2 – Software process and device identification and authentication	5.4				
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1				
SR 1.3 – Account management	5.5	YES			
SR 1.3 RE 1 – Unified account management	5.5.3.1				
SR 1.4 – Identifier management	5.6	YES			
SR 1.5 – Authenticator management	5.7	YES			
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1				
SR 1.6 – Wireless access management	5.8	YES			
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1				
SR 1.7 – Strength of password-based authentication	5.9	YES			
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1				
SR 1.7 RE 2 – Password lifetime restrictions for all users	5.9.3.2				
SR 1.8 – Public key infrastructure certificates	5.10				
SR 1.9 – Strength of public key authentication	5.11				
SR 1.9 RE 1 – Hardware security for public key authentication	5.11.3.1				
SR 1.10 – Authenticator feedback	5.12	YES			
SR 1.11 – Unsuccessful login attempts	5.13	YES			
SR 1.12 – System use notification	5.14	YES			
SR 1.13 – Access via untrusted networks	5.15	YES (S.I.)			
SR 1.13 RE 1 – Explicit access request approval	5.15.3.1				

FR 2 – User Control (UC)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 2.1 – Authorization enforcement	6.3	YES			
SR 2.1 RE 1 – Authorization enforcement for all users	6.3.3.1				
SR 2.1 RE 2 – Permission mapping to roles SR	6.3.3.2				
SR 2.1 RE 3 – Supervisor override	6.3.3.3				
SR 2.1 RE 4 – Dual approval SR	6.3.3.4				
SR 2.2 – Wireless use control	6.4	YES			
SR 2.2 RE 1 – Identify and report unauthorized wireless devices	6.4.3.1				
SR 2.3 – Use control for portable and mobile devices	6.5	YES			
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices	6.5.3.1				
SR 2.4 – Mobile code	6.6	YES			
SR 2.4 RE 1 – Mobile code integrity check	6.6.3.1				
SR 2.5 – Session lock	6.7	YES			
SR 2.6 – Remote session termination SR	6.8				
SR 2.7 – Concurrent session control SR 2.8	6.9				
SR 2.8 – Auditable events	6.10	YES (S.I.)			
SR 2.8 RE 1 – Centrally managed, system-wide audit trail	6.10.3.1				
SR 2.9 – Audit storage capacity	6.11	YES			
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached	6.11.3.1				
SR 2.10 – Response to audit processing failures SR	6.12	YES (S.I.)			
SR 2.11 – Timestamps	6.13				
SR 2.11 RE 1 – Internal time synchronization	6.13.3.1				
SR 2.11 RE 2 – Protection of time source integrity SR	6.13.3.2				
SR 2.12 – Non-repudiation	6.14				
SR 2.12 RE 1 – Non-repudiation for all users	6.14.3.1				

FR 3 – System Integrity (SI)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 3.1 – Communication integrity	7.3	YES			
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1				
SR 3.2 – Malicious code protection	7.4	YES			
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1				
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2				
SR 3.3 – Security functionality verification	7.5	YES (S.I.)			
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1				
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2				
SR 3.4 – Software and information integrity					
SR 3.4 RE (1) Automated notification about integrity violations					
SR 3.5 – Input validation	7.7	YES			
SR 3.6 – Deterministic output	7.8	YES (S.I.)			
SR 3.7 – Error handling	7.9				
SR 3.8 – Session integrity	7.10				
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1				
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2				
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3				
SR 3.9 – Protection of audit information	7.11				
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1				
SR 4.1 – Information confidentiality	8.3	YES			
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks	8.3.3.1				
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries	8.3.3.2				
SR 4.2 – Information persistence	8.4				
SR 4.2 RE 1 – Purging of shared memory resources	8.4.3.1				
SR 4.3 – Use of cryptography	8.5	YES			

FR 5 – Restricted Data Flow (RDF)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 5.1 – Network segmentation	9.3	YES			
SR 5.1 RE 1 – Physical network segmentation	9.3.3.1				
SR 5.1 RE 2 – Independence from non-control system networks	9.3.3.2				
SR 5.1 RE 3 – Logical and physical isolation of critical networks	9.3.3.3				
SR 5.2 – Zone boundary protection	9.4	YES			
SR 5.2 RE 1 – Deny by default, allow by exception	9.4.3.1				
SR 5.2 RE 2 – Island mode	9.4.3.2				
SR 5.2 RE 3 – Fail close	9.4.3.3				
SR 5.3 – General purpose person-to-person communication restrictions	9.5	YES			
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications	9.5.3.1				
SR 5.4 – Application partitioning	9.6	YES			

FR 6 – Timely Response to Events (TRE)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 6.1 – Audit log accessibility	10.3	YES			
SR 6.1 RE 1 – Programmatic access to audit logs	10.3.3.1				
SR 6.2 – Continuous monitoring	10.4				

FR 7 – Resource Availability (RA)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 7.1 – Denial of service protection	11.3	YES			
SR 7.1 RE 1 – Manage communication loads	11.3.3.1				
SR 7.1 RE 2 – Limit DoS effects to other systems or networks	11.3.3.2				
SR 7.2 – Resource management	11.4	YES (S.I.)			
SR 7.3 – Control system backup	11.5	YES (S.I.)			
SR 7.3 RE 1 – Backup verification	11.5.3.1				
SR 7.3 RE 2 – Backup automation	11.5.3.2				
SR 7.4 – Control system recovery and reconstitution	11.6	YES			
SR 7.5 – Emergency power	11.7	YES			
SR 7.6 – Network and security configuration settings	11.8	YES			

FR 7 – Resource Availability (RA)					
SRs and REs		**SL1**	**SL2**	**SL3**	**SL4**
SR 7.6 RE 1 – Machine-readable reporting of current security settings	11.8.3.1				
SR 7.7 – Least functionality	11.9	YES			
SR 7.8 – Control system component inventory	11.10	YES			

References

(1) *IEC 62443-1-1: Industrial communication networks- Network and system security- Part 1-1: Terminology, concepts and models (IEC/TR 62443-1-1:2009)*

(2) *ISA- 62443-1-2: Security for industrial automation and control systems- Master Glossary, Draft 1, Edit 5, August 2014 (ISA-TR62443-1-2)*

(3) *ISA-62443-1-3: Security for industrial automation and control systems- Part 1-3: Cyber security system conformance metrics, Draft 1, Edit 19, October 2015*

(4) *ISA-62443-2-1: Security for industrial automation and control systems- Part 2-1: Industrial automation and control system security management system, Draft 7, Edit 5, November 9, 2015*

(5) *ISA-62443-2-2: Security for industrial automation and control systems: Implementation guidance for and IACS security management system, Draft 1, Edit 4, April 2013*

(6) *IEC 62443-2-3: Security for industrial automation and control systems- Part 2-3: Patch management in IACS environment (IEC /TR 62443-2-3:2015)*

(7) *IEC 62443-2-4: Security for industrial automation and control systems- Part 2-4: Security program requirements for IACS providers (IEC 62443-2-4:2015)*

(8) *ISA-62443-3-2: Security for industrial automation and control systems: Security risk assessment for system design, Draft 6, Edit 3, August 5, 2015*

(9) *IEC 62443-3-3: Industrial communication networks- Network and system security- Part 3-3: System security requirements and security levels (IEC 62443-3-3: 2013)*

(10) *IEC/NP 62443-4-1: Industrial communication networks- Network and system security- Part 4-1: Product development requirements based on ISA-62443-04-01, Draft 1, Edit 9, April 2013*

(11) *ISA-62443-4-1: Security for industrial automation and control systems- Part 4-1: Secure product development life- cycle requirements, Draft 3, Edit 11, March 2016*

(12) *ISA -62443-4-2: Security for industrial automation and control systems technical security requirements for IACS components, Draft 2, Edit 4, July 2, 2015*

(13) *ISO/IEC 27001: Information technology- security techniques- information security management systems- requirements (ISO/IEC 27001:2013)*

(14) *ISO/IEC 27002: Information technology- security techniques- code of practice for information security controls (ISO/IEC 27002:2013)*

(15) *VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung- Blatt 1: Allgemeines Vorgehensmodell*

(16) *Leitfaden Industrial Security IEC 62443 einfach erklärt- Pierre Kobes (VDE Verlag 2016)*

United States Office
Emerson Automation Solutions
Intelligent Platforms, LLC
2500 Austin Dr
Charlottesville, VA 22911
T +1 (888) 305-2999

Germany Office
Emerson Automation Solutions
ICC Intelligent Platforms GmbH
Memminger Straße 14
Augsburg, DE 86159
T +49 7721 99 838 0

Brazil Office
Emerson Automation Solutions
Rua Irmã Gabriela,
51 œCidade Monções
São Paulo œ SP, 04571-130

Italy Office
Emerson Automation Solutions
Proea Srl
Via D'Annunzio 295, Modena,
41123, Italy
T +39 059 451060

India Offices
Emerson Automation Solutions
Intelligent Platforms Pvt. Ltd.,
Building No.8, Ground Floor
Velankani Tech Park,
No.43 Electronics City Phase I,
Hosur Road Bangalore-560100

China Office
Emerson Automation Solutions
Intelligent Platforms
(Shanghai) Co., Ltd
No.1277, Xin Jin Qiao Road,
Pudong, Shanghai, China, 201206

Switzerland Office
Emerson Automation Solutions
Progea International SA
Via Sottobisio 28,
6828 Balerna, Switzerland
T +41 091 9676610

Singapore Office
Emerson Automation Solutions
Intelligent Platforms Asia Pacific Pte. Ltd.
1 Pandan Crescent,
Singapore, 128461

www.emerson.com/industrial-automation-controls
LinkedIn.com/company/Emerson-Automation-Solutions
Twitter.com/MachineAutoSol
YouTube.com/MachineAutoSol

EMERSON