SLOVENSKI STANDARD
oSIST prEN IEC 62443-2-4:2022

01-november-2022

Zaščita industrijske avtomatizacije in nadzornih sistemov - 2-4. del: Zahteve za program varnosti zaščite za ponudnike storitev IACS

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

Sécurité des automatismes industriels et des systèmes de commande - Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

Ta slovenski standard je istoveten z: **prEN IEC 62443-2-4:2022**

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

oSIST prEN IEC 62443-2-4:2022 **en,fr,de**

65/936/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER:	
IEC 62443-2-4 ED2	
DATE OF CIRCULATION:	CLOSING DATE FOR VOTING:
2022-09-09	**2022-12-02**
SUPERSEDES DOCUMENTS:	
65/848/CD, 65/854A/CC	

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION	
SECRETARIAT: France	SECRETARY: Mr Didier GIARRATANO
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 44,SC 45A,TC 57,SC 62A,SC 121A,ISO/IEC JTC 1/SC 41	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

PROPOSED STABILITY DATE: 2025

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

Ed.2

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-2-4 Ed. 2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation in collaboration with the liaison International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Edition 2 of IEC 62443-2-4 makes editorial corrections discovered since its release and provides clarifications that have been identified as necessary, primarily through the use of the document during conformity assessment and during the development of profiles. One area of clarification

is that some requirements were interpreted as technical requirements, when the intention was for them to be the use/configuration of technical capabilities.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of the base publication and its amendment will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS).

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

Ed.2

1 Scope

This part of IEC 62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of Profiles that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program for IACS Asset Owners. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 1 illustrates the integration and maintenance security capabilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. Some of the IEC 62443-2-4 security program requirements are associated with security requirements described in IEC 62443-3-3 and IEC 62443-4-2.

NOTE 3 The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation, and maintenance.

NOTE 4 Maintenance of legacy system with insufficient security functional capabilities, implementation of policies, processes and procedures are recommended as risk mitigations.

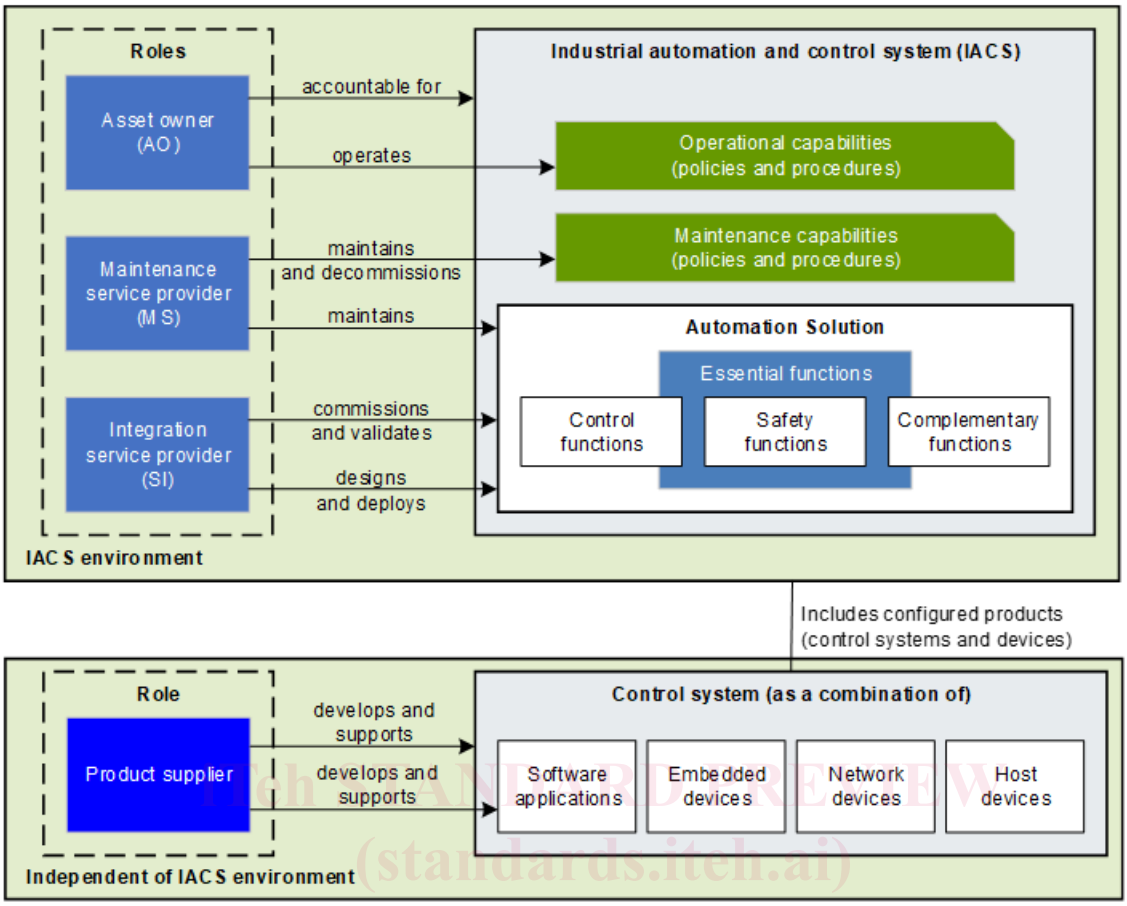

Figure 1 – Scope of service provider capabilities

In Figure 1, the Automation Solution is illustrated to contain the Essential Functions that include safety functions, commonly implemented by a Safety Instrumented System (SIS), and complementary and control functions, commonly implemented by supporting applications, such as batch management, advanced control, historian, and security related applications. The dashed boxes indicate that these components are “optional”.

NOTE 5 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

NOTE 6 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

NOTE 7 Service providers often provide reference architectures.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

“None”

3 Terms, definitions, abbreviated terms and acronyms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1

asset owner
role of an organization responsible for one or more IACSs

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: This definition includes the components that are part of the IACS.

Note 3 to entry: In the context of this standard, asset owner also includes the operator of the IACS.

3.1.2
attack surface
physical and functional interfaces of a system that can be accessed and through which the system can be potentially exploited

Note 1 to entry: The size of the attack surface for a software interface is proportional to the number of methods and parameters defined for the interface. Simple interfaces, therefore, have smaller attack surfaces than complex interfaces.

Note 2 to entry: The size of the attack surface and the number of vulnerabilities are not necessarily related to each other.

3.1.3
Automation Solution
collection of control system and any complementary components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this part of IEC 62443.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (e.g. a specific number of workstations, controllers, and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution may be provided by multiple suppliers, including the product supplier of the control system and the product suppliers of complementary components.

Note 4 to entry: The Automation Solution does not include the processes and procedures used during integration, maintenance, and operation of the IACS.

Note 5 to entry: An Automation Solution, once integration into a given environment is complete, is ready for operation

3.1.4
basic process control system
system that responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety integrated functions (SIF)

Note 1 to entry: Safety instrumented functions are specified in the IEC 61508 series.

Note 2 to entry: The term “process” in this definition may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

3.1.5
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.6
consultant
subcontractor that provides guidance, including expert advice, to the asset owner, integration or maintenance service provider, or product supplier

Note1 to entry: a consultant can provide assistance for component or system countermeasures

3.1.7
control system
hardware and software components used in the design and implementation of an IACS

Note 1 to entry: As shown in Figure 1, control systems are composed of field devices, embedded control devices, network devices, and host devices (including workstations and servers).

Note 2 to entry: As shown in Figure 1, control systems are represented in the Automation Solution by a BPCS and an optional SIS.

3.1.8
handover
act of turning an Automation Solution over to the asset owner

Note 1 to entry: Handover effectively transfers responsibility for operations and maintenance of an Automation Solution from the integration service provider to the asset owner and generally occurs after successful completion of system test, often referred to as Site Acceptance Test (SAT)

3.1.9
harden
process of improving the security of a system or component through a reduction of risk factors

Note 1 to entry: Hardening generally involves adapting and configuring the Automation Solution / components and related policies and procedures to meet the security needs of the asset owner's site

3.1.10
industrial automation and control system
collection of personnel, hardware, software, procedures and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

Note 1 to entry: The IACS may include components that are not installed at the asset owner's site.

Note 2 to entry: The definition of IACS was taken from IEC-62443-3-3 and is illustrated in Figure 1. Examples of IACSs include Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. IEC 62443-2-4 also defines the proper noun "Automation Solution" to mean the specific instance of the control system product and possibly additional components that are designed into the IACS. The Automation Solution, therefore, differs from the control system since it represents a specific implementation (design and configuration) of the control system hardware and software components for a specific asset owner.

3.1.11
integration service provider
service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover

Note 1 to entry: Integration service providers are often referred to as integrators or Main Automation Contractors (MAC).

3.1.12
maintenance service provider
service provider that provides support activities for an Automation Solution after handover

Note 1 to entry: Maintenance is often considered to be distinguished from operation (e.g. in common colloquial language it is often assumed that an Automation Solution is either in operation or under maintenance). Maintenance service providers can perform support activities during operations, e.g. managing user accounts, security monitoring, and security assessments.

3.1.13
portable media
portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to: CD / DVD / Blu-ray Media, USB memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds, and portable computers.

3.1.14
product
system, subsystem or component that is manufactured, developed or refined for use by other products

Note 1 to entry: The processes required by the practices defined in this document apply iteratively to all levels of product design (for example, from the system level to the component level).

3.1.15
product supplier
manufacturer of hardware and/or software product

Note 1 to entry: Used in place of the generic word vendor to provide differentiation.

3.1.16
profile
named combination of options, chosen according to a specified framework, that are necessary to accomplish a particular function

Note 1 to entry: The options can be chosen from one or several documents or subdivisions of documents.

3.1.17
remote access
access to a control system through an external interface of the control system

Note 1 to entry: Examples of applications that support remote access include RDP, OPC, and Syslog.

Note 2 to entry: In general, remote access applications and the Automation Solution will reside in different security zones as determined by the asset owner. See IEC 62443-3-2 for the application of zones and conduits to the Automation Solution by the asset owner.

3.1.18
safety instrumented system
system used to implement functional safety

Note 1 to entry: See IEC 61508 and IEC 61511 for more information on functional safety.

Note 2 to entry: Not all industry sectors use this term. This term is not restricted to any specific industry sector, and it is used generically to refer to systems that enforce functional safety. Other equivalent terms include safety systems and safety related systems.

3.1.19
security compromise
violation of the security of a system such that an unauthorized (1) disclosure or modification of information or (2) denial of service may have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

3.1.20
security incident
security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term “of some significance’ is relative to the environment in which the security compromise is detected. For example, the same compromise may be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

3.1.21
security patch
software patch that is relevant to the security of a software component

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches may address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

3.1.22
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS

Note 1 to entry: The security program for IACS service providers refers to the policies and procedures defined by them to address security concerns of the IACS.

3.1.23
service provider
role of an organization (internal or external organization, manufacturer, etc.) that provides a specific support service and associated supplies in accordance with an agreement with the asset owner

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.24
subcontractor
service provider under contract to the integration or maintenance service provider or to another subcontractor that is directly or indirectly under contract to the integration or maintenance service provider

3.1.25
system
interacting, interrelated, or interdependent elements forming a complex whole

Note 1 to entry: A system may be packaged as a product.

Note 2 to entry: In practice, the interpretation of its meaning is frequently clarified by the use of an adjective, such as control system. In the context of a control system, the elements are largely hardware and software elements.

3.1.26
verify
check that the specified requirement was met

3.1.27
vulnerability
flaw or weakness in the design, implementation, or operation and management of a component that can be exploited to cause a security compromise

Note 1 to entry: Security policies typically include policies to protect confidentiality, integrity, and availability of system assets.

3.2 Abbreviations

AES_GCM Advanced Encryption Standard Galois/Counter Mode

BPCS Basic Process Control System

BR	Base Requirement
CEF	Common Event Format
DCS	Distributed Control System
EWS	Engineering Workstation
IACS	Industrial Automation and Control System
RE	Requirement Enhancement
RDP	Remote Desktop Protocol
RFC	Request For Comment
RFQ	Request For Quote
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SNMP	Simple Network Management Protocol
SOW	Statement Of Work
SSID	Service Set Identifier
SP	Security Program
TR	Technical Report
VPN	Virtual Private Network

4 Concepts

4.1 Use of IEC 62443-2-4

4.1.1 Use of IEC 62443-2-4 by service providers

“Service provider” and “asset owner” are terms that represent roles of an organization. While they can be in the same organization, they are typically in separate organizations, with the service provider under contract to the asset owner’s organization.

This part of the IEC 62443 series defines a single set of requirements for security-related processes to be supported by security programs of both integration and maintenance service providers (see 4.1.5 and 4.1.6). Although implementation of these requirements by integration and maintenance service providers can be different, the requirements apply equally to both. Support for these requirements means that the service provider can provide them to the asset owner upon request.

The terms and conditions for providing these capabilities are beyond the scope of this standard. In addition, IEC 62443-2-4 can be used by these service providers to structure and improve their security programs.

In addition, service providers can use IEC 62443-3-3 and IEC 62443-4-2 in conjunction with IEC 62443-2-4 to work with suppliers of underlying control systems/components. This collaboration can assist the service provider in developing policies and procedures around a capability of a system/component, e.g. backup and restore based on the recommendations from the suppliers of the systems/components used.

NOTE IACS is a generic expression used to describe an industrial automation and control systems (based on the definition taken from IEC 62443-1-1), that can be extended to other automation vertical industries. For example: Substation Automation Solutions, smart grid, distributed grid, medical device manufacturing, building automation systems, elevators, and escalators.

The security programs implementing these requirements are expected to be independent of different releases of the control system that is embedded in the Automation Solution. That is a new release of the control system product does not necessarily require a change to the service provider's security program. However, changes to the security program will be required when changes to the underlying control system make the existing security program deficient with respect to these IEC 62443-2-4 requirements.

EXAMPLE 1 A service provider may have experience with a specific control system line of products. Developing policies and procedures for that line of products will be based on the recommendations of the product supplier and the capabilities of the product line. Therefore, when the product capabilities for backup and restore are changed, the corresponding capabilities of the service provider's security program (corresponding to SP.12.XX) may have to be changed to remain consistent with the updated product capabilities. On the other hand, the service provider's policies and procedures around non-disclosure agreements or personnel background checks (corresponding to SP.01.03 and SP.01.04) and are very likely independent of the control system product used in the Automation Solution.

This collaboration can also be used to improve security in these systems/components. First, the service provider can recommend new or updated security features to the system/component supplier. Second, the service provider can gain knowledge about the system/component that allows it to add its own compensating security measures to the Automation Solution during deployment or maintenance.

The requirements are specified in Annex A, and are defined in terms of the capabilities that these security programs are required to provide. Clause 4.1.4 discusses the ability of industry groups to subset these capabilities into profiles to address risk reduction. See IEC 62443-3-2 for more detail on security risks.

IEC 62443-2-4 also recognizes that security programs evolve and that capabilities go through a lifecycle of their own, often starting as completely manual and evolving over time to become more formal, more consistent, and more effective. Clause 4.2 addresses this issue of evolving capabilities by defining a maturity model to be used with the application of this standard.

EXAMPLE 2 A specific capability might be introduced as a set of manual procedures and then later supplemented with automated tools.

As a result, the requirements in Annex A are stated abstractly, allowing for a wide range of implementations. Integration service provider security program processes that meet these requirements are used during the deployment, configuration, handover, and commissioning of the Automation Solution, while maintenance service providers security program processes are used to update and maintain the security of the Automation Solution once it becomes operational.

It is expected that service providers and asset owners will negotiate and agree on which of these required processes are to be provided and how they are to be provided. These aspects of fulfilling the requirements are beyond the scope of IEC 62443-2-4, although the use of profiles that are accepted by the asset owner and the service provider could make this easier.

EXAMPLE 3 A service provider capable of supporting complex passwords has to be capable of supporting specific variations of complex passwords as defined by the password policies of asset owners.

EXAMPLE 4 Many capabilities have a timeliness aspect related to their performance. What is considered timely should be agreed to by both the asset owner and the service provider.

4.1.2 Use of IEC 62443-2-4 by asset owners

IEC 62443-2-4 can be used by asset owners to request specific security capabilities from the service provider. More specifically, prior to such a request, IEC 62443-2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs.

In general, IEC 62443-2-4 recognizes that asset owner requirements vary, so it has been written to encourage service providers to implement the required capabilities so that they can be adaptable to a wide variety of asset owners. For example, the asset owner can evaluate whether