



Cybersecurity and IEC 62443

Part I–Overview

White Paper

Contents

- 1. Introduction 3
- 2. Key Concepts12
- 3. IEC 62443 Parts 18
- 4. Certification Schemes24
- 5. Summary25
- 6. Recommended Additional Reading26
- 7. Endnotes27

1. Introduction

List of Acronyms and Abbreviations

ANSI	American National Standards Institute
IACS	Industrial Automation and Control System
BPCS	Basic Process Control System
CB	Certification Body
CR	Component Requirement
CSMS	Cyber Security Management System
EPC	Engineering & Procurement Contractor
FRs	Foundational Requirements
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISO27K	ISO/IEC 27000 Series of Standards
IT	Information Technology
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation
OEM	Original Equipment Manufacturer
OT	Operational Technology
PCA	Process Capability Assessment
PLC	Programmable Logic Controller
RE	Requirement Enhancement
SDL	Secure Development Lifecycle
SDLA	Secure Development Lifecycle Assessment
SIF	Safety Instrumented Function
SL	Security Level
SL-A	Achieved Security Level

SL-C	Capabilities Security Level
SL-T	Target Security Level
SP	Security Program (Requirement)
SR	System Requirement
TC	Technical Committee
VDE	Association for Electrical, Electronic & Information Technologies (Verband der Elektrotechnik Elektronik und Informationstechnik e.V.)
VDI	The Association of German Engineers (Verein Deutscher Ingenieure e.V.)
WIB	Werkgroup voor Instrument Beoordeling (Working-party on Instrument Behavior)
WG	Working Group

Overview

This is the first in a multi-part series of white papers dealing with cybersecurity of Bently Nevada products and services as they relate to the ISA/IEC 62443 family of technical specifications, technical reports, and standards. Table 1 summarizes the installments that are envisioned for this series.

Table 1: IEC 62443 Cybersecurity White Papers Series

Doc #	Topic	62443 Part(s)
179M4409	Part I – Overview	All
179M4410	Part II – Secure Product Development Lifecycle Process Certification	4-1
179M4439	Part III – Component Certification Overview	4-2
179M4442	Part IV – Orbit 60 Component Certification	4-2
179M4443	Part V – Orbit 60 Communications Gateway Module	4-2
180M8346	Part VI – Orbit 60 Certificates Handling	4-2
184M5163	Part VII – Orbit DCM Component Certification	4-2
184M6631	Part VIII – Orbit DCM Certificates	4-2
*	Part IX – Orbit Studio and Orbit Display Component Certification*	4-2
*	Part X – System I Component Certification*	4-2
*	Part XI – System Certification Overview*	3-3
*	Part XII – Service Provider Certification*	2-4
*	Parts XIII and above – Certifications for other Bently Nevada Products*	4-2

* Future; chronological publication order may not necessarily follow numerical order.

In this first installment, we focus on an overview of the 62443 family itself rather than the particulars of any specific Bently Nevada product. This is because much confusion exists over the types of cybersecurity certifications compared to other types of certifications that tend to be discrete in nature. For example, a product either has a particular hazardous area approval or it does not; a product either carries the CE mark or it does not; a product either has a SIL rating or it does not. In contrast, there are more nuances and variations in cybersecurity approvals and to understand those (and to properly interpret a product's cybersecurity certificate), it is important to understand the basic elements of the 62443 family of standards.

A Clear Mandate

Over the last five years, Bently Nevada has engaged in more than 200 focused customer consultations with the specific objective of understanding industry's landscape of needs, trends, regulations, and priorities. We spoke directly with end users, machinery OEMs, EPCs, other control and automation providers, and system integrators. At the top of the ensuing list was cybersecurity. This has resulted in dedicated Bently Nevada personnel focused on cybersecurity, company-wide processes focused on cybersecurity, and a company-wide commitment that all future products¹ will be "secure by design" given their tight interconnection with industrial automation and control systems (IACS) and both the operational technology² (OT) and information technology (IT) domains.

This focus is not confined to new products, either. Existing products – the majority of which originated at a time when cybersecurity was not a primary customer requirement – are also included in Bently Nevada's commitment to cybersecurity. This is particularly true of software such as System 1. Developed in the late 1990s and launched in 2000, the concept of cybersecurity for industrial instrumentation was not even on the radar when System 1 was conceived. However, the intervening two decades have seen cybersecurity move from a non-issue to the industry's single most prominent issue. A major System 1 redesign effort in 2017 resulted in a product that now works within modern, cybersecure IT and OT practices and infrastructures, incorporating technologies such as data diodes, virtual machines, cloud-based servers, and server replication. In the future, formal cybersecurity certification of the System 1 platform will be pursued.

Why Cybersecurity Matters

Above, it was noted that cybersecurity is a high priority with customers. It is helpful to review how and why this has become such a major concern, as this sets the stage for not only why Bently Nevada products must be cybersecure, but why compliance with industry standards dealing with cybersecurity has become so important.

Although the first instance of a computer virus dates all the way back to 1971³, it was the Stuxnet Worm⁴ in 2010 that dispelled a number of misconceptions and resulted in a dramatic increase in awareness of (and emphasis on) industrial cybersecurity. Some of these misconceptions included beliefs that:

- Cyberattacks were only aimed at the IT level of an organization – not the OT level.
- Special-purpose industrial devices such as PLCs⁵ with proprietary embedded software, operating systems, and protocols were essentially invulnerable.
- Motivations for cyberattacks were primarily monetary in nature⁶.
- Cyberattacks were focused on intellectual property (such as data) and could not be used to destroy physical infrastructure (such as machines)^{7, 8}.
- Actors in a cyberattack were always rogue individuals or terrorist organizations, not state-funded and coordinated entities such as government agencies⁶.

Although Stuxnet was instrumental in creating heightened awareness that cyberattacks could indeed target the OT domain instead of only the IT domain, it was by no means the only example of OT breaches during the era. Researchers at Idaho National Laboratory identified 22 different cyberattacks specifically targeting IACSs between 2000 and 2017⁹.

The Ukraine Power Grid Attack¹⁰ in 2015 is especially noteworthy as it represented the first known successful attack on a power grid. Although the Aurora Generator Test in 2007¹¹ showed that such an attack was indeed possible – raising considerable concern of power grid vulnerability – the Ukraine

incident made these concerns reality when the lights went off for more than 220,000 households. The Ukraine incident was also noteworthy in that it involved apparatus employing serial communications – an older technology thought to be particularly less vulnerable than newer ethernet-based technologies¹². Lastly, the Ukraine incident combined an attack on the IACS with a simultaneous attack on the utility's call centers¹³.

All of these incidents served to underscore that concerns over cyberattacks could no longer be relegated to simply the IT domain; instead, the OT domain and the specialized IACS apparatus were also at risk. Where vulnerabilities at the IT level were typically related to financial concerns, privacy concerns, and intellectual property concerns, vulnerabilities at the OT level had even larger implications as they could take down entire plants or even entire power grids, could wreak environmental havoc, and could cause disasters leading to loss of human life.

It is within this context of risks and consequences that the behavior of asset owners began shifting in two fundamental ways:

1. By placing increased emphasis on development of standards that could help assure cybersecurity in both their IT and OT domains.
2. By embracing those standards as the basis for their own cybersecurity programs while holding suppliers, system integrators, and service providers to those same standards in delivery of their products and services.

IT and OT Standards

The ISO/IEC 27000¹⁴ family of standards was first published in 2009 and quickly emerged as the preeminent guidelines for cybersecurity in the IT domain. Approximately 60 separate but interrelated and harmonized standards, technical specifications, and technical reports comprise the so-called "ISO27K" family, and several of these documents can trace their roots to the early 1990s, reinforcing that electronic information security has been a concern for many decades.

ISO27K established – among many other things – the concept of an Information Security Management System (ISMS). However, it was quickly realized that even with such a large inventory of topics, the ISO27K family did not adequately address the special needs of the OT domain. For that, a new family of standards was needed. It would eventually become the ISA/IEC 62443 family, and with it, a concept comparable to ISMS: the Cyber Security Management System (CSMS). Where the ISMS is focused on the IT domain, the CSMS is focused on the OT domain.

Bently Nevada examined a number of cybersecurity standards as it evaluated which one(s) to use as the basis of its product, service, and process certifications. These included the ISO/IEC 27000 series (discussed above), the NIST 800 series of standards¹⁵, NERC RSTC¹⁶, VDI/VDE 2182¹⁷, and ISO/IEC 15408¹⁸. However, it became clear that 62443 was the standard most frequently embraced by asset owners, most able to address IACS security across all industries, and most able to address the entire IACS lifecycle. It is also a global standard and thus embraced and recognized worldwide.

The Roots of ISA/IEC 62443

The family today known as ISA/IEC 62443 can be traced primarily to the ISA99 standards development committee^{19, 20}, and, to a lesser extent, a process automation users' association known as the WIB^{21, 22}. The ISA99 committee developed all of the currently released standards except 62443-2-422. Originally, they were known as the ANSI/ISA-99 series of standards, but they were renumbered in 2010 as ISA/IEC 62443 after ISA99 and IEC TC 65 developed a formal liaison agreement²³. As such, any references to ANSI/ISA-99 documents are largely obsolete and instead covered under 62443.

ISA/IEC 62443 has today grown into a family of nine technical specifications, technical reports, and international standards with additional documents in the family currently in various stages of preparation (refer to Table 224). The family is jointly available from both ISA and IEC and can be purchased from either organization. The technical content in the ISA and IEC versions is identical; the versions differ only in their non-normative content such as copyright statements, forewords, preambles, and introductions.

At first glance, ISA/IEC 62443 can be bewildering and overwhelming due to its size and complexity. It currently comprises more than 1,000 pages and is continually growing as new content is being developed and approved by the voting members. 62443 comes under the oversight of ISA99 and IEC Technical Committee 65 / Working Group 10 (TC 65/WG 10).

Numbering Scheme

The IEC numbering scheme is of the format 62443-T-P:YYYY where T and P are the tier and part, respectively, and YYYY is the year of publication. For example, IEC 62443-1-1:2009 refers to Part 1-1 published in 2009 (Edition 1.0). The ANSI/ISA numbering scheme is nearly identical but uses a dash instead of a colon to set off the year of publication (62443-T-P-YYYY). For example, ANSI/ISA-62443-4-2-2018 refers to Part 4-2 published in 2018 (Edition 1.0). When the edition or year of publication is not of importance, the YYYY is generally dropped.

Scope of ISA/IEC 62443

ISA/IEC 62443 does not confine itself simply to technology. It also concerns itself with people, processes, and the entire lifecycle of an IACS to ensure that a system that is cybersecure at time of commissioning remains cybersecure throughout its life. This is conveyed in Figure 1.

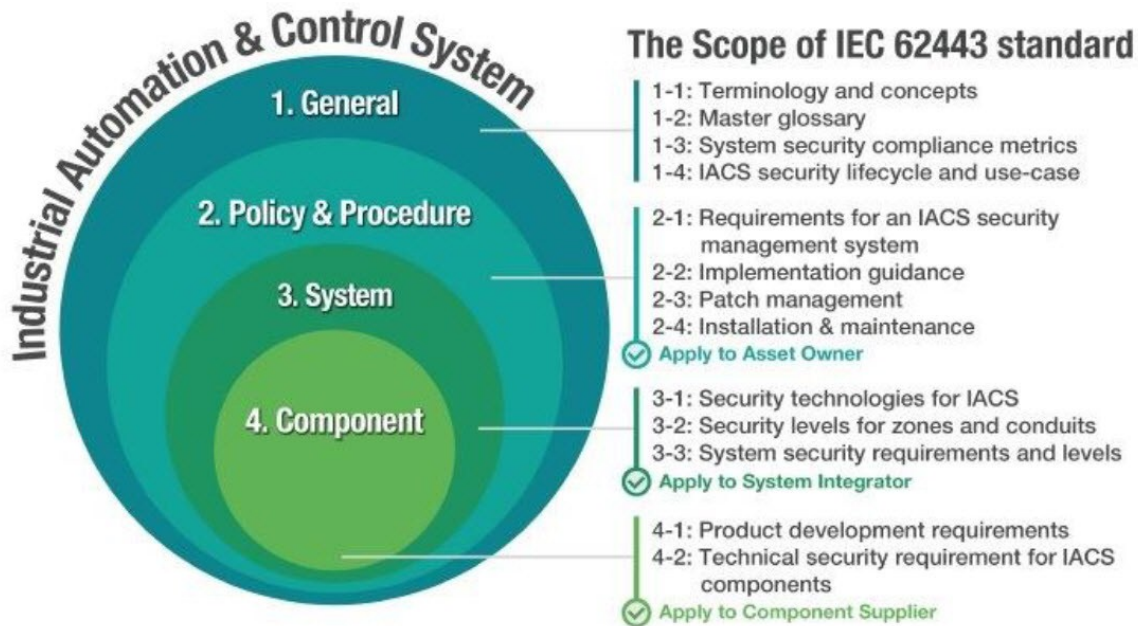


Figure 1: The ISA/IEC 62443 family is currently composed of four “tiers”, each with a primary intended audience and focus. Another tier (Tier 6) is currently in development along with several new parts (see Table 2).

Status of Constituent 62443 Parts

Table 2 shows the current release status of the various documents within the 62443 family. Of particular interest to component manufacturers is the content under development for Part 6 of the standard as this will allow a more uniform and consistent approach to conformity assessment against 2-4 and 4-2 and thus less variations in the certifications issued by different certifying bodies (CBs). It also allows manufacturers such as Bently Nevada to self-assess their readiness for the certification process and even to include the same test criteria in their product release practices that a CB would use. This helps to ensure that both the spirit and letter of the 62443 requirements are understood and met.

As would be expected, cybersecurity is a rapidly evolving topic and the 62443 family is likewise evolving to maintain pace with changes in technology, threats, and best practices. IEC standards undergo a 5-year cycle during which they must be reaffirmed, amended, replaced with a new edition, or withdrawn. This helps ensure they remain current and relevant. For example, the stability date²⁵ in Table 2 indicates that many of the documents in the series are coming due to be updated or reaffirmed.

Table 2: Structure and Content of ISA/IEC 62443²⁴

Tier	Released	Parts / Content	Stability ²⁵	Edition	Type ²⁶	Date
1 General	Tier 1 covers topics that are common to the entire family :					
	Yes	Part 1-1: Terminology, concepts, and models	2025	1.0	TS	7/2009
	No	Part 1-2: Master glossary of terms and definitions ²⁷		1.0	TR	
	No	Part 1-3: System security conformance metrics ²⁷		1.0	IS	
	No	Part 1-4: IACS security lifecycle and use cases ²⁷		1.0	TR	
	Yes	Part 1-5: Scheme for 62443 cyber security profiles.	2026	1.0	TS	9/2023
	No	Part 1-6: Application of the IEC 62443 standards to the Industrial Internet of Things ²⁸		1.0	TS	03/2025

Tier	Released	Parts / Content	Stability ²⁵	Edition	Type ²⁶	Date
2 Policies and Procedures	Tier 2 focuses on methods and processes associated with IACS security and pertains primarily to owners and users of IACS, as well as IACS service providers to owners and users:					
	Yes	Part 2-1: Establishing an IACS security program	2027	2.0	IS	08/2024
	No	Part 2-2: IACS Security Protection ²⁸		1.0	IS	8/2024
	Yes	Part 2-3: Patch management in the IACS environment	2027	1.0	TR	6/2015
	Yes	Part 2-4: Security program requirements for IACS service providers	2027	2.0	IS	12/2023
	No	Part 2-5: Implementation guidance for IACS asset owners ²⁷		1.0	IS	
3 System	Tier 3 is about requirements at the system level and pertains to those with system responsibilities (i.e., system integrators):					
	Yes	Part 3-1: Security technologies for IACS	2027	1.0	TR	7/2009
	Yes	Part 3-2: Security risk assessment for system design	2027	1.0	IS	6/2020
	Yes	Part 3-3: System security requirements and security levels	2027	1.0	IS	8/2013

Tier	Released	Parts / Content	Stability ²⁵	Edition	Type ²⁶	Date
4 Components and Requirements	Tier 4 provides detailed requirements for IACS components (products) and pertains to component manufacturers such as Bently Nevada:					
	Yes	Part 4-1: Secure product development lifecycle requirements	2024	1.0	IS	1/2018
	Yes	Part 4-2: Technical security requirements for IACS components	2024	1.0	IS	2/2019
6 Conformance Evaluation Methodology	Tier 6 provides evaluation methodologies for determining conformance of component suppliers and service providers to selected parts of 62443:					
	Yes	Part 6-1: Security evaluation methodology for 62443-2-4	2026	1.0	TS	3/2024
	No	Part 6-2: Security evaluation methodology for 62443-4-2 ²⁸		1.0	TS	4/2025

2. Key Concepts

Most readers of this series of articles will have a particular interest in the certification of Bently Nevada products, processes, and services. Consequently, the key concepts identified here are not intended to capture all major topics within the 62443 family, but merely those especially relevant to understanding certification schemes.

Roles

An important key to understanding 62443 is that it segments the participants involved in IACS cybersecurity into four distinct roles:

1. **Asset owners**

Asset owners own (or are responsible for) the IACS. They establish an IACS security program within their organization, manage that program by means of a CSMS, and select IACS service providers, system integrators, and component suppliers that comply with 62443 parts 2, 3, and 4 respectively. This compliance is most easily ascertained when the suppliers are *certified* to the relevant portions of ISA/IEC 62443. Hence, the substantial industry emphasis on 62443 *system* (part 3-3), *component* (part 4-2), and *service provider* (part 2-4) certifications. System and component providers are also frequently requested to certify their secure development processes to part 4-1 of the standard.

2. **Service providers**

Service in 62443 is divided into two categories: integration services and maintenance services. Service providers are certified to Part 2-4 of the standard which contains 120+ enumerated **security program requirements** (SPs) that an asset owner may request in the service provider's security program.

3. **System providers (integrators)**

System providers are responsible for developing the overall automation solution from components and subsystems. The systems are certified to part 3-3 of the standard which contains 100 enumerated **system requirements** (SRs). System providers can also have their product development processes certified to part 4-1 of the standard which contains 47 enumerated **secure development lifecycle** (SDL) requirements.

4. **Component providers**

Component providers are analogous to system providers, but they provide individual components instead of integrated collections of components (systems). Components are certified to part 4-2 of the standard which contains 120+ enumerated **component requirements** (CRs). Component providers can also be certified to part 4-1 of the standard which contains 47 enumerated secure development lifecycle (SDL) requirements. 4-2 certifies products²⁹ while 4-1 certifies processes³⁰.

Different parts of the 62443 family are thus intended to pertain to different roles, as shown in both Figure 1 and Figure 2.

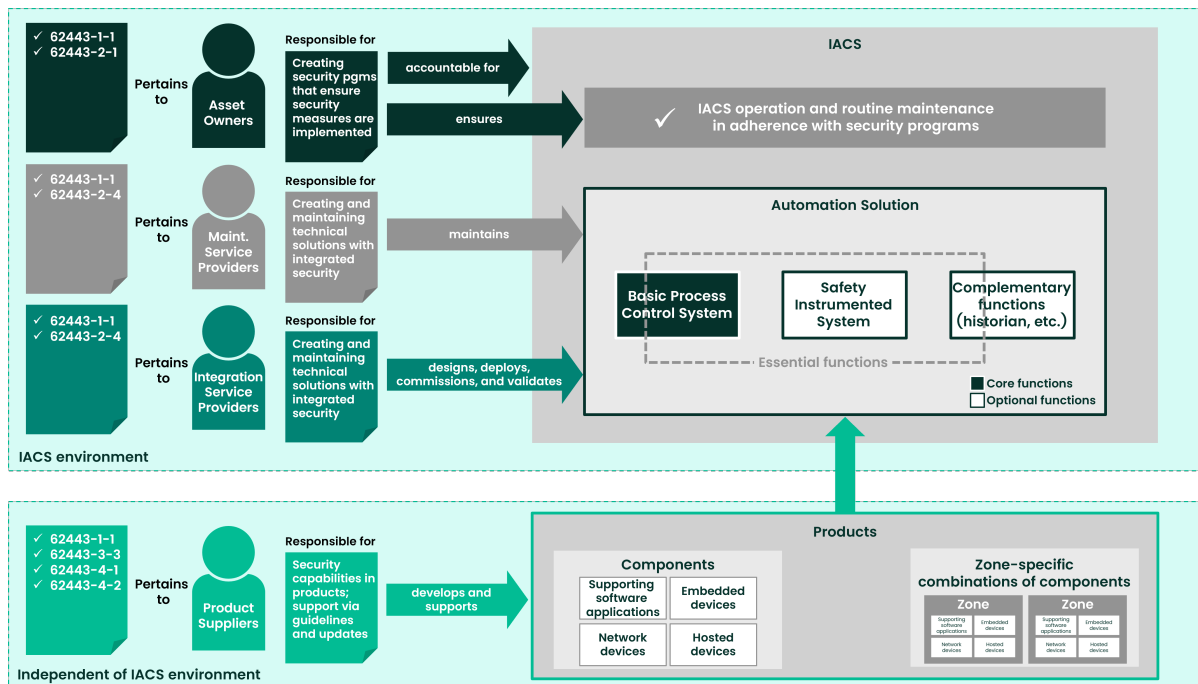


Figure 2: Different parts of the ISA/IEC 62443 family pertain to each of the four roles depicted here³¹. Product Suppliers are shown at the bottom of the figure and may be either System Providers (3-3 pertains) or Component Providers (4-2 pertains). Part 4-1 (process) pertains to both System Providers and Component Providers. Part 1-1 pertains to all roles.

In some cases, a single entity may perform multiple roles. For example, some asset owners may have their own in-house instrument & control staff that provides maintenance. In this instance, they are both asset owners and maintenance service providers. Or, a manufacturer may also have extensive system integration capabilities and field product maintenance capabilities, thus conceivably acting in the three bottom-most roles of Figure 2. In other instances, the roles may be filled by four separate and distinct entities. The key is that the portion of 62443 that pertains is a function of the role and its corresponding responsibilities.

Essential Functions

The distinction between essential and non-essential functions is an important aspect of 62443. It defines an essential function as follows:

Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.

62443 further clarifies that:

Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively.

Notice, for example, that less than 100% of the BPCS box and less than 100% of the Complementary Functions box in Figure 2 are encompassed by the "Essential Functions" box. This is because there are parts of these systems that are not strictly required in order to maintain health, safety, the environment, or availability of the equipment under control. As an example, the BPCS might have local displays or indicators on some of the loop controllers. If these local indicators were to fail, it may be

inconvenient for operators and maintenance personnel, but the controller could still continue to provide its essential functions: to control the loop within its setpoints (constraints) and to provide this information on the primary operator display stations in the main control room.

Many Bently Nevada products, such as Orbit 60, provide machinery protection. As such, this aspect of the component would be considered an essential function while other aspects – such as the ability to generate an event log or report–would not.

Security Levels (SLs)

The concept of SLs is fundamental to understanding 62443. The standard defines four security levels³² with SL 1 being the least stringent and SL 4 being the most stringent. Table 3 summarizes the relative differences between – and intent of – the four security levels.

Table 3: Security Levels (SLs) as defined in 62443-3-3 Annex A

SL	Protection Against	Profile	Skills	Motivation	Means	Resources
1	Casual or coincidental violation	Staff	None	Mistakes	Unintentional	Individual
2	Intentional violation	Low-Level Hacker	Generic	Low	Simple	Low (isolated individuals)
3	Intentional violation	Hacker, Terrorist	IACS-specific	Moderate	Sophisticated (attack)	Moderate (hacker groups)
4	Intentional violation	Nation State	IACS-specific	High	Sophisticated (campaign)	Extended (multi-disciplinary teams)

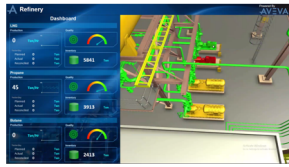
It is also worth noting that 62443 discusses **achieved** security levels (SL-As), **target** security levels (SL-Ts) and **capability** security levels (SL-Cs). The SL-T is the SL the asset owner has decided is required for a particular zone ([see Zones on the next page](#)). The SL-A is the SL that is actually reached and is based on component configurations, interconnections, networks, and other factors such as the firmware version of a component or the discovery of a new vulnerability that has not yet been patched. The SL-C is the SL that the component is capable of (when configured and installed correctly) based on its conformity to the various CRs enumerated in part 4-2.

Part 3-3 of the standard provides an extensive narrative discussion of security levels in Annex A as well as the information contained in Table 4. It treats security levels as vectors that are best described in terms of multiple variables rather than a single number.

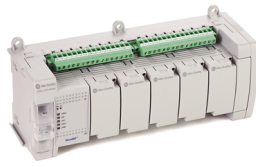
Components

Components are the basic hardware and software elements that make up systems and are defined in part 4-2. Components generally fall into one of four basic categories, as shown in Figure 3, but may sometimes be hybrid in nature and thus embody the characteristics of multiple categories.

Components can be certified to a particular SL-C using the criteria in part 4-2. This is discussed in greater depth in part III of this article series.



Software Applications
(e.g., HMI software)



Embedded Devices
(e.g., PLCs)



Host Devices
(e.g., panel-mount PCs)



Network Devices
(e.g., industrial firewalls)

Figure 3: Components can be classified according to the four different device types described in 62443-4-2. Some components may reflect multiple device types. Most Bently Nevada products (excluding software) are considered “embedded devices”.

Systems

Systems are analogous to components and are indeed comprised of components. Like components, they can be certified to a particular SL-C but use part 3-3 of the standard instead of part 4-2 as the basis of certification.

Zones

Zones are the groupings of systems, components, and interconnecting networks that have a common security level. 62443 defines a zone as follows:

Grouping of logical or physical assets that share common security requirements.

It also clarifies the concept of a zone as follows:

A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

The concept of a zone is important because the achieved security level of a zone is governed by the security levels of the components and systems within the zone. Thus, a zone may have a target security level (SL-T) of 3, but it will only have an achieved security level of 3 if all of the components and systems within the zone have an SL-A of 3 or higher.

Communication Channels

A communication channel is simply the logical or physical communication link between IACS assets. For example, a channel is what allows a connection to be established between a software component and an embedded device, allowing them to communicate with one another.

Conduits

Conduits are groups of communication channels and are considered a special type of security zone. When conduits connect one zone to another zone, they are designed in such a way to preserve the desired security level. Thus, if a conduit connects one Zone 2 area to another Zone 2 area, the conduit itself must meet or exceed SL-A 2.

Compensating Countermeasures

When a component or system is unable to inherently meet a particular CR or SR without external apparatus or special precautions, a countermeasure is required to compensate for the deficiency.

The countermeasure thus compensates for the inability of the system or component to natively conform to a requirement. An example might be the need for a locked cabinet to house apparatus that does not provide inherent protection against physical tampering along with a switch that alerts personnel and generates a log entry when the cabinet is opened.

Maturity Levels (MLs)

When seeking certification of its SDL processes to part 4-1 of the standard, it is useful to classify a product manufacturer's degree of process rigor to distinguish those with only rudimentary practices from those with more advanced practices. Maturity Levels are thus defined in part 4-1 of the standard, allowing asset owners to better understand a product manufacturer's ability to create and sustain secure products. These levels are summarized in Table 4.

Table 4: SDL Process Maturity Levels

ML	Phase	Description
1	Initial	Processes are ad hoc and undocumented or incompletely documented
2	Managed	Processes are fully documented but not entirely implemented
3	Practiced	Processes are fully documented and fully implemented
4	Improving	Process are fully documented and implemented, with active measurement of results and continuous improvement

Foundational Requirements (FRs)

For convenience and harmonization of numbering, CRs and SRs are organized into subgroups where each subgroup has common attributes that are foundational to robust cybersecurity. These are known as foundational requirements and fall into the following seven categories:

- **FR 1: Identification and Authentication Control**

This describes all of the CRs or SRs that pertain to identifying and authenticating users — whether human or other connected devices — and thus protection against access by unidentified and unauthenticated users. For example, SR 1.4 and CR 1.4 pertain to identifier (e.g., username) management while SR 1.5 and CR 1.5 pertain to authenticator (e.g., password) management. There are 14 individual system or component requirements (1.1 – 1.14) within the FR 1 category.

- **FR 2: Use Control**

This describes all of the CRs or SRs that pertain to enforcement of privileges and restrictions on how the system or component may be used. For example, a user may have view privileges for data but not edit privileges and the system or component must enforce these restrictions (see SR 2.1 and CR 2.1). There are 13 individual system or component requirements (2.1 – 2.13) within the FR 2 category.

- **FR 3: System Integrity**

This describes all of the CRs or SRs that pertain to protection against unauthorized manipulation or modification of the system or component. For example, SR 3.10 and CR 3.10 require the ability to update/upgrade systems and components to address new security vulnerabilities as they are discovered, and hardware manufacturers typically provide such capabilities via firmware

upgrades. There are 14 individual system or component requirements (3.1 – 3.14) within the FR 3 category.

- **FR 4: Data Confidentiality**

This describes all of the CRs or SRs that pertain to data confidentiality and thus protection against disclosure of data to unauthorized parties. For example, SR 4.2 and CR 4.2 require the ability to perform a factory reset on hardware devices such that all protected information is erased. There are 3 individual system or component requirements (4.1 – 4.3) within the FR 4 category.

- **FR 5: Restricted Data Flow**

This describes all of the CRs or SRs that pertain to the segmentation of the IACS into zones and conduits such that the flow of data into unnecessary zones or conduits is limited. For example, SR 5.1 and CR 5.1 require devices with multiple network connectors to be isolated from one another such that one connector can serve one zone and the other connector can serve a different zone. There are 4 individual system or component requirements (5.1 – 5.4) within the FR 5 category.

- **FR 6: Timely Response to Events**

This describes all of the CRs or SRs that pertain to notification of security violations in both a proper and timely manner. For example, SR 6.1 and CR 6.1 require the ability for authorized users to be able to view (but not edit) logs of security-related events occurring in the system or component. There are 2 individual system or component requirements (6.1 – 6.2) within the FR 6 category.

- **FR 7: Resource Availability**

This describes all of the CRs or SRs that pertain to protection against degradation or denial of essential functions under Denial of Service (DoS) events. For example, SR 7.4 and CR 7.4 require the ability to restore a system or component to a known secure state after a disruption or failure. There are 8 individual system or component requirements (7.1 – 7.8) within the FR 7 category.

3. IEC 62443 Parts

Given this background, we now show briefly how the various parts harmonize with one another to address the needs of asset owners, service providers, and product manufacturers.

Part 3-3: Product Certification

Pertains to: Product Manufacturers

Product Types: Systems

Part 3-3 contains enumerated SRs consisting of base requirements and requirement enhancements (REs). Annex B in part 3-3 maps each SR and RE against the corresponding Capability Security Level 1-4. In this manner, a system provider can see exactly which requirements (and requirement enhancements) are needed to meet a particular SL-C. SL-C1 has the least number of requirements (38) while SL-C4 has the most (100).

Because a system can be no more secure than the security of its weakest link, it cannot have an SL-C greater than that of its components. For example, if a system consists of three components meeting SL-C2 and eight components meeting SL-C3, the system itself cannot exceed SL-C2.

The details of system requirements, guidance on how to read and interpret a 3-3 conformity certificate, and a more comprehensive description of part 3-3 of the standard is slated for a future date (part XI) in this series of white papers.

Part 4-2: Product Certification

Pertains to: Product Manufacturers

Product Types: Components

For every SR in Part 3-3, there is a corresponding CR in Part 4-2. In other words, SRs and CRs are harmonized such that they pertain to the same security attributes and use the same numbering. The only difference is that the nomenclature for system requirements is SR X.X while that for component requirements is CR X.X. CRs are enumerated in part 4-2 and organized into base requirements and requirement enhancements (REs). Annex B in part 4-2 maps each CR and RE against the corresponding Capability Security Level 1-4. In this manner, a component manufacturer can see exactly which requirements (and requirement enhancements) are needed to meet a particular SL-C. SL-C1 has the least number of requirements (55) while SL-C4 has the most (102)³³.

The details of component requirements, guidance on how to read and interpret a 4-2 conformity certificate (see Figure 4), and a more comprehensive description of part 4-2 of the standard are covered in part III of this series of white papers.


VALID DE 7-0872	Cyber Security Certificate 2023-12-19
TYPE Product Capability Assessment	
CERTIFICATE COVERAGE (INCLUDING VERSION) UPS management interface card; SCMSX1000X2X3 (X1=0 or 1; X2, X3=0-9, A-Z; see the report for definition of variables X). (Version V1.0.1)	
STANDARD(S) USED IEC 62443-4-2:2019	
REQUIREMENTS ASSESSED Common Component Security Constraints (4,0,4) Identification and authentication control (11,11,22) Use Control (11,10,21) System Integrity (8,11,19) Data Confidentiality (3,2,5) Restricted data flow (1,3,4) Timely response to events (2,1,3) Resource availability (9,2,11) SAR (0,3,3) EDR (6,7,13) HDR (0,14,14) NDR (0,22,22)	
DATE OF ISSUE 2023-12-19	
CERTIFICATE ISSUED BY <div style="display: flex; justify-content: space-between; align-items: center;"> <div> TÜV NORD CERT GmbH Am TÜV 1 Essen 45307 Germany </div> <div style="text-align: center;">  </div> </div>	

Figure 4: A typical cybersecurity certificate for a component conforming to 62443-4-2. Because this particular component is an embedded device, it does not (nor does it need to) conform with any of the requirements for a network device, a host device, or a software application and thus no requirements were assessed in those categories. Notice also that certification can be granted even though the assessed requirements in any given category are less than the total requirements. This is discussed in greater detail in part III of this white paper series. Certificates for conformity with 2-4, 3-3, and 4-1 are similar in format and provide a granular breakdown showing how the system, component, or service provider scored against the relevant criteria in each category. However, the categories differ depending on whether the certificate pertains to 2-4, 3-3, 4-1, or 4-2.

Part 4-1: Secure Development Lifecycle (SDL) Process Certification

Pertains to: Product Manufacturers

Product Types: Systems, Components

Whether a product provider is focused on systems or components, the SDL process they use should reflect the ability to create products that are “secure by design” and then sustain that security over the lifecycle. Part 4-1 outlines the elements of a **Secure Development Lifecycle process** against which the product provider’s own processes can be audited for conformity assessment. This is often termed SDLA (Secure Development Lifecycle Assessment) or PCA (Process Conformity Assessment).

There are 8 “practices” within 4-1 that are analogous in spirit to the 7 foundational requirements used in 3-3 and 4-2. Thus, individual process requirements are grouped under these 8 practices. For example, practice 2 deals with the *specification* of security requirements and has 5 requirements (SR-

1 through SR-5) while practice 4 deals with the *implementation* of security requirements and has 2 requirements (SI-1 and SI-2). There are 47 total requirements across the 8 practices within 4-1. The robustness of a manufacturer's SDL process can thus be ascertained by not only the number of practices with which they conform, but also their maturity level (1-4) and this is quantitatively conveyed in the conformity certificate issued. An example of a conformity certificate issued against 4-1 is shown in Figure 5.

It is important to note that in order for a provider's products to be certified to 3-3 or 4-2, their SDL process must first be certified to 4-1. This ensures that a product will be securely managed over its lifecycle – not just at time of development.

The details of process certification, guidance on how to read and interpret a 4-1 conformity certificate, and a more comprehensive description of part 4-1 of the standard are covered in part II of this series of white papers.

VALID FR_Cyber10115	Cyber Security Certificate 2023-12-08
TYPE Process Capability Assessment	
CERTIFICATE COVERAGE (INCLUDING VERSION) CTC Union Product Security Development Lifecycle & Process V1.0.0	
STANDARD(S) USED IEC 62443-4-1:2018	
REQUIREMENTS ASSESSED Security management (13,0,13) Specification of security requirements (5,0,5) Security by design (4,0,4) Secure implementation (2,0,2) Security verification and validation testing (5,0,5) Management of security-related issues (6,0,6) Security update management (5,0,5) Security guidelines (7,0,7) Maturity Level: ML2	
DATE OF ISSUE 2023-12-08	
CERTIFICATE ISSUED BY LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE 33 Avenue du Général Leclerc Fontenay-Aux-Roses 92260 France	

Figure 5: A typical cybersecurity certificate for an SDL process conforming to 62443-4-1. This is discussed in greater detail in part II of this white paper series. Certificates for conformity with 2-4, 3-3, and 4-2 are similar in format and provide a granular breakdown showing how the system, component, or service provider scored against the relevant criteria in each category. However, the categories differ depending on whether the certificate pertains to 2-4, 3-3, 4-1, or 4-2.

Part 2-4: Security Program Certification

Pertains to: Service Providers and Asset Owners

Service Types: Maintenance Services, Integration Services

Part 2-4 of the standard enumerates the 120+ **security program (requirements)** (SPs) that an asset owner may request in the service provider's security program. The precise number of SPs needed by an asset owner is subject to negotiation with the service provider and is based on the type of service performed and the security levels of the systems and components requiring service. An asset owner will thus assemble in a la carte fashion the list of SPs that they require and will generally want the service provider's security program to be certified for conformity to 62443-2-4.

There are 14 functional areas into which the SPs are categorized/grouped. When examining a 2-4 conformity certificate, the service provider's score within each of these 14 functional areas is thus provided.

The details of service provider security program certification, guidance on how to read and interpret a 2-4 conformity certificate, and a more comprehensive description of part 2-4 of the standard will be covered in a future installment (part XI) in this series of white papers.

Part 1-1: Terminology, Concepts, and Models

Pertains to: All roles

Part 1-1 of the standard provides common concepts, definitions, terms, and models used throughout all the other parts of the standard. It is not designed as a document against which conformity can be assessed and there are thus no certifications issued to part 1-1. It is highly useful when interpreting other parts of the standard and in understanding the individual parts within the context of the whole.

Part 2-1: Establishing an IACS Security Program

Pertains to: Asset Owners

Part 2-1 defines the elements necessary to establish a cyber security management system (CSMS) for an IACS and provides guidance on how to develop those elements. It is designed as a document against which conformity can be assessed so that an asset owner's CSMS can be evaluated and its robustness quantified.

Part 2-3: Patch Management in the IACS Environment

Pertains to: Asset Owners and Product Providers

Part 2-3 contains recommendations for asset owners and product suppliers with a series of best practices and examples for managing patches, along with insight into the consequences of poor patch management. Patches are designed to resolve bugs, operability, reliability, and cyber security vulnerabilities and may be variously referred to as:

- upgrades
- service packs
- hotfixes
- basic input output system (BIOS) updates
- other digital electronic program updates

Because part 2-3 is a technical report, it is not designed as a document against which conformity can be assessed. Consequently, there are no certifications issued to part 2-3.

Part 3-1: Security Technologies for IACS

Pertains to: All roles

Part 3-1 categorizes and defines cybersecurity technologies, countermeasures, and tools currently available to provide a common basis for later technical reports and standards to be produced within the 62443 series. Its intent is to document the known state of the art of cybersecurity technologies, tools, and countermeasures applicable to the IACS environment, clearly define which technologies can reasonably be deployed today, and define areas where more research may be needed.

Because part 3-1 is a technical report, it is not designed as a document against which conformity can be assessed. Consequently, there are no certifications issued to part 3-1.

Part 3-2: Security Risk Assessment for System Design

Pertains to: All roles (but has special relevance for asset owners)

Part 3-2 provides guidance to those responsible for designing an IACS in terms of zones and conduits. It helps the asset owner with the process of assessing risk and applying security countermeasures to reduce risk to tolerable levels. This is done by determining target security levels for various zones and conduits and aligning them with the capability security levels of the systems within each zone.

Asset owners can be assessed against the requirements of Part 3-2 in order to document their achieved security levels (SL-A), allowing them to ensure that they are meeting or exceeding their target security levels (SL-T).

Part 6-1: Security Evaluation Methodology for 62443-2-4

Pertains to: Certifying Bodies, Service Providers

Part 6-1 is slated for release in 2024 and is thus currently nearing release. When released, it will address two important issues:

- Certificates for conformity assessment against IEC 62443-2-4 issued by different CBs are not comparable because there is no uniform and consistent evaluation methodology used across all CBs.
- Service providers do not know the evaluation criteria that a CB will use to assess conformity and it becomes difficult to confidently build a security program that will pass a conformity audit without multiple iterations and refinements.

Part 6-1 will resolve these issues by providing a consistent methodology for assessing conformity of a service provider's security program to each SP in part 2-4.

Part 6-2: Security Evaluation Methodology for 62443-4-2

Pertains to: Certifying Bodies, Component Manufacturers

Part 6-2 is not slated for release until early 2025 and is currently in preparation. When released, it will address two important issues:

- Certificates for conformity assessment against IEC 62443-4-2 issued by different CBs are not comparable because there is no uniform and consistent evaluation methodology used across all CBs.
- Component manufacturers do not know the evaluation criteria that a CB will use to assess conformity and it becomes difficult to generate user requirements, test plans, and audit readiness when developing products that are to conform to the standard.

Part 6-2 will resolve these issues by providing a consistent methodology for assessing conformity of a component to each CR and RE in part 4-2.

4. Certification Schemes

Certification for conformity with the relevant parts of ISA/IEC 62443 are generally issued according to one of the following three schemes:

1. **The IECCE certification scheme**

Bently Nevada has elected to use this certification scheme and this series of White Papers thus assumes both the IECCE certificate format and scoring rubric. As of this writing, the [IECCE scheme](#) represents the majority of certifications across the industry³⁴.

2. **The ISASecure® certification scheme**

The [ISASecure scheme](#) gives manufacturers less flexibility in their conformity strategy but is nevertheless a robust, transparent, and well-respected scheme.

3. **CB-specific certification schemes**

Certain certification bodies offer their own conformity schemes that are not tied to either the IECCE scheme or the ISASecure scheme. [Exida](#) and [TÜV Rhineland](#) are two such examples, but they also offer ISASecure® certifications as an alternative to their own “in house” brands.

Some certification bodies offer only certification against the IECCE scheme, while others offer both IECCE and ISASecure, while still others offer only ISASecure. Manufacturers such as Bently Nevada ultimately select a certification body based on the certification scheme they wish to use, market acceptance of the certification scheme, and the reputation and quality of the CB. Regardless of the scheme used, all certificates show the identity of the CB used.

5. Summary

The ISA/IEC 62443 family of standards³⁵ has emerged as the leading consolidation of industry best practices for OT cybersecurity, growing out of work originally performed primarily by the ISA99 committee. Like all good standards, it arose from an unmet industry need where practical guidance was required via a document carrying the weight of an international standard and with sufficient detail to allow compliance audits and corresponding certifications for manufacturers and service providers seeking conformity of their offerings with the standard. Today, more than a dozen certified bodies provide conformity assessment to the relevant parts of ISA/IEC 62443, underscoring that there is considerable demand by asset owners to establish certified cybersecurity regimens. It also underscores that asset owners are increasingly demanding the ability to purchase certified IACS systems and components from manufacturers, and to obtain integration and maintenance services from those with security programs that are certified to 62443.

In Part I of this article series, an overview of the ISA/IEC 62443 family of standards, has been provided to allow the reader to understand how the parts work together and which parts of the standard are used as the basis for conformity assessments of products and service providers. It was intended to be quite general in nature, without reference to particular Bently Nevada products and services. However, the remaining parts of this article series (refer to Table 1) are designed to more narrowly focus on specific parts of 62443 and/or on particular Bently Nevada products and services. For example, part IV addresses the conformity certificate to 62443-4-2 for Orbit 60 while part III discusses component conformity certifications in general. Combined, this series of notes allows the reader to understand why cybersecurity is important, how cybersecurity is achieved, and the ways in which Bently Nevada products and services deliver cybersecure functionality that conforms to recognized industry standards.

6. Recommended Additional Reading

- *Quick Start Guide: An Overview of ISA/IEC 62443 Standards: Security of Industrial Automation and Control Systems*

June 2020, ISA Global Cybersecurity Alliance (www.isa.org/isagca)

- *Industrial Automation and Control System Taxonomy: Definition of Terms*

Dec 2020, ISA Global Cybersecurity Alliance (www.isa.org/isagca)

- *Security Lifecycles in the ISA/IEC 62443 Series: Security of Industrial Automation and Control Systems*

Oct 2020, ISA Global Cybersecurity Alliance (www.isa.org/isagca)

- *Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments*

Jul 2021, ISA Global Cybersecurity Alliance (www.isa.org/isagca)

- *Effective ICS Cybersecurity Using the IEC 62443 Standard*

Nov 2020, SANS Institute (www.sans.org)

- *Understanding IEC 62443*

Feb 2021, IEC (www.iec.ch)

- *IoT Security Lab: What is IEC 62443*

Feb 2021, Cisco (www.cisco.com)

7. Endnotes

1. The Orbit 60 platform is the first product to receive certification to 62443-4-2 and is discussed in parts IV, V, and VI of this series.
2. Operational Technology is defined as networks, control systems, computers, software, and other automation apparatus focused on controlling and monitoring industrial processes. This can also include environmental systems such as building heating, ventilation, and air conditioning (HVAC).
3. [“A brief history of computer viruses and what the future holds”](#), Kaspersky Labs (retrieved Nov 1, 2021)
4. Kushner, D., [“The Real Story of Stuxnet”](#), IEEE Spectrum, Feb 2013, IEEE (retrieved Nov 1, 2021)
5. In the case of Stuxnet, the infected devices were Siemens PLCs.
6. In the case of Stuxnet, the motivation was national security and the goal was to impede the development of Iran’s nuclear weapons program; the actors were believed to be the Israeli and US governments.
7. The Stuxnet Worm is thought to have destroyed 20% of Iran’s uranium enrichment centrifuges, or about 1,000 machines. See: Broad, W., Markoff, J., Sanger, D., [“Israeli Test on Worm Called Crucial in Iran Nuclear Delay”](#) Jan 15, 2011, New York Times (retrieved Nov 1, 2021)
8. This ability to damage or destroy physical assets via a cybersecurity breach is now known as a “cyber-kinetic attack.” Source: “Cyber-Kinetic Attack.” Wikipedia, Wikimedia Foundation, 29 July 2021, https://en.wikipedia.org/wiki/Cyber-kinetic_attack.
9. Hemsley, K., Fisher, R. [“History of Industrial Control System Cyber Incidents”](#), Report INL/CON-18-44411 (Rev 2), Idaho National Laboratory, Dec 2018
10. ICS Alert (IR-ALERT-H-16-056-01), [“Cyber-Attack Against Ukrainian Critical Infrastructure”](#), Feb 25, 2016, US Cybersecurity & Infrastructure Security Agency (www.cisa.gov)
11. “Aurora Generator Test.” Wikipedia, Wikimedia Foundation, 3 May 2021, https://en.wikipedia.org/wiki/Aurora_Generator_Test.
12. Chhillar, S. [“Common ICS Myth #4: Serial Communications”](#) Jan 12, 2021, ISAGCA Blog (<https://gca.isa.org/blog>), (accessed Nov 4, 2021)
13. The attackers overwhelmed utility call centers with automated telephone calls, impacting the ability to receive outage reports from customers and frustrating response efforts. This highlights the level of sophistication and coordination that can characterize a cyberattack. Source: [“Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case”](#), Report, March 18, 2016, Electricity Information Sharing and Analysis Center (www.eisac.com), Washington, DC. (retrieved 15 April 2024)
14. ISO/IEC 27000:2018 “Information technology — Security techniques — Information security management systems — Overview and vocabulary”

15. <https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information>
16. North American Electric Reliability Council – Reliability and Security Technical Committee (<https://www.nerc.com/comm/RSTC/Pages/default.aspx>)
17. VDI/VDE 2182 is a series of German standards also dealing with cybersecurity of industrial automation systems. It was submitted to and used by the IEC working group (TC 65/WG 10) responsible for 62443, but did not influence the content of 62443 as heavily as the ISA99 committee or the WIB.
18. ISO/IEC 15408-1:2022 “Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model”
19. ISA99 Standards Development Committee: Industrial Automation and Control Systems Security
20. Cosman, E. “Speaking of Standards,” InTech Magazine, Sept/Oct 2020, International Society of Automation (retrieved Oct 2021)
21. “WIB Releases Comprehensive Cyber Security Standard” Nov 10, 2010, automation.com. .
22. The document that would later become ISA/IEC 62443-2-4:2017 was originally authored by Ted Angevaare as a Shell Design & Engineering Practice (DEP) specification, and then became WIB Report M2784 (now withdrawn). Source: <https://tedangevaare.nl/useful-standards/>
23. There are IEC [Type C Liaison Agreements](#) between ISA99 and both IEC TC 65/WG 10 and IEC TC 65/WG 23.
24. This table is based on information in the article Understanding IEC 62443 on the IEC website at <https://www.iec.ch/blog/understanding-iec-62443> (retrieved Oct 2021) as well as publicly available information on the same website pertaining to activities of IEC Technical Committee 65 (TC65) which is responsible for 62443.
25. The stability date reflects the date through which the standard will remain unchanged. After that date, the standard may be reaffirmed without changes, withdrawn, amended, or replaced by a revised edition.
26. IS = International Standard; TR= Technical Report; TS=Technical Specification
27. These documents are in the very early stages of preparation and do not yet have a forecasted publishing date.
28. These documents are not yet published but are in preparation with an expected release date as shown.
29. Refer to part III in this series of white papers for a detailed discussion of component certification to part 4-2.
30. Refer to part II in this series of white papers for a detailed discussion of SDL process certification to part 4-1.

31. This is a slightly modified version of Figure 2 in IEC 62443-4-1 ed. 1.0 and is used by permission. Copyright © 2018 IEC Geneva, Switzerland. www.iec.ch.
32. Technically, there is also the concept of Security Level 0 with no security requirements at all. When no SL is specified, it is assumed to be SL 0.
33. The exact number will depend on whether the component is an embedded device, a host device, a network device, or a software application. Network devices have the most numbers of requirements, while software applications have the fewest. The numbers shown in this white paper reflect an embedded device since it is the device type indicative of Bently Nevada hardware such as Orbit 60 and Orbit DCM.
34. As of Jan 2024, the IEC certification scheme accounts for 118 certifications to 62443-2-4, 18 to part 3-3, 91 to part 4-1, and 53 to part 4-2. In contrast, less than half this many certifications have currently been granted under the ISASecure schemes.
35. Bently Nevada thanks the International Electrotechnical Commission (IEC) for permission to reproduce information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by Bently Nevada, nor is IEC in any way responsible for the other content or accuracy herein.



Bently Nevada, M2, Orbit 60, Orbit DCM, System 1 and Orbit Logo are registered trademarks of Bently Nevada, a Baker Hughes business, in the United States and other countries. The Baker Hughes logo is a trademark of Baker Hughes Company. All other product and company names are trademarks of their respective holders. Use of the trademarks does not imply any affiliation with or endorsement by the respective holders.

The information contained in this document is the property of Baker Hughes and its affiliates; and is subject to change without prior notice. It is being supplied as a service to our customers and may not be altered or its content repackaged without the express written consent of Baker Hughes. This product or associated products may be covered by one or more patents. See [Bentley.com/legal](https://www.bentley.com/legal).

1631 Bently Parkway South, Minden, Nevada USA 89423
Phone: 1.775.782.3611 (US) or [Bentley.com/support](https://www.bentley.com/support)
[Bentley.com](https://www.bentley.com)